Toward a Socio-Cognitive Stage Model of Cybersecurity Behavior Adoption

Cori Faklaris
CMU-HCII-22-101
June 2022

Human-Computer Interaction Institute,
School of Computer Science,
Carnegie Mellon University
5000 Forbes Ave.,
Pittsburgh, PA, 15213 USA

Thesis Committee:
Jason I. Hong (Co-chair, HCII)
Laura Dabbish (Co-chair, HCII)
Geoff Kaufman (HCII)
Sauvik Das (Georgia Institute of Technology)
Michelle Mazurek (University of Maryland, College Park)

Submitted in partial fulfillment of the requirements for the degree
of Doctor of Philosophy in Human-Computer Interaction

This work was supported by the U.S. National Science Foundation, grant no. CNS-1704087,
by the CyLab Security and Privacy Institute,
and by the Center for Informed Democracy and Social Cybersecurity.
Sponsors were not involved in any phase of research or thesis preparation.

Keywords: behavior change, behavior models, stage models, process models, usable security, psychometrics, mixed methods, quantitative, qualitative, cybersecurity, information security, data security, human-computer interaction, usability, security, user experience, social psychology, social influence, social cognition, password managers, two-factor authentication, multi-factor authentication, two-step authentication, passwords, software updates, device security, phishing, malware, scams, misinformation, fake news, false news, account sharing, user classification, user models, path diagram, security awareness, security adoption, technology acceptance, protection motivation, innovation diffusion

ABSTRACT

My research looks at how to apply insights from social psychology, marketing, and public health to reduce the costs of cybercrime and improve adoption of security practices. The central problem that I am addressing is the widespread lack of understanding of cyber-risks. While many solutions exist (such as using password managers), people often are not fully aware of what they do or use them regularly. To address the problem, we should look to insights from social psychology, marketing, and public health that behavior change unfolds as a process in time and is influenced at each stage by relevant contacts, and that interventions are more successful when grounded in appropriate theory. Other researchers have developed models to describe behaviors such as reasoned action, technology acceptance, health/wellness adoption, and innovation diffusion. But we lack a model that is specifically developed for end-user cybersecurity and that accounts for social influences and for non-adoption. In my thesis, I used an exploratory sequential mixed-methods approach to specify such a preliminary model, comprised of six steps of adoption, their step-associated social influences, and each step's obstacles to moving forward.

To this end, I conducted two phases of research. In Phase 1, a remote interview study (N=17), I gathered data to synthesize a common narrative of how people adopt security practices. In Phase 2, an online survey study (N=859), I validated the Phase 1 insights with a U.S. Census-matched panel of adults aged 18 and older. I documented the distribution of the steps of adoption for password managers (either built-in or separately installed), and which factors were significantly associated with each step. I then integrated these findings and triangulated them with prior research on the influences of threat awareness, social proof, advice-seeking, and caretaking roles in people's security behaviors.

The results are a data-driven diagram and description of the six steps of cybersecurity adoption and a survey-item algorithm for classifying people by adoption step. These steps are 0: No Learning or Threat Awareness, 1: Threat Awareness, 2: Security Learning, 3: Security Practice Implementation, 4: Security Practice Maintenance, and "X": Security Practice Rejection. My Step Classifications exhibit reliability and convergent validity, showing an expected significant variance by steps on mean scores for adapted Transtheoretical Model scales (p<.001). The trialability of password managers and the availability of troubleshooting help were significantly positively associated with adoption of password managers (Step 3 and Step 4, p<.001), and the lack of troubleshooting help was significantly positively associated with rejection of password managers (Step X, p<.001). Other authority influences (mandates, adoption leadership, caretaking) and peer/media influences (advice on password managers, exposure to news of others' security breach experiences) also were significantly associated with adoption decisions.

My thesis helps move the field of usable security away from "one size fits all" strategies by providing a theoretical basis and a method for segmenting the target audience for security interventions and directing resources to those segments most likely to benefit. It establishes an agenda for future experiments to validate whether specific step-matched interventions influence adoption and are more likely to lead to long-term change. It contributes to the literature on Diffusion of Innovations and extends other established theoretical models, such as Protection Motivation Theory, the Technology Acceptance Model, and the Transtheoretical Model. Finally, it suggests specific design interventions for boosting security adoption.

[this page intentionally left blank]

ACKNOWLEDGEMENTS

I started my PhD journey in August 2017. My cohort's orientation overlapped with a solar eclipse partially visible from Pittsburgh. This auspicious event, in the "Heart of the Lion" at 28º 52′ Leo Sign, foretold "success but also danger of loss"[1]. We experienced the latter most explicitly with the arrival of the Covid-19 pandemic, and most personally with the passings in 2021 of Women@SCS coordinator Olivia "Liv" Zane, and in 2022 of fellow PhD student Sujeath Pareddy. I am grateful to be alive and well amid so much suffering, and grateful to everyone in my life who has supported me, guided me, and comforted me along the way. You helped me to persist and finish my degree despite the many obstacles (such as forced WFH in a sweltering/freezing off-campus apartment!). Now I am open to new experiences, in the spirit of the beautiful "Super Flower Blood Moon" lunar eclipse[2] that overlapped with my work on this document.

Mentors, Collaborators, and Colleagues

It was my honor to have been co-advised in scholarship by Jason I. Hong and Laura Dabbish. I knew both of their work before arriving at the HCII, and I could never have dreamed ten years ago that I'd have the privilege of their time each week to receive their feedback and guidance. I developed into the scholar I am today thanks to their generous encouragement and their tips on communication and on meticulous methodology. They are each kind and thoughtful, incisive with their critiques, intent on fostering a social and comfortable working environment for their labs.

My academic advisor and counselor, Queenie Kravitz, was no less instrumental in keeping me on the right path to graduation and in offering seeming unlimited support, advice, and sodas and snacks. She is an angel walking this earth in human form.

It was also my extraordinary good fortune to be taught by and/or to earn the recommendations and support of Jodi Forlizzi, Lorrie Faith Cranor, Kathleen Carley, Jessica Hammer, Geoff Kaufman, Brad Myers, Niki Kittur, Raelin Musuraca, Skip Shelly, Motahhare Eslami, Patrick Carrington, Scott Hudson, Jeff Bigham, Chinmay Kulkarni, Françeska Xhakaj, Michael Hilton, Charlie Garrod, Ziv Scully, and Bailey Flanigan. I will miss seeing them and others, such as Nik Martelaro, John Zimmerman, Bob Kraut, Henny Admoni, Nicolas Christin, Lujo Bauer, Justine Sherry, Hirokazu Shirado, and Lining Yao, in the HCII kitchenette or in the halls of SCS or elsewhere on campus – but I know we will be running into each other frequently at conferences!

My lab mates are very close to my heart. At the forefront are Isadora Krsek and Maria Tomprou, who shared their small office with me in turn and put up with my frequent asides and questions. I also thank Bogdan Vasilescu, Hong Shen, Tianshi Li, Daniel Klug, Sophie Qiu, Siyan Zhao, Haojian Jin, Fannie Liu, Tianying Chen, David Widder, Zhongmin Cai, Fiona Nah, Alex Cabrera, and others for their camaraderie and their insights. I also would have far fewer papers and results without the help of Animesh Singh, Anahita Hassan, Faye Kollig, Serena Wang, Yunpeng Song, Cheul Young Park, and other research collaborators and assistants through the years.

I have found a welcoming and stimulating "community of communities" in human-computer interaction. Among those are CMU alums and thesis committee members Sauvik Das and Michelle

[1] https://astrologyking.com/solar-eclipse-august-2017/#:~:text=The%20solar%20eclipse%20on%20Monday,growth%20and%20happiness%20you%20desire.

[2] https://www.elitedaily.com/lifestyle/may-2022-super-flower-red-moon-lunar-eclipse-spiritual-meaning

Mazurek, who have both given generously of their time and their ideas to help improve my usable security research, as has my future colleague at the University of North Carolina at Charlotte, Heather Richter Lipford. I was lucky to get to know people outside my home labs even despite the pandemic, such as Yixin Zou, Allison McDonald, Moses Namara, Melinda McClure Haughey, Jack Parker, Maggie Oates, Jessica Colnago, Sanchari Das, Pardis Emami-Naeini, Hana Habib, and Tom Magelinski.

No one really knows the difficulties of this path in this moment in history except for my fellow HCII PhD students. I appreciate and am grateful for my time hanging out and working on class projects with these amazing researchers, such as Sam Reig, Julia Cambre, Karan Ahuja, Prerna Chikersal, Michael Xieyang Liu, Lea Albaugh, and Lynn Kirabo.

If I learned only one lesson in my time as a journalist, it was to make connections with the admins! I am deeply grateful to Lauren Hardwig, Nancy Beatty, Marian D'Amico, and others for their timely submission of my reimbursement requests and their help in navigating bureaucracy. I also value the assistance of and camaraderie with others in HCII and SCS such as Lindsay Olshenske, Catherine Copetas, Ryan Ries, Karen Harlan, Diana Rotondo, and Nicole Willis.

Family and Friends

My parents, Duke and Carol Faklaris, were the first people I told about that unexpected lightning bolt of an email informing me of my PhD acceptance. Their love and support has sustained me through my periodic mental and physical disabilities and has unflaggingly helped me, since a little girl, to challenge my intellect and dream big dreams. My dad and sister Kate Pinnow (along with friends Shawn Neidorf, Mark Athitakis, and Adam Hirsh) preceded me in grad school and helped me orient to this new world. My other sister, Andrea Harvey, and my brother, Jeff Faklaris, cheered me on with every milestone, as did my nieces Grace Pinnow, Emily Pinnow, and Lila Harvey, and nephew Triton Griffin; my brothers-in-law Tait Pinnow and David Griffin; and my extended family, including Joan and Joe Clark, Jan Briney, Bob and Dee Bockler, Roger Liss, and Peggy and John Bockler.

I don't think I would have stayed sane without the constant friendship of and regular Sunday NYT crosswords over Zoom with my Indianapolis "urban family": Nancy Orem, Robert Thompson, Kevin Poortinga, Chad Sievers, Chris Rickett, and Kaylene Rieman Rickett. I've been delighted to visit with them and with Diane Moore, Jon Murray, and Lyonna Lam during my PhD purgatory.

I didn't get out in Pittsburgh as much as I might have, thanks to the pandemic, but I was lucky to have the Zen Group of Pittsburgh here to help me reconnect with the social side of spiritual practice. Many thanks to Matthew Kizior and other members for their friendship and dharma devotion!

Funding Sponsors

This work was supported by the U.S. National Science Foundation, grant no. CNS-1704087. I also received fellowship support from the CyLab Security and Privacy Institute and the Center for Informed Democracy and Social Cybersecurity, both at Carnegie Mellon University. Sponsors were not involved in any phase of research or thesis preparation.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

My research goes to the core of a central problem in computing: the widespread lack of understanding of cyber-risks that leads to insecure behaviors [131,230,233–236]. This problem has persisted for decades, in which hundreds of millions of dollars and thousands of hours of staff time have been spent; and yet, human interaction is still blamed in more than 99 percent of cyberattacks [234]. My approach rejects the predominant "one size fits all" paradigm for security training and for the design of security tools and practices. Instead, I draw on prior work in social psychology, marketing, public health, and other fields that behavior change unfolds as a process in time and is influenced by relevant social contacts [31,51,117,124,157,171,210]. Moreover, behavior interventions are more successful when grounded in appropriate theory [33,49,82,87,88,121]. My goal is to produce a model of security behavior adoption by stage that will enable designing and directing interventions to those most likely to benefit.

1.1 Thesis Motivation

Computing systems are increasingly central to society, but many people do not understand enough about how they work or what cyber-threats to guard against [115], contributing to a global cybercrime cost of over $1 trillion [185]. While many good solutions exist (such as using password managers), people have been slow to become fully aware of what they do and to use them regularly [151,188,222]. Further, enterprise training can cost around $300,000 and hundreds of staff hours [180].

To reduce costs and improve awareness and adoption, we should look to insights from social psychology, marketing, and public health that behavior change unfolds as a process in time and can be influenced by contacts that are relevant at a given stage of the process, and that interventions are more successful when guided by appropriate theory. For example:

- Kreuter et al. [123,124] found that health communications regarding mammogram use were more effective when tailored to individual characteristics of the target audience, vs. cultural characteristics, and when delivered at a time and via a method (such as computer post or print magazine) to which they would be most receptive, as predicted by behavior change theories.
- Sahin and Thompson [172] found in a study of university faculty's learning about and adoption of instructional technology that use of self-directed informational sources, use of data analysis tools, and interaction with colleagues were significant predictors of their technology adoption level.
- Shi and Zhang [181] found in a study of online grocery shopping that customers' behavioral states evolved over time, varying by use of a specific decision aid (such as the interface sort function or a list of prior orders), baseline behavior state, and purchase category characteristics.
- Prochaska and DiClemente [158] identified ten experiential and behavioral processes (such as self-reevaluation and stimulus control) associated with participants' five stages of quitting smoking.
- Weinstein et al. [208,210] used messaging about radon risks to move undecided homeowners to decide to test for radon, and used how-to-act information to motivate decided homeowners to order in-home radon test kits.
- And Kelly et al. [117] found that recruiting opinion leaders to help diffuse HIV prevention strategies among gay men in clubs in three small U.S. cities was effective for increasing condom use, as measured by post-intervention community surveys.

A common thread in these examples is that the target audience for behavior change is analyzed and split into segments, either by stage in the change process or by individual characteristics. Researchers then can zoom in and identify the processes or factors that differentiate each segment and that can explain the evolution in time of thinking and emotions about the target behavior. This avoids a "one size fits all" approach and produces a classification scheme that can be used to design and direct an intervention to those who are most likely to benefit from it.

Researchers have created many models of behavior change, such as the Theory of Reasoned Action/Theory of Planned Behavior [2,74,132], the Technology Acceptance Model [46,47,197], the Transtheoretical Model [52,69,157,196], and Diffusion of Innovations [19,167,168]. However, no one has yet established or validated such a model for end-user cybersecurity, nor one that accounts for social influences by stage. Cybersecurity needs this new model. It is a more complex behavior system than those modeled in prior work, involving social interactions that occur both online and offline (for which time and place, anonymity, physical appearance, and physical distance can be very different [14,15,136]). Moreso than elsewhere in human-computer interaction, cybersecurity involves multiple actors with conflicting objectives (attackers, both internal and external, vs. an array of legitimate non-malicious users, such as administrators and end users), for whom usage of the same technologies will vary dramatically [20]. It also is unlike physical security, say for nuclear defense, because it is much messier in terms of number and kinds of actors, involving massively more distributed technologies, the lack of a shared consensual outcome among all stakeholders, and widespread disagreements about which security tradeoffs are acceptable [179,205]. For end users, prior work has shown that cybersecurity practices compound the obstacles faced in other types of behavior change: they oblige people to interact with technology that they find scary, confusing or dull [32,97,151]; they afford abstract and non-absolute protections against specific threats [114,160,168]; and they provide solutions to collective problems that the potential adopter may not see as affecting them personally [168,186,206,222]. Fear appeals are important [22,133,169] but not sufficient to persuade people to adopt cybersecurity practices [211]; they also need awareness, motivation, and knowledge of how to use these practices to protect against threats, a framework known as security sensitivity [42,133,169]. Security sensitivity, in turn, has been shown to be informed by social influences, such as whether a trusted family member or authority figure gives advice about which security practices to use [164,165], whether people hear stories that teach them about security practices [161–163,202], or whether people observe trusted contacts such as friends engaging in secure behaviors [41,42,44].

My research to date has shown that, as with mask-wearing [111] or vaccinations [105], people's attitudes [70] and social contexts [150,186] factor into the extent to which they engage in protective behaviors for cybersecurity, such as checking that their antivirus software is up-to-date or keeping their network password confidential. I found that attitudes toward security practices are significantly associated with their experiences of security breaches, with their security behavior intention, and with their recalled security actions. I also found that, within the trusting norms of romantic relationships and workgroups, people are likely to share credentials for online accounts to maintain these relationships and to manage logistics and collaborations, despite designs or policies that discourage such sharing.

With my thesis, I extend this work to describe the social and cognitive factors that differentiate each stage of a cybersecurity adoption process. I started by drawing on components of existing behavior models such as Diffusion of Innovations. The most important of these components that have not already been mentioned above are the characteristics of the specific cybersecurity practices: whether they are mandatory or voluntary [2,132]; whether they are easy to use and/or useful [46]; and whether they are

easy to try out [168]. These characteristics associate with different attitudes and different social influences or social contexts at each stage of the behavior change process. My insights establish a basis for a stage model with benefits akin to the Capability Maturity Model for software engineering [223,237]. The resulting classification algorithm will help to assess the ability of groups to implement security practices. The associated diagram and description of the steps of security behavior adoption will help to define best practices for the targeting and timing of security interventions.

1.2 Thesis Statement

An empirical understanding of the cybersecurity adoption process will help us to specify the mental states and social influences acting at each step, leading to better targeting and timing of security interventions.

1.3 Summary of This Research

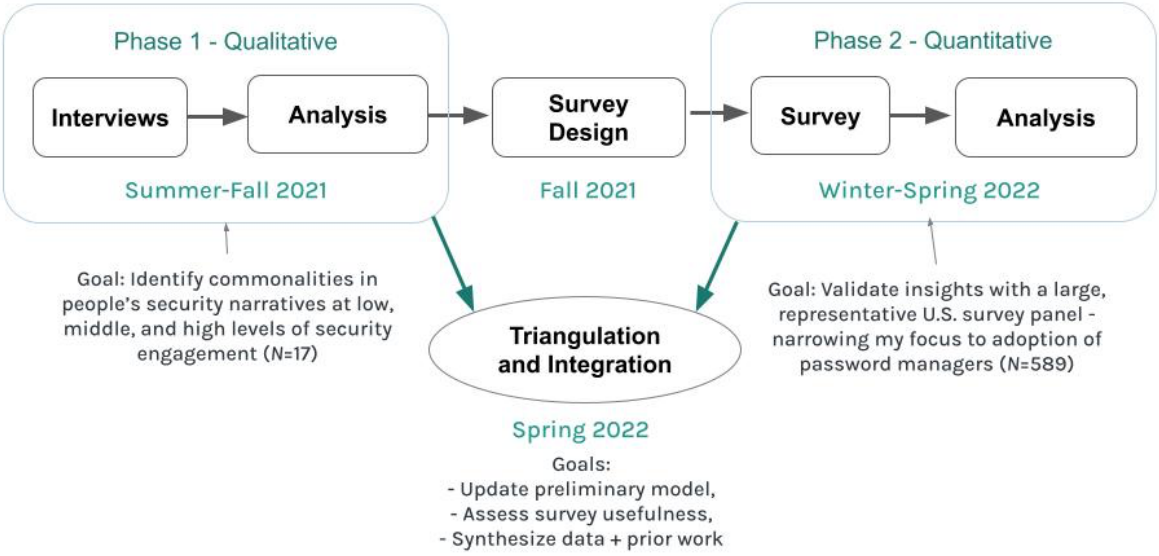

Figure 1: Overview of the research design, the timeline, and the goals for each phase.

To pursue my thesis research, I chose an exploratory, sequential mixed-methods approach in three phases (Figure 1). In Phase 1, I recruited and interviewed *N*=17 adult U.S. residents, locating them through a mix of posts on Craigslist, Facebook, and Google that advertised a pre-interview screening survey. Using this qualitative method, I gathered data about the commonalities in their spoken narratives of security adoption. I asked them, first, to tell me about a recent security concern and how they responded to it, and second, to tell me about their adoption or non-adoption of 1-2 other key practices, such as: using a password manager, using two-factor authentication, updating software, verifying the credibility of internet messages, and securing laptops and smartphones from prying eyes. I then formulated two follow-up research questions and three hypotheses for testing. In Phase 2, I contracted with Qualtrics to recruit a survey panel of *N*=859 adult U.S. internet users that matched U.S. Census parameters for age, gender, and income level. With the collected quantitative data, I used statistical analysis techniques to validate the insights from the Phase 1 study, answering the research questions and

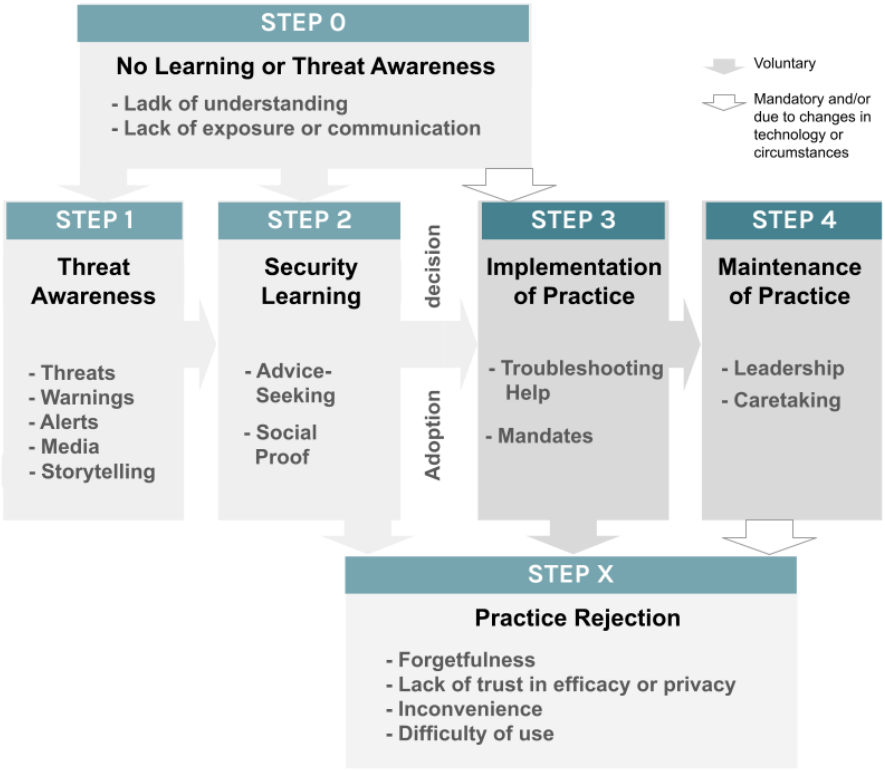

Figure 2: Summary diagram of the six steps of security behavior adoption, each step's associated social influences, and the path relationships among these steps, as informed by this thesis research.

testing the hypotheses. In Phase 3, I triangulated the data with the prior literature and integrated the data from each phase to produce a streamlined list of survey questions for others' use, a data-driven path diagram, and a results table.

What I learned, is, first, that people's adoption trajectory can be categorized in four steps, preceded, and sometimes followed, by two additional steps (Figure 2). These are: Step 0: No Learning or Threat Awareness, Step 1: Threat Awareness, Step 2: Security Learning, Step 3: Security Practice Implementation, Step 4: Security Practice Maintenance, and Step X: Security Practice Rejection. I identified specific social influences that are associated with each step of the adoption trajectory: for Step 1, communications (threats, warnings, alerts, media reports, and storytelling about threats); for Step 2, advice-seeking and social proof; for Step 3, troubleshooting help and mandates; and for Step 4, leadership and caretaking. Step 0 is associated with no person or source being available to help with security, and no authority mandating security awareness training. Step X is associated with receiving advice not to use a given security practice, lacking troubleshooting help, and lacking mandates.

Second, I devised and deployed a survey algorithm to classify any person into one and only one step of this security adoption model (Figure 3). This survey algorithm begins with one item asking people whether they have currently adopted the given security practice, then shows follow-up items to determine whether, if they have adopted, this was during the most recent six months, and if they have not adopted, whether they ever used the practice or why they never started. Participants who were classified into the successive steps also exhibited the expected rising pattern of scores on an existing and widely used

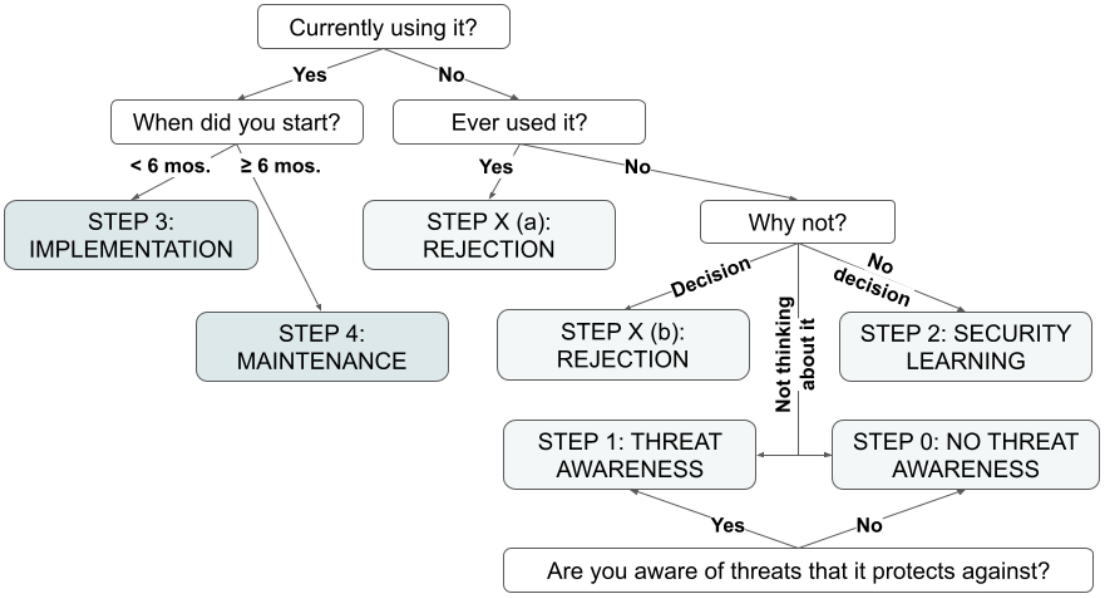

Figure 3: Diagram of the item tree for the step-classification algorithm, starting from (top left) asking about current adoption, then proceeding to narrow down adoption (left side) by timing and non-adoption (right side) by thinking.

classification scale, the University of Rhode Island Change Assessment (URICA), based on a similar stage model of behavior, the Transtheoretical Model.

Third, I identified and explained new step-specific recommendations for leveraging social influence and overcoming obstacles in the adoption process. These are summarized in Table 1. The recommendations derive from the Phase 1 qualitative findings, which can be found in Chapter 3, and from the Phase 2 quantitative findings, which can be found in Chapter 4. The main Phase 2 quantitative findings also are summarized in Table 2.

Table 1: Summary of step-specific descriptions, social influences, obstacle(s) to moving forward, and recommendations.

Step	Description	Social Influences	Obstacle(s)	Recommendation(s)
No Learning or Threat Awareness (Step 0)	- Lack of understanding about a recommended security practice or the importance of guarding against the specific threats it protects against. - *Examples:* No knowledge of where to go for advice, ignorance that software updates are for security.	- No person or source to help with security. - No authority mandating training.	- Cultural differences. - Fear of tech headaches. - Lack of interest.	- Use translators - Work with community groups and policymakers - Create sample instructional materials for classrooms
Threat Awareness (Step 1)	- Mention of threat, risk, harm, or potential harm; perception that event has implications for security. - *Examples:* Receiving a threatening email, reacting to media, suspecting your smartphone was hacked.	- Threats. - Warnings. - Media. - Storytelling.	- No awareness of a practice or other technology.	- Use translators - Work with community groups and policymakers - Create sample instructional materials for classrooms
Security Learning (Step 2)	- Knowledge of existence of a given security practice or other technology, but no action. - *Examples:* Hearing about secure messaging, finding out how to verify a post, being told to update.	- Advice-seeking. - Social proof.	- Not feeling threat (skipped Step 1). - Rejecting adoption before it is tried.	In line with prior work, ideate and test novel social interventions: - Build online crowdsourcing - Designate and train tech helpers
Security Practice Implemen-tation (Step 3)	- Acting to test the security practice to evaluate its usefulness; acting to put the decision into effect. - *Examples:* Using a trial offer, playing around with a practice; acquiescing to a policy.	- Trouble-shooting help. - Mandates.	- Discontinuing adoption after the practice has been used at least once.	Make use of opinion leaders who are in Step 4 for interventions aimed at Step 2 and Step X.
Security Practice Maintenance (Step 4)	- Acting to finalize the decision to use a practice; expanding use; mention of past implementation. - *Examples:* Stepping up frequency of use; making statements like "I still use this" or "I currently use it."	- Leadership. - Caretaking.	- The context becomes obsolete. - Waning effectiveness.	Troubleshooting help should go together with improving usability so that those who try out security practices will not reject them.
Security Practice Rejection (Step X)	- Either discontinuing adoption of a security practice or deciding not to implement the security practice. - *Examples:* Stopping after a few uses; making statements like "It felt like overkill" or "Effort is too much for the benefit."	- Advice not to use it. - Lack of help with troubleshooting. - Lack of mandates.	- Forgetfulness. - Lack of trust in efficacy or data privacy. - Inconvenience - Difficulty of use.	Soften the stances of those in Step X with transparency, increased usability, and on-demand support.

Table 2: A recap of the significant findings from Phase 2, with their category, sub-section, and page(s).

Category	Summary of Phase 2 quantitative findings	Sub-section	Page(s)
RQs and Hypotheses from Phase 1	The step-classification algorithm demonstrates reliability and convergent validity.	5.2.2.1	64-65
	H1-2 retained: Authority influences and peers/media influences will significantly associate with evidence of an adoption decision.	5.2.2.3	66-67
	H2(a)-2 partly retained: Trialability will be positively associated with adoption of a tool-based security practice.	5.2.2.4	67
	H2(b)-2 retained: Troubleshooting help will be positively associated with adoption of a tool-based security practice.	5.2.2.5	67-68
Reasons Given for Non-Adoption	Lack of understanding, of mandatoriness, and of awareness of password managers were associated with Step 0.	5.2.3.1	70-71
	Lack of understanding and of awareness of password managers were associated with Step 1.	5.2.3.1	71-72
	Lack of understanding and of mandatoriness were associated with Step 2.	5.2.3.1	72-73
	Lack of mandatoriness, of a pleasing and trouble-free user experience, and of trust in password managers were associated with Step X.	5.2.3.1	73-74
Reasons Given for Adoption	Convenience, troubleshooting help and mandatoriness were associated with Step 3.	5.2.3.2	75-76
	Convenience and mandatoriness were associated with initial adoption for Step 4.	5.2.3.2	77-78
	Convenience and usefulness were associated with continued adoption for Step 4.	5.2.3.2	78-79
Social Factors	Those in Step 3 and Step 4 scored significantly higher on the Adoption Leader scale.	5.2.3.3	80-81
	Those in Step 4 scored significantly higher on the Educating Others scale.	5.2.3.3	81-82
	Those in Step 3 rated password managers significantly higher on the Image scale than those in Step X, Step 2, or Step 0.	5.2.3.3	82-83
	Those in Step 3 or Step 4 rated password managers significantly higher on the Visibility/Trialability scale than those in any non-adoption step (0, 1, 2, and X).	5.2.3.3	83-84
	No association existed between a participant's individual frequency of experiencing security breaches and their likelihood of being in adoption (Step 3 or Step 4).	5.2.3.3	84-86
	Those with frequent social exposure to breaches (through a close tie or media/peers) were significantly more likely to be in Step 3 or Step 4 than in a pre-decision step (0, 1, or 2).	5.2.3.3	84-86
Individual Factors	Those with a high score on Internet Know-How were significantly more likely to be aware of password managers (Steps 2, X, 3, or 4).	5.2.3.4	86-87
	Those under 40 were significantly more likely to be in Step 3 or Step 4.	5.2.3.4	87
	Those without any experienced with computer science, information science, or sensitive data were significantly less likely to be in Step 3 or Step 4.	5.2.3.4	87-88
	Those who identified as non-White and/or non-Caucasian were significantly more likely to be in Step 0 and significantly less likely to be in Step 3.	5.2.3.4	88-89

To recap, my contributions are as follows:

- An example of an exploratory, sequential mixed-methods approach to identify commonalities in people's spoken narratives of security adoption (*N*=17) and validate insights with an online, U.S. Census- representative survey panel (*N*=859).
- A synthesized model of security practice adoption that accounts for social influences by step.
- A method for assessing which step someone is in.
- New step-specific recommendations for leveraging social influence and overcoming obstacles in the adoption process.

1.4 Definitions

Communication

The act of one person conveying or stimulating meaning in the minds of another person or persons through the use of mutually understood signs and semiotic rules [217].

Diffusion

The process by which an innovation is passively communicated to members of a social system over time [168].

Dissemination

The process by which the diffusion process is deliberately and actively facilitated [168].

Innovation

Any technology, program, or policy that is new to its potential users [168].

Mental States

Aspects of a person's mind such as cognitions, appraisals, dispositions, impulses, and feelings [92,104,130].

Process

A series of actions or steps taken in order to achieve a particular end [238].

Security

A collection of practices, policies, and properties (such as confidentiality, integrity, and availability) that ensure a computational device and/or network will be dependable and free of exploitation (such as harm, theft, or unauthorized malicious use) [36,60,84,102]. Used interchangeably here with "cybersecurity," "online security," "computer security," and "device security."

Security Practice

Any method of either dealing with ("treating" or addressing) or preventing a security concern, whether cyber/virtual or physical [222].

Social Influences

Efforts to change another person's beliefs, attitudes, or behaviors via conformity, sales, socialization, leadership, peer pressure, persuasion, and/or marketing [28,29,225].

Usable Security

An approach and methodology for understanding security from an end-user's perspective that ensures they are 1) reliably aware of the needed security tasks, 2) able to figure out how to successfully perform these tasks, 3) able to avoid dangerous errors in the performance of these tasks, and 4) sufficiently comfortable to use and be happy with the interface for the security task [54,213].

2. INFLUENCES ON SECURITY AWARENESS AND ADOPTION

In this chapter, I will, first, summarize some relevant prior work describing the domain of end-user cybersecurity (Section 2.1). I will detail obstacles to security adoption for users-in-the-loop (2.1.1); known social influences on security awareness and adoption (2.1.2); and what is already known about the process of struggling with security practices (2.1.3). Second, I will describe my completed empirical research to understand the security adoption process (Section 2.2), in the areas of account sharing (2.2.1) and security attitude measurement (2.2.2). Third, I will describe existing theoretical behavior models that are useful to security (Section 2.3). I will delve into three expectancy-value models (2.3.1 – the Theory of Reasoned Action/Theory of Planned Behavior, Protection Motivation Theory, and the Technology Acceptance Model) and two stage models (2.3.2 – the Transtheoretical Model of Behavior Change and the Diffusion of Innovations Adoption Process model) that I draw on in this thesis. I conclude with my guiding research question (Section 2.4).

2.1 Background on End-User Cybersecurity

People's lived experiences of cybersecurity tend to fall into what Ackerman termed the socio-technical gap, where our technical systems as realized do not fully support users' social needs [1,218]. Using research findings and methods from psychology, behavioral economics, ethnography, design, marketing, and communication can help us to understand these needs.

When it is not possible to remove humans from the security loop entirely, security designers must either create intuitive systems that are easy to use, or teach people to perform tasks that are security-critical [35]. Many good security practices now exist for the humans-in-the-loop to help safeguard their networks and their online data and accounts. These practices can be grouped in four categories: using good password practices, securing hardware and devices from potential attackers, keeping systems and software up-to-date, and staying alert for phishing, scams, and misinformation [62]. However, people have been slow to become fully aware of what security practices do and to voluntarily use them regularly, such as in the instances of password managers or Virtual Private Networks [151,188]. In 2021, years of low voluntary adoption of two-factor authentication [239] led Google to auto-enroll 150 million accounts in the security feature and to require 2 million YouTube creators to turn it on [30,232].

Egelman and Peer [63,64] noted that the "myth of the average user" is a problem in user-centered design approaches. They argued for designing systems to account for individual differences in decision-making and risk-taking [64] and in security behavior intentions [61,62]. Similarly, Wash and Rader [204] found that differences in security knowledge and strength of beliefs led to differences in home computer users taking protective actions, recommending that not all users receive more of or the same security information. Schneier [179] notes the difference between the actual security of a system and a person's perception of security as a tension, as the former can be assessed mathematically but the latter is a qualitative construct. He notes five areas where a gap occurs: risk severity, risk probability, risk magnitude, mitigation effectiveness, and the acceptability of the security tradeoff. Inside organizations, cybersecurity involves a large and diverse number of stakeholders, and involves metrics, individual differences, technological inputs, team processes, and team-level situations, all of which complicate the efforts to address individual and group differences [39].

A related issue is that of insider threat, in which system users misuse their privileges in a way that exposes the network to cyberattack [227,228]. Salem et al. [174] defined such threats as malicious and of

two types, traitors (legitimate users inside the system who act contrary to security policy and mean to do harm) and masqueraders (outsiders who impersonate or steal the credentials of legitimate users, in order to do harm). However, Greitzer et al. [89] noted the existence of a third and non-malicious type, the unintentional insider threat (UIT) that occurs when legitimate users "accidentally jeopardize security through data leaks or similar errors." This thesis is primarily concerned with preventing UIT.

2.1.1 Obstacles to Security Adoption for Users-in-the-Loop

Prior work has found negative attitudes toward security practices to be widespread. Participants in one 2018 U.S. study described cybersecurity as "scary," "confusing," and "dull" [70]. Some think the use of extra cybersecurity measures (such as encryption) is "paranoia" [42,85]. Users may feel that they only visit "trusted" websites that won't lead to a data breach, or that they are not rich or important enough to attract a hacker's attention [202]. Further, the rigidity of security requirements can lead users to feel "ambushed" such as when being forced to deal with password policies at login [177]. Engagement with security practices is associated with negative experiences, such as security breaches [70] or hearing stories of others' problems [163,203].

While fear appeals are important [22,133,169], they are not sufficient to spark adoption [211]. People need awareness, motivation, and knowledge of how to use these practices to protect against threats, a framework known as "security sensitivity" [42,133,169]. Many Americans lack adequate awareness and knowledge of good cybersecurity practices [149,199]. For example, a 2019 study found that just 28% of adults can identify an example of two-factor authentication [199]. Two studies of self-reported security behaviors by experts vs. non-experts, published four years apart [25,109], found that Western non-experts consistently failed to name the experts' top three recommendations: regularly installing updates, using a password manager, and enabling two-factor authentication.

People weigh the real or perceived costs of security practices against the potential benefits of their use, a calculation that may not favor adoption, particularly when media coverage makes it clear that it is impossible to be 100% safe [170]. Security practices afford abstract and non-absolute protections against specific threats [114,160,168]; and they provide solutions to collective problems that the potential adopter may not see as affecting them personally [168,186,206,222]. A 2020 paper [222] reported that security, privacy, and identity theft protection practices were commonly partially adopted or abandoned because users found them inconvenient, unusable, or unnecessary due to low perceived risk. Previous work found that the balance of security and convenience was central to the decision-making process, and that the relative weight of different risk and practicality benefits and costs differed from user to user [67,135,151]. Rader et al. found that people gather more accurate information when they seek advice, but that they often do not put together advice from multiple sources in a way that helps them accurately judge the most persistent and frequent threats, such as phishing, vs. the less frequent but more sensational, such as hackers [161]. Fagan and Khan [67] found low social motivations for security awareness and adoption vs. individual, instrumental motivations. Redmiles et al. [165,166] also found a knowledge gap specifically for computer users with low socioeconomic status that impacted how well they could deal with security concerns.

The relationship between other socio-demographic characteristics and security and privacy behaviors is not consistent across studies, suggesting that other factors are confounding the associations. One study shows that a user's affinity for masculine vs. feminine characteristics is a better predictor than binary gender of their security behaviors [108], along with knowledge, motivation, confidence, and risk propensity. Another focused on users of online services with low socio-economic status, and found they

exhibited resignation, fear, and low perceived efficacy in dealing with security and privacy concerns [198]. An earlier telephone survey [166], however, concluded that access to different advice sources, not socioeconomic status per se, was the key factor associated with their security and privacy incidents. A fourth found that younger study participants tend to believe privacy threats affected others more than themselves, but that this was due more to their over-estimating the risks to groups of other people in society rather than under-estimating the risks to themselves [10].

2.1.2 Social Influences on Security Awareness and Adoption

Prior work has shown that social influences have an impact on security awareness and adoption at four scales: intimate, personal, social, and public [218]. Examples at smaller scales include whether a trusted family member or authority figure gives advice about which security practices to use [161,164,165], whether people hear stories that teach them about security practices [161–163,202], or whether they observe others engaging in secure behaviors [41,42,44]. Peers tend to share information about who conducts attacks, while experts focus on how attacks are conducted and news articles focus on the consequences of attacks; this fractured advice may prevent users from forming a consistent mental model for making security decisions [162]. People who consider themselves knowledgeable about security report feeling an accountability and obligation to protect friends and loved ones [41,42]. And, having access to informal tech helpers [125,145,155] or security advocates [96,97] helps nonexperts to engage in secure behaviors -- though relying on others [145] also can preclude people from overcoming their fears and confusion about security. Trust relationships and proximity are associated with sharing behaviors, such as household members sharing devices [135] and romantic couples [129,150] and coworkers [186,211] sharing accounts. Social proof, in which people look to others for signifiers of correct behaviors [28], is a social influence on security awareness and adoption [41,42] that can operate at a larger scale [45,218]. A pair of studies found that social influence in Facebook friend networks affected users' likelihood to adopt a security feature, varying by the attributes of the feature (observability) and how the feature has already diffused through the network [43,44].

Another form of social influence that can operate at different scales is authority [28,29]. Depending on the context for security, it is possible to distinguish between authority that is based on expertise ("authoritativeness") versus authority derived from relative position in a hierarchy [29]. For example, in a 2016 interview study on advice sources for digital security [164], participants considered friends and family authoritative when they were seen as "tech-savvy," and some media outlets as authoritative if they were technology-oriented or written by "computer people." People with this perceived authoritativeness fill the role of "tech manager" [145], "tech caregiver" [125] or "helper" [155] for friends, family and coworkers, at times inconsistently with traditional power dynamics [125,145,155]. Authority derived from a hierarchy, by contrast, can cue or force action (such as with mandates) and can be seen as impersonal [29]. Its effectiveness in teaching people what to do and in nudging compliance can vary depending on the type of security practice, individual characteristics, and advice form [164]. Two studies of password sharing in the workplace found that employees would ignore official policies that passwords must be kept confidential when they conflicted with productivity or social needs [186,211].

2.1.3 The Process of Struggling with Security Practices

Software updates are a security practice that almost all experts recommend for safeguarding security [25,109], but which many computer users are either not aware of or actively struggle with [193].

Vaniea and Rashidi [194] surveyed 307 Mturk workers about memorable software updates and used content analysis to discover the stages of the software-update process and what obstacles participants faced. They found the process stages to be: 1) awareness (usually through a notification), 2) deciding to update, 3) preparation, 4) installation, 5) troubleshooting, and 6) post state. Some described reaching out to social contacts for advice when unclear whether the update was trustworthy. Others described hearing about needed updates through the news. Some monitored reviews to help them decide whether the update would benefit or hurt their tech setups; others recalled word of mouth reaching them in other ways about potential problems. Troubleshooting was mentioned at almost every step, but most commonly when the update failed during installation, or when the updated software exhibited problems. At least one participant sought professional help, but most participants were technically skilled and said they often receive rather than seek requests for assistance.

Prior work has found security on home computer networks to be a pain point for users who are not technically skilled [18,91,107,155,202]. Poole et al. [155] focused on informal technical support for these computer networks. They found that people seeking help had a long-term relationship with a single helper within their social networks who they turn to when they don't know how to find professional help or when access to professionals is limited due to policy or cost. The informal helpers scale their availability based on many factors, including the time they have available, the urgency of the seeker's needs, and the degree to which they will benefit (such as learning something new or increasing their respect and self-image).

2.2 Completed Research to Understand the Security Adoption Process

In my completed research, I and my collaborators have found that, just as with mask-wearing and vaccinations, people's attitudes and social contexts factor into their adoption of cyber-protective behaviors (such as checking for antivirus updates and keeping passwords confidential).

2.2.1 Account Sharing

Account sharing is defined as multiple individuals accessing a single account with the same login and password. In these situations, people make an individual or collective choice not to keep their account passwords or other authentication codes confidential. Most system administrators and platform terms of service forbid or discourage such sharing, as it contravenes the "1 user - 1 account" design for most authentication schemes. Nevertheless, account sharing has been documented in several studies of usable security [16,116,120,150,186]. It exemplifies Ackerman's socio-technical gap [1], in that the technical functioning of the system as designed does not support the social needs of the system's users. It also can be considered an example of what Rogers termed re-invention [168] (the degree to which an innovation is changed by the adopter after its original development), because users are modifying the original "1 user - 1 account" design as part of the process of implementing the innovation and sustaining its continued use after the time when it was introduced.

My first study of account sharing, Park et al. 2018 [150], established that relationship formation and household formation are cues for romantic couples to start influencing each other's security practices, as shown by their sharing of entertainment and financial accounts, respectively. We documented the novel finding of *relationship maintenance* as a motivator for account sharing among romantic couples, along with *household maintenance* [135], *trust* [184], and *convenience* [184], in a thematic analysis of N=174 open-ended survey responses from workers on Amazon Mechanical Turk (Mturk). By integrating these

responses with statistical analyses of several variables' impact on the ratio of shared and owned accounts, we found that the "1 user - 1 account" design default for authentication schemes poses usability challenges for romantic couples across the life cycle of their relationships. People in new relationships (defined as less than seven months' duration) would demonstrate affection and support by sharing the password to their individually owned Netflix account, for example, before the video service made it easier to add multiple users on a single account. More-established couples (defined as seven months' duration or more) shared more jointly owned accounts than did newer couples, particularly once they began to co-habitate. They found it difficult to navigate the security setups when apart, such as when the two-factor authentication code would appear on one partner's phone at work but the other partner at home was trying to access the account. Some partners reported hiding accounts, either for maintaining other relationships or their individual privacy, or for gifts. Finally, during a breakup or domestic dispute, the other partner often was considered an "insider threat" [80,146] to personal data being held in shared accounts, and participants reported difficulties in making sure that they had removed the ex-partner from shared access and in keeping track of whether their accounts were being accessed without their permission.

My second and third studies of account sharing, reported in Song et al. 2019 [186], established that, among co-workers, social and logistical needs influenced their security practices to the extent that account sharing was considered "normal and easy" – though still challenging -- in a workplace context. In the second study, we found in an analysis of N = 98 survey responses from Mturk workers that they shared accounts with coworkers for four reasons: centralizing collaboration, boundary management, saving money, and demonstrating trust. Further, these workers found account sharing challenging due to a lack of individual accountability for account activity, conflicts over when co-workers would access the shared accounts, difficulties with controlling boundaries, and difficulties in managing passwords. The challenges were magnified by employee turnover -- for example, a former employee being listed as the primary owner of a shared account and not being able to change that, or a disgruntled ex-employee posting to company accounts for social media. In the third study, which collected N=288 survey responses from workers on Mturk and Prolific, participants reported sharing around 11 accounts on average with co-workers, with 52% sharing 10 or more. The top three accounts shared were Facebook, company domain email, and Google Drive. Workers in this study also reported that centralizing collaboration (42%) was a primary reason for sharing accounts, followed by smoothing boundary management (29%), saving money on resources (18%), and demonstrating trust and connection (8%).

My fourth study of account sharing, Wang, Faklaris et al. 2022 [201], found evidence that an educational and/or research context influences lax and/or disorganized security practices among students and other non-IT employees. In a thema/tic analysis of N=23 interviews with employees of a U.S. research university, we found that IT employees reported using the most systematic and least problematic practices for account sharing with coworkers, such as using an Enterprise Random Password Manager (ERPM). The reported use of the ERPM was described by IT employees in context as mandatory. Among non-IT employees, students' account sharing practices were more systematic than those of the full-time employees interviewed, but remained somewhat problematic, such as storing passwords in plain text files inside email or messaging apps. The reported use of account sharing practices by non-IT employees was described in context as voluntary, and none described using a third-party password manager such as Last Pass or 1Password. Further, many non-IT employees saw account sharing as low risk and securing accounts as secondary to other priorities. Similar to prior work on workplace account sharing [16,116,120,211], we found this was due, in part, to their focus on the personal impacts over impacts to others of a security breach and to not perceiving non-financial data as of interest to attackers, along with

their trust in their colleagues not being a security threat. However, we found evidence that two unique characteristics of this research university influenced security practices: *paternalistic norms of education*, as shown by their stated trust in the campus authorities (IT and/or "the system") to keep their data and accounts safe; and the overall culture of *academic freedom*, which implies no limits on tech use to teach, to learn, to publish, or to inquire, with a corresponding lack of top-down security mandates.

In summary, the above studies provide evidence that social contexts are influences on people's security practices. The first study, Park et al. 2018, indicates that people's reported account sharing evolves over time as their romantic relationship progresses through its life cycle. The second and third studies from Song et al. 2019 hint at account sharing's evolution in tandem with work relationships: it becomes more imperative as tasks become more collaborative, but more challenging with an increase in employee turnover and termination of sharers' jobs. The fourth, Wang et al. 2021, introduces the idea that whether security practices are *mandatory* (in this case, for the IT staff who use an ERPM) or *voluntary* (in this case, for non-IT staff who devise ad-hoc password-sharing practices in the absence of top-down security mandates) will affect the degree to which coworkers are engaged with and attentive to security practices. However, more research is needed to specify the stages of the security adoption process, whether these stages differ depending on whether the practices are mandatory or voluntary, and how social influences act at each step.

2.2.2 Security Attitudes

While social contexts are important influences on people's cyber-protective behaviors, so are their attitudes. *Attitudes* represent people's evaluation of objects, groups, events, that is, how they orient to the world around them [3]. An extensive body of research in psychology examines attitudes, their antecedents and consequences, and their relationship to intentions and behavior [3,4,40,122]. In fields as different as organizational psychology [152] and environmental sustainability [11,94], researchers measure attitudes to understand behavior and general tendencies. A measure (or several measures) of security attitudes allows researchers to examine what leads to different security attitudes, and the effect of these attitudes on intentions and on behavior.

We have created several quantitative measures of security attitude and examined their statistical relationships with other variables of interest to usable security researchers, such as the Security Behavior Intentions Scale, or SeBIS [62]. The most widely known of our security attitude measures is SA-6, for six-item security attitude measure, as reported in Faklaris et al. 2019 [70]. Building on the work of Das and others [41,42,44] in determining positive mental states for security adoption, the SA-6 scale measures a person's general engagement with and attentiveness to security practices. A person's SA-6 score is computed as the average of their ratings of agreement or disagreement (1=Strongly Disagree to 5=Strongly Agree) with statements such as "I often am interested in articles about security threats" and "I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe." We employed an iterative process to create SA-6, the final phases using survey samples from Mturk (N=478) and a U.S. Census-weighted panel from Qualtrics (N=209). The resulting scale displayed desirable psychometric properties, such as goodness-of-fit, internal consistency, and expected associations and variances with previously validated constructs (such as privacy concerns) and participant sociographics (such as age and gender). To allow us to assess SA-6's predictive validity, we adapted the wordings of 10 SeBIS items regarding intention to engage in specific security practices (such as checking that antivirus software is up-to-date) to measure whether a participant in fact recalled engaging in that security practice in the past week. We labeled this 10-item measure the Recalled Security Actions (RSec)

inventory. Both SeBIS and RSec ask about specific actions in four areas: keeping systems up-to-date; maintaining good password hygiene; watching out for scams and misinformation; and securing devices and networks.

For my 2019 study [70], using the Qualtrics (N=209) dataset, we found that security attitude, as measured by SA-6, was significantly positively associated with security behavior intention and with recalled security behaviors – a relationship that is consistent with the Theory of Reasoned Action and Theory of Planned Behavior [2,132]. We found that SA-6 significantly explained 28% of the variance in security behavior intention ($p<.01$), as measured by SeBIS; and that it significantly explained 15.8% of the variance in security actions recalled being performed in the past week ($p<.01$), as measured by RSec. Further, we found that SA-6 scores were significantly higher (indicating more attentiveness and engagement in security practices) among those who reported that they or their close ties had frequently experienced security breaches, and among those who reported hearing or seeing a great deal about security breaches in the past year. These findings are evidence of social influences' associations with security attitude. Finally, we found that SA-6 scores were significantly positively correlated with measures of internet know-how, computer confidence, and web-oriented digital literacy. This suggests that someone's awareness, motivation, and knowledge of how to use security practices will rise or fall with their awareness, motivation, and knowledge of how to use computational devices and internet-connected applications.

However, one drawback of SA-6 is that it fails to capture other, less positive mental states that we know are factors in decisions to adopt either a modified security practice (such as account sharing) or a more stringent practice (such as passwords that are confidential, long, complex, and unique). For example, some users of computing devices have remarked that the use of extra cybersecurity measures such as encryption is evidence of "paranoia" [42,85]. Users may feel that they only visit "trusted" websites that won't lead to a data breach, or that they are not rich or important enough to attract a hacker's attention [202]. Further, the rigidity of security requirements can lead users to feel "ambushed" at inopportune times by a security feature demanding new input, such as being required to deal with password policies at login [177]. Most people also see complying with cybersecurity as a secondary goal at best in their use of computing devices, as we saw in Wang et al. 2021. This adds incentives to ignore security advice or cut corners with requirements [177] to avoid the perceived costs of compliance (the "level of effort or financial cost associated with incorporating a protective measure") [86]. At the same time, many users express concern about their threat exposure due to what they hear and see highlighted in media sources [41], and they tend to conflate security and privacy concerns, which can mislead them about which tools are effective [188]. Expanding SA-6 to incorporate items to measure mental states such as these can help us determine the degree to which a person might need extra persuasion to try out a new security practice, or their likelihood of abandoning a new security practice when they encounter even a minor difficulty with it.

To this end, in Faklaris et al. 2021 [71], we reanalyzed the N=209 dataset from Faklaris et al. 2019 to create a 13-item, four-factor measure of security attitude that we call SA-13. We added seven items to SA-6 that measure *resistance* to security practices (such as "I usually will not use security measures if they are inconvenient") and *concernedness to improve* security practices (such as "I want to change my security behaviors to keep my online data and accounts safe"). SA-13 exhibited significant associations and variances with many of the same other variables as did SA-6. However, SA-13 was found to be significantly associated with several measures for which SA-6 did not: General Decision-Making Styles subscales for avoidance ($r=.249$, $p<.01$) and dependence ($r=.265$, $p<.01$); the DoSpeRT

Health/Safety measure of risk-taking propensity (r=.230, p<.01); and the Consideration of Future Consequences scale (r=-.148, p<.05). These differences may indicate that SA-13 is more suited than SA-6 to use in populations with dependence, avoidance, or risk-taking propensities – all of whom seem likely to exhibit degrees of security noncompliance.

Further, three of the four factors of SA-13 demonstrated desirable psychometric properties as standalone scales: SA-Engagement (the three items from SA-6 that measure active engagement with security practices), SA-Attentiveness (the three items from SA-6 that measure awareness, motivation and knowledge of how to use security practices, or "security sensitivity" [42,44]), and SA-Resistance (the four items that express resistance of various types to security practices). The SA-Engagement subscale significantly explained the most variance in the RSec variable (12.9%, p<.001), while the SA-Attentiveness subscale significantly explained the most variance in the SeBIS variable (25.9%, p<.001). These findings seem consistent with the idea that attitudes toward a target set of behaviors will change as someone progresses to intention and then to action. As for the SA-Resistance subscale, it exhibited several statistically significant relationships that are different from the other measures. We found significant negative associations for SA-Resistance with Internet Know-How (r=-.169, p<.05) and with GDMS-Avoidance (r=-.485, p<.01), the Barratt Impulsiveness Scale (r=-.438, p<.01), DoSpeRT Health/Safety Risk-Taking Propensity (r=-.302, p<.01), and GDMS-Dependence (r=-.198, p<.01). We also found that SA-Resistance dropped, rather than rose, with an increase in personal experiences with security breaches in the past year (low M=3.48, SD=.91 vs. high M=2.78, SD=.90): t(207)=-5.15, p<.001; and with an increase in a close tie experiencing a security breach (low M=3.43, SD=.91 vs. high M=2.97, SD=.97): t(207)=-3.42, p<.005. These results are evidence that the SA-Resistance scale may be particularly suited to use in populations that are averse to individual risks, but also have not learned enough to adequately perceive network or collective risks.

In summary, the above studies document that significant relationships exist among security attitudes, security behavior intentions, and recalled security actions, as predicted by prior descriptive models of behavior. The development of SA-13 and its subscales suggests that different factors of security attitudes might be more strongly associated with different stages of security behavior adoption, with attentiveness being more strongly associated with security behavior intention, while engagement being more strongly associated with security behaviors in the recent past. The results for SA-Resistance, moreover, suggest that several traits or cognitive styles cause them to focus on and overweight the costs of security compliance, without this thinking being balanced by either abstract know-how of internet threats and security practices, or concrete knowledge gained through experiences of security breaches by them or their close ties. However, more research is needed to determine which aspects of security attitude are acting at each stage of the security adoption process; and, to what extent resistance affects progression through the stages.

2.3 Existing Theoretical Behavior Models That Are Useful to Security

A model is a simplified map of a topic space. In design, they are used to describe the current state of the world (what "is") and to help guide the creation of a preferred future state (what "could be") [57,58,65]. In statistics, they are used more narrowly, to encode a set of assumptions about the sample data and to make predictions about the real world [101]. And relatedly, in the social sciences, models are used to set out theoretical variables, describe their relationships, and document assumptions; once developed, these models are used to specify and to test hypotheses [38,139].

Interventions to change behaviors are more successful when grounded in appropriate theory [33,49,82,87,88,121]. Several prior models of behavior adoption have been published in the social sciences that offer insights on decision-making for usable security and can help explain and predict security adoption. I group these into *expectancy-value models* and *stage models* [68].

Expectancy-value models generally follow Vroom's theory that people act as a result of *expectancy* (how likely they perceive that a desired, *instrumental* outcome will occur) and *value* (how much they perceive that outcome to have importance or utility) [189,192,200]. However, these models often differ by the implicit or explicit assumptions of the degree to which people engage in conscious, rational, "System 2" thinking versus unconscious and possibly irrational "System 1" thinking [26,59,113,118]. For instance, the *Fogg Behavioral Model* [75–79] conceptualizes behavior as the result of three elements converging in the same moment -- motivation, ability, and a prompt – with a convex function (the "action line") representing the change in the probability of a prompt's success from changes in motivation and ability. (A similar model in health care is the *Capability-Opportunity-Motivation Behavior (COM-B)* model [142,143].) In contrast, *Decisional Balance Theory* [34,112] and related theories posit that people weigh the pros and cons of a decision, with action taking place once possible benefits and self- and social-approval from the action outweigh the likely costs or self- or social-disapproval that might result. And *Prospect Theory* [114,160] argues that people think about gains differently than they do losses, because they are *more averse to losses* than they are attracted to gains. A relevant corollary for cybersecurity is that people cognitively *over-weight events with low probabilities* (treating a 1% chance as if it were 5%) and *under-weight events with high probabilities* (treating a 99% chance as if it were 95%).

Stage models of behavior change differ from expectancy-value models in that they account for the progress of time, roughly following the *Lewin Change Model* of "unfreeze," "move," and "refreeze" [24,88]. While the process they describe is continuous, the segmentation of the process into stages helps in describing people's journey through the process and of distinguishing the characteristics of one point in time from another. One example is the *Precaution Adoption Process Model* [208,210], which breaks down inaction into four stages (unaware, unengaged, undecided, and decided not to act) and action into three stages (decided to act, action, and maintenance). Another is the *Concerns-Based Adoption Model* [9,93], which conceptualizes feelings or emotions about change within educational institutions as Stages of Concern (awareness, informational, personal, management, institutional); Levels of Use (orientation, preparation, mechanical, routinization/refinement, integration, and renewal), and Innovation Configurations (checklists of techniques and variations used).

Below, I describe several models and the relevant components that will inform my research. I selected these based on how well they seem to correspond to results in my prior work in usable security (such as the SA-6 security attitude scale or account sharing among close ties) and those of researchers pursuing similar lines of inquiry (such as behavior change for increasing physical or mental wellness).

2.3.1 Expectancy-Value Models

The *Theory of Reasoned Action/Theory of Planned Behavior* [2,74,132] (Figure 4) falls near the System 2 end of the EVM spectrum. It presents *attitudes*, *norms* and (in the TPB) *perceived behavioral control* as key antecedents of intention and action, along with background factors and beliefs. Intention's influence on action is moderated by both perceived behavioral control and by actual control over behavior. An advantage of this model is that it explicitly acknowledges social and environmental factors as influences on behavior, akin to *Social Cognitive Theory* [13], through perceived norm, perceived

behavioral control, and actual control. One limitation is that neither perceived risks nor perceived tradeoffs are noted as antecedents of behavior. For cybersecurity, these are important parts of threat modeling [22,133,169,211].

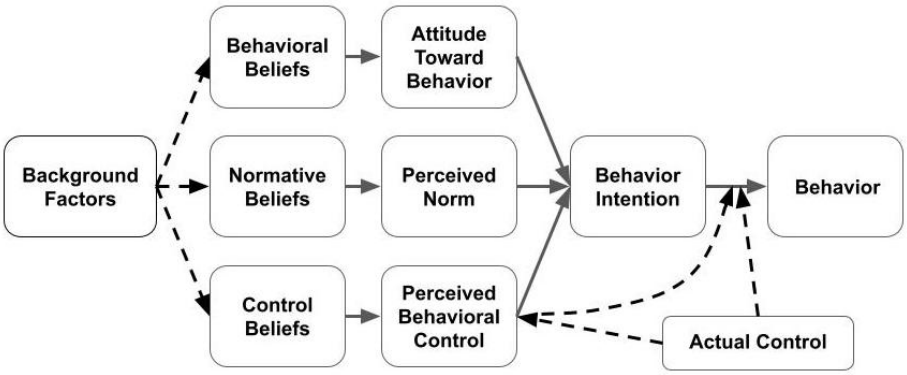

Figure 4: Causal diagram for the Theory of Planned Behavior. Background factors are antecedents of all components except for actual control. The latter is comprised of skills, abilities, and environmental factors.

In cybersecurity, the TRA and TPB have been used to guide research into security attitudes [70,71], security behavior intentions [61,62], and hospital employees clicking on phishing links [110]. However, this reasoned-action approach does not directly account for awareness, a factor that is known to drive security compliance [7]. Dinev et al. have proposed incorporating technology awareness in the TPB as a predictor of behavioral intentions [55]. Regarding privacy behaviors, Mendel and Toch [138] found in a study of 167 Mturk workers that attitudes were an important overall factor in participants' self-reported willingness to follow Facebook privacy advice. Users with high perceived behavioral control were more susceptible to peer influence and were more willing to promote their behaviors to others.

Protection Motivation Theory [133,169] (Figure 5) is another System 2 EV model. It argues that, in the presence of a threat, *threat appraisal* and *coping appraisal* will lead to protection motivation. Threat appraisal is measured as the combination of perceived severity and vulnerability, minus any rewards from starting or continuing behaviors that contribute to the threat. Coping appraisal is measured as the combination of perceived response efficacy and self-efficacy, minus any physical or psychological costs from enacting the response. These calculations hearken back to Decisional Balance Theory, in that they involve weighing the pros and cons of enduring a threat and of responding to that threat. However, the PMT does not address motivation's path to action, nor the influence of cues to action on action. PMT also does not explicitly address social and environmental factors, in contrast with the TRA and TPB. Finally, PMT does not account for unconscious, System 1 reactions that involve no conscious thought.

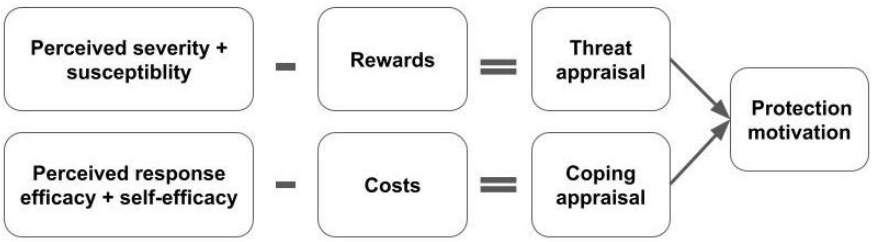

Figure 5: Illustration of Protection Motivation Theory. Threat appraisal and coping appraisal are the key antecedents of protection motivation; each is the result of a calculation of pros and cons.

PMT has been used widely in cybersecurity [214], suggesting interventions in the form of fear appeals such as messaging about potential threats [22] and their potential severity [214]. But, Menard et al. noted that applying PMT has not always resulted in individuals performing a behavior to safeguard information [137]. Their 2017 study found that individuals were more likely to form intentions to adopt security measures if they felt competent, had an emotional connection with their data, and were otherwise motivated to perform the correct response. In addition. Hanus et al. [99] and Alsaleh et al. [8] found that security awareness was an antecedent of protection motivation for desktop security and smartphone security, respectively. Van Schaik et al. [178] found that people use an affect heuristic to help them judge cybersecurity risks and that this influences their protection motivation.

The *Technology Acceptance Model* [46,47,197] (Figure 6) is a mix of System 1 and System 2 and assumes technology awareness. It adapts the reasoned-action approach to behaviors in information systems [48], proposing that *external factors* (such as gender, age, and skills) and *cognitive/affective factors* that I term "technology appraisal" (perceived ease of use, perceived usefulness, and user attitudes) lead to usage intention and to actual usage. An advantage of this model is that it helps explain behavior intention and behavior by tracing back to technology characteristics and other factors that influence user appraisal. As with the TRA and TPB, neither perceived risks nor perceived tradeoffs are explicit antecedents of behavior. However, they could be considered part of other variables in the model, such as perceived usefulness or attitude toward behavior. Many versions of TAM exist, such as the Unified Theory of Acceptance and Use of Technology [197], which pulls out factors such as gender and social influence as separate variables.

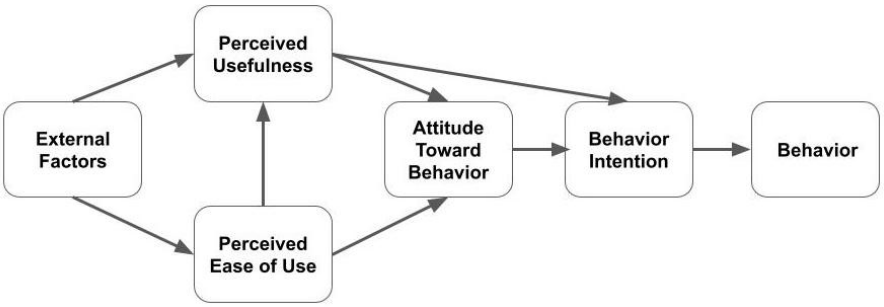

Figure 6: Causal diagram of the Technology Acceptance Model, in one of its most well-known forms.

TAM is one of the most widely applied models in human-computer interaction, such as in the conception of usability as consisting of effectiveness, efficiency, and user satisfaction [240]. Yen et al. [220] and Hornbæk and Hertzum [106] noted the value of its explanatory power and parsimony, although the latter finds it unable to fully account for the user experience, for instance, psychological needs and negative emotions.

In summary, the above EV models have components that appear relevant to cybersecurity adoption: attitudes, perceived norms, perceived behavioral control, threat and coping appraisal, and technology appraisal [68]. However, EV models lack a consideration of the progress of time and the consequent evolution of people's cognition and of social contexts for behavior, for example, how employees' security awareness can improve with constant feedback [21]. This makes it difficult in practice to effectively target and time a cybersecurity intervention to reach those who are most primed to benefit from it. In this proposed research, I want to identify a model that not only incorporates concepts of user expectancy and value for security practices but also the evolution of people's security thinking, emotions, and behaviors through time. Such a model will be a stage model.

2.3.2 Stage Models

The *Transtheoretical Model* [69,157] (Figure 7) incorporates insights from a variety of other models and theories, starting with Decisional Balance Theory. It proposes a cyclical process of *precontemplation*, *contemplation*, *determination* (sometimes called *preparation*), *action*, and either *maintenance* or *relapse* (called *termination* if it is final). At least one relapse is considered normal and expected. People move through these *Stages of Change* using 10 *Processes of Change*, with some being more relevant to a specific stage than other processes (see Figure 8). The *Experiential Processes* are (1) Consciousness Raising/Get the Facts, (2) Dramatic Relief/Pay Attention to Feelings, (3) Environmental Re-evaluation/Notice Your Effect on Others, (4) Self-Re-evaluation/Create a New Self-Image, and (5) Social Liberation/Notice Public Support. The *Behavioral Processes* are (6) Self-Liberation/Make a Commitment, (7) Counter Conditioning/Use Substitutes, (8) Helping Relationships/Get Support, (9) Reinforcement Management/Use Rewards, and (10) Stimulus Control/Manage Your Environment. The advantages of this model include its flexibility, since it can be used in conjunction with many psychological theories; and its usefulness in tailoring an intervention to an individual's readiness to change, as assessed with a stage diagnostic. A disadvantage is that the Transtheoretical Model has not been experimentally validated, and it does not account for social influences by stage.

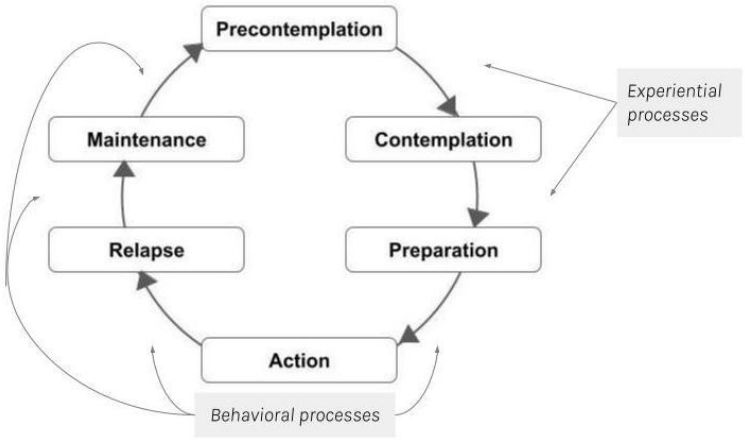

Figure 7: Diagram of the Stages of Change in the Transtheoretical Model, with arrows pointing to the stage transitions motivated by either Experiential or Behavioral Processes of Change. People enter the cycle at Precontemplation and proceed clockwise around, but they can exit and re-enter the process at any point.

In medicine and public health, the TTM has been used to tailor messaging [103] and other interventions to move people toward exercise [127], smoking cessation [53,196] and sobriety [141], and to identify anorexia patients at risk of treatment relapse [134]. Noar et al. found in a meta-analysis of 57 studies using print communications for health behavior change [148] that the type of material used and the use of TTM constructs such as the Stages of Change were associated with significantly greater effect sizes for print communications tailored for individuals, while tailoring on non-TTM constructs such as social norms did not produce significant gains. Moreover, the TTM was found to be an effective weight management intervention in a Brazilian randomized controlled trial, in which the intervention group received additional 30-minute sessions with a dietitian to increase decisional balance and self-efficacy [81]. Those assessed to be in "pre-action" (including TTM precontemplation, contemplation, and preparation stages) used goal-setting and problem-solving to boost awareness and motivation to overcome

health challenges, and those in "action" (including TTM action and maintenance stages) used similar techniques related to more detailed guidance on nutrition concepts and physical activity [81]. In HCI, Lin et al. adapted the TTM Stages of Change as a framework for measuring the effectiveness of the Fish'n'Steps social computer game for boosting physical activity in a workplace [128]. Grimes et al. applied the TTM Processes of Change to development of the OrderUP! casual mobile game for boosting healthier meal choices [90].

In cybersecurity and in privacy, Sano et al. [175,176], Faklaris et al. [69], and Ting et al. [190] have explored applying the Stages of Change and Processes of Change to end user studies. These researchers identified a theoretical and/or empirical basis for classifying computer users by whether they are in either precontemplation (Stage 1), contemplation/preparation (Stages 2-3), or action/maintenance (Stages 4-5) of adopting practices such as updating their operating systems, checking for https in URLs, and using antivirus software. Sano et al. [175,176] tested messaging strategies by stage, for example, finding that a message emphasizing ease of the OS update was significantly associated with users in the preparation stage answering "I update OS now" to a survey item. Additionally, Faklaris et al. used handouts about two-step authentication as an intervention for Amazon Mechanical Turk workers and found a significant difference in progress toward Stage 4-5 vs. the control group, which did not see handouts, as measured by a post-test survey conducted three days after the intervention.

Diffusion of Innovations [168] (Figure 8) is best known for its *adopter stages* by time to adoption (innovator, early, early majority, late majority, and laggards), specified *environmental factors* for diffusion (messaging channels, time, and social systems) and *attractiveness of innovation* characteristics that support diff (relative advantage, complexity, trialability, potential for re-invention, and observable effects). These are part of the overall innovation-decision process, which unfolds in five stages: *knowledge*, *persuasion*, *decision*, *implementation*, and *confirmation*. Among its advantages are the focuses on communication and on innovation characteristics as antecedents of the decision process, and its applicability to decision-making units larger than the individual. A limitation is that it is better suited to large social units or societies, rather than to individuals or small groups.

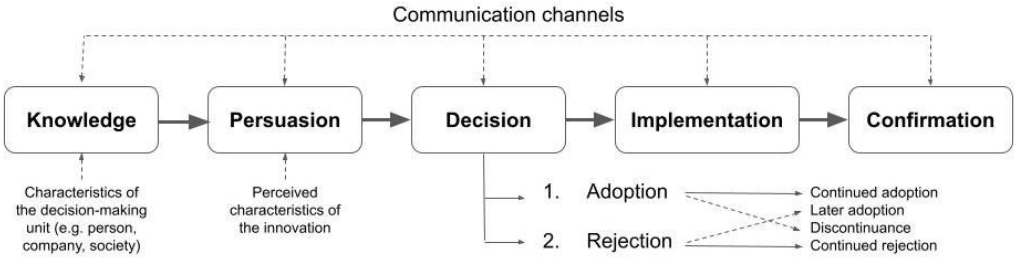

Figure 8: The innovation-decision process in Diffusion of Innovations. This describes how a person (or other decision-making unit) moves through, first, knowledge of an innovation; then, to forming an attitude toward the innovation; next, to a decision to adopt or reject it; and, finally, to implementing the new idea and to confirmation of the decision. Communication influences each stage of the process.

DoI has been used in hundreds of studies, more recently on topics such as mobile banking [5] and ls! HIV prevention [117]. One study proposed it as an overarching framework for measuring the spread of innovative health programs, using measures of Organizational Climate, Awareness-Concern-Interest, Relative Advantage, Complexity, Observability, Levels of Use, Levels of Success, and Levels of Institutionalization [187]. Often, researchers first observe the diffusion process at work, and then apply these learnings to develop interventions for dissemination [50]. In cybersecurity, DoI concepts have been

used to explain diffusion of awareness, motivation, and knowledge among end users [42,44] and the diffusion of security behaviors [126]. Witschey, Xiao, and collaborators [215,216,219] found DoI concepts such as communication channels to fit their data from their studies of software developers' adoption of security tools. Their statistical model showed that significantly predictive factors for tool adoption were Observability, Advantages, Policies, Inquisitiveness, Education, and Exposure [216].

The TTM and other stage models are not without their critics. Some such as Weinstein et al. [207,209] have challenged tests of stage theories that rely on cross-sectional research designs as not persuasive of their effectiveness for behavior change. They advocate the use of experiments that include a control and that test for not just whether a stage-matched intervention is effective (such as an awareness intervention for Stage 1) but whether a stage-mismatched intervention is ineffective (such as an awareness intervention for Stages 2-3). Prochaska et al. [159] have laid out a hierarchy of stage-theory evaluation criteria, including *clarity*, *consistency*, *parsimony*, *testable*, *empirical adequacy*, *productivity*, *utility*, and *practicality*. Meyer [140] notes that most diffusion studies focus on quantitative, retrospective data collected at a single point in time from adopters of a single innovation, and that this has limited what is known about aspects such as rejection or discontinuance of the innovation, or the direction of the causal relationships among between change agent contacts, social status, and greater adoption.

The DoI model appears to be a good match to describing how cybersecurity practices diffuse because, similarly to technology appraisal in the TAM, the *characteristics* of the cybersecurity practices (such as being easy to use or mandatory) are important to persuading people to use them, and because people's *degree of adoption or non-adoption can change over time* (such as how often they choose to create strong and unique passwords) [68]. However, I theorize that the TTM's *Processes of Change* show promise for predicting what cybersecurity interventions will suit which segments of a target audience [69]. If someone shows a high level of *resistance* to security practices, for instance, they could be primed for a reflection on the pros and cons of adopting these practices, akin to the TTM use of motivational interviewing [34,69]. Someone who has a high level of *concern* about the security of their accounts or data, but who isn't yet fully aware or knowledgeable about security practices, could be matched with a game that simulates everyday cybersecurity issues and teaches people effective practices [34,69]. Those who are *attentive* to security practices, but who haven't adopted them, could be given a 30-day trial or a social nudge [34,69]. And someone who is fully *engaged* with security practices could be reinforced with a rewards program and forums where they can show off their knowledge and educate others [34,69].

2.4 Guiding Research Question

To restate: I believe that an empirical understanding of the cybersecurity adoption process will help us to specify the mental states and social influences acting at each step, leading to better targeting and timing of security interventions. My work [34,68–70,150,186] has found that social contexts influence whether people choose to keep their passwords confidential, and that security attitudes are significantly associated with experiences of security breaches, security behavior intention, and recalled security actions. I have identified these relevant components of existing behavior models: attitudes, perceived norms, perceived behavioral control, threat and coping appraisal, appraisal of the characteristics of security practices, changes in adoption or non-adoption through time, and experiential and behavioral processes of change. In this proposed empirical research, I seek to answer the following question:

- ***RQ-0:*** *What stages do people go through in adoption (or non-adoption) of cybersecurity behaviors?*

3. THESIS RESEARCH DESIGN

In this short chapter, I give an overview of my chosen research design (Section 3.1), then describe each of its three phases (Sections 3.2-3.4).

3.1 Overview of Exploratory Sequential Mixed Methods

The research design that I chose is known as exploratory sequential mixed methods [38]. In this design (Figure 9), a researcher starts with interviews in a small sample to investigate the research question, then develops a survey instrument from that data; and, finally, deploys the survey instrument with a larger, different sample of the same population to see if the findings will generalize. The findings from the qualitative and the quantitative studies can then be triangulated and integrated to produce a synthesized model. The qualitative findings subsequently can be used to develop a participant-informed intervention, while the survey instrument and quantitative findings can be used to evaluate that intervention's effectiveness. While a disadvantage is the time and cost that it takes to complete the multi-part research project, an advantage is that it combines each method's strengths and that their weaknesses do not overlap (small *N* vs. large *N*, details vs. trends, in-depth findings vs. ability to generalize) [37].

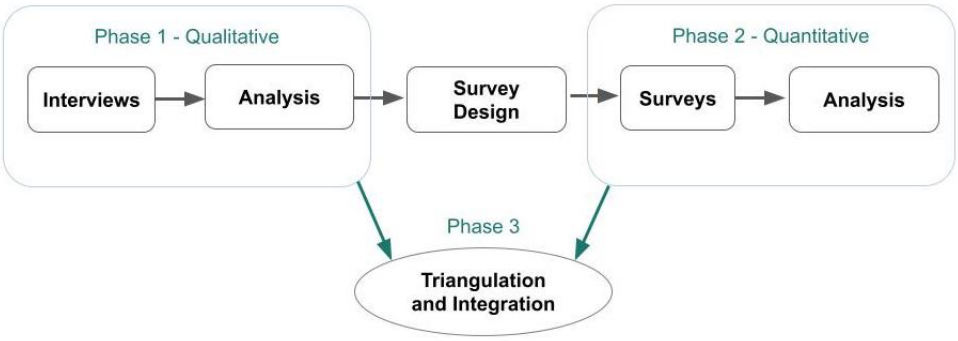

Figure 9: Diagram of my research design, showing how the interview phase leads to the survey phase, and finishes with a phase of triangulating and integrating the data from the two previous phases.

3.2 Phase 1 (2021): Synthesizing a Common Narrative

Phase 1 was a remote interview study with four rounds of data collection – A, B, C, and D. The first two were used to refine the interview protocols. The last two were included in the analysis. The goals were to identify the steps of security behavior adoption that participants have undergone and the social influences [41,44,66,165] that were relevant at each step, along with participants' mental states [42,62], prior experiences of security breaches [70], and internet and/or security know-how [115]. This was done through, first, eliciting participants'' recollections about what security concerns they had recently experienced and how they dealt with those concerns, then second, asking them follow-ups about 1-3 other security practices.

3.3 Phase 2 (2022): Validating the Phase 1 Insights

Phase 2 was an online questionnaire study with five rounds of data collection. The first four were used to refine the survey protocols. The final round is included in the analysis. The goal was to create generalizable knowledge about the prevalence of the Phase 1-identified steps of security practice adoption

in the U.S. population and the association of these steps with certain social influences and practice characteristics.

3.4 Phase 3 (2022): Triangulation and Integration

Phase 3 was an analysis to triangulate [224] and integrate [73] the results of Phases 1-2 with prior work. With the study team, I have reflected on these results considering existing models of behavior change and their associated processes of change, along with comments of anonymous paper reviewers and academics at three other universities who have been given versions of the results for feedback. The output is a list of suggested survey items and the survey display logic for determining which step someone is in, a data-informed diagram of the steps of security behavior adoption, and a table describing each step, the main social influences associated with each step, and the chief obstacles to moving forward.

4. PHASE 1 STUDY (2021): SYNTHESIZING A COMMON NARRATIVE

In this chapter, I describe the first phase of my thesis research. Methods (Section 4.1) describes participants, procedures, and analysis, while Results (Section 4.2) describes the sample characteristics and the interview findings and insights, leading to research questions and hypotheses to test (Section 4.3).

To summarize: I found that interview participants' narratives of security practice adoption had four steps in common. These are Threat Awareness (Step 1), Security Learning (Step 2), Security Practice Implementation (Step 3), and Security Practice Maintenance (Step 4). Furthermore, I identified step-specific social influences and obstacles to moving forward. I found that trialability and troubleshooting help are the social factors significantly associated with Step 3, and leadership and caretaking with Step 4.

4.1 Methods

Phase 1 was a remote interview study with four rounds of data collection – A, B, C, and D. Only the last two were included in the analysis. The goals were to identify the steps of security behavior adoption that participants have undergone and the social influences [41,44,66,165] that were particularly relevant at each step, along with participants' mental states [42,62], prior experiences of security breaches [70], and internet and/or security know-how [115]. This was done through, first, eliciting participants' recollections about what security concerns they had recently experienced and how they dealt with those concerns, then second, asking them follow-ups about 1-3 other security practices.

4.1.1 Participants

My target population was internet users aged 18 and older who frequent U.S.-based websites. In the A and B rounds, I piloted interview materials and a pre-interview screener in Qualtrics with N=3 lab members and N=3 contacts on social media. For the C and D rounds (N=3 and N=14, respectively), people who self-identified as U.S. residents age 18 or older were recruited for the screener via Craigslist, Facebook and Google posts targeted to reach 12 U.S. metropolitan statistical areas (MSAs) [23,231]. These areas represent a diversity of MSAs by size and region of the country (Table 3). Seeding recruitment in these areas simplified the process, although some saw posts outside of these areas because of algorithmic optimization or organic spread. In these posts, I introduced myself and briefly described this research, then provided a contact email where interested people can receive our study information sheet and ask questions. Those who agreed to participate were emailed a link to the screener and received a $3 e-gift card for filling it out.

Table 3: The 12 Metropolitan Statistical Areas (MSAs) targeted for Phase 1 participant recruitment. Two are the largest in size (>10 million population), five are mid-tier (10-1 million), and five are small (<1 million).

Rank	Metropolitan Statistical Area (MSA)	2019 pop. est.	Area of US
1	New York City-Newark-Jersey City, NY-NJ-PA MSA	19,216,182	NE
2	Los Angeles-Long Beach-Anaheim, CA MSA	13,214,799	WSW
10	Phoenix-Mesa-Chandler, AZ MSA	4,948,203	SSW
18	Tampa-St. Petersburg-Clearwater, FL MSA	3,194,831	SSE
27	Pittsburgh, PA MSA	2,317,600	Mid-E
41	Oklahoma City, OK MSA	1,408,950	Mid-S
47	Salt Lake City, UT MSA	1,232,696	W
74	Charleston-North Charleston, SC MSA	802,122	ESE
130	Gulfport-Biloxi, MS MSA	417,665	S
150	Fort Collins, CO MSA	356,899	Mid-W
168	Olympia-Lacey-Tumwater, WA MSA	290,536	NW
170	Duluth, MN-WI MSA	288,732	N

This screener collected people's responses to items about security attitudes using the SA-13 items [34] and to awareness and adoption of security practices in four general areas [62,222]: keeping software up-to-date, maintaining good password hygiene, staying alert for phishing, scammers and "fake news", and securing devices and networks. It also collected personal data to aid in diversifying the sample: their previous experiences of or exposure to communication about security breaches, their age bracket, their gender and racial/ethnic identities, their education and income levels, the size of their households, and their security-relevant training or knowledge. To get a quick read on each participant, I calculated separate composite scores for the SA attitude scales and for the awareness and adoption items using a simple average of participant ratings for each item, using 0 for N/A or missing data. I then calculated the overall "Security Score" by summing the participant ratings for each item for the attitude, awareness, and adoption items. See Appendix A for a copy of this survey and the scoring method.

Using the Security Score primarily and the other items secondarily, participants were selected and invited by email to participate in 60-minute interviews held over Zoom. The selections were made to get at least three people with a Security Score that was either low, medium, or high, to offer a diversity of security literacy in the sample, then to also diversify by gender, age, and racial/ethnic identity. The three C interviews were chosen from the Pittsburgh MSA, and their data was retained for the final analysis because the study protocol had needed no changes. The D interviews were chosen outside Pittsburgh.

4.1.2 Procedure

Those who agreed to participate in an interview were asked to schedule a Zoom meeting and given the choice to use either an internet link or a telephone call to join the meeting. These sessions were recorded to the secured cloud server for Carnegie Mellon University's Zoom enterprise account, with the audio automatically transcribed there and by Otter.ai, a separate third-party service. We informed participants that we intended to make use of 3rd party transcription and annotation services such as that provided by Zoom and that we were taking measures to guard participant confidentiality from these 3rd parties, such as not including personally identifiable information (PII) in recording metadata. Participants

were cautioned to talk in a place where it is unlikely that they would be overheard and where bystanders would not be recorded. They received $15 electronic gift cards as an incentive, emailed shortly afterward.

The interview protocol was structured to answer the following sub-research questions:

- ***RQ1-1:*** *To what extent are participants aware of, motivated to use and/or knowledgeable about how to deal with their security and privacy concerns?*
- ***RQ2-1:*** *What are the steps of participants' security adoption decision process?*
- ***RQ3-1:*** *At each step of the adoption process, to what extent do peers, authorities or media coverage influence people's thinking about security measures?*
- ***RQ4-1:*** *At each step of the adoption process, to what extent do perceived characteristics of the security measures influence people's thinking about the measures?*

This was done by eliciting their stories about recent security concerns and how they had dealt with them, and then following up with questions about their sources of security advice and their experience of using security practices. I also asked about 1-3 other security practices, time permitting. Participants were then able to ask me questions of their own. See Appendix B for a copy of this interview protocol and the detailed research sub-questions.

4.1.3 Analysis

For the Phase 1 screener survey, I downloaded datasets from the Qualtrics online survey software[3]. The collected datasets were cleaned by deleting seemingly bad-faith responses that had not been caught by the programming checks for fraud and low-quality responses. Bad-faith responses included those to open-ended questions that were gibberish (such as "sdwerevwe"), had been copy-pasted from elsewhere (such as "and it was most definitely not so," in response to a question about security behaviors), or did not follow directions (leaving the input box blank, in response to an instruction to respond with "None" if the item did not apply to them). An attention-check question directed participants to respond with answer 4; all other responses led to rejection of the data. The Security Score was computed by summing responses to items about awareness, frequency of use, and attitudes toward security practices. See Appendix A for the full protocol and directions for computing the Security Score.

For the Phase 1 interviews, the initial audio transcripts were generated automatically through Otter.ai[4], which was integrated with the principal investigator's Zoom conferencing software[5]. Two members of the study team went through the resulting files and cleaned up language that was not transcribed accurately. We excluded the first two rounds of pilot testing from analysis (labeled "A" and "B") but included the third round (labeled "C") because the interview structure and data quality were on par with that of our final round of interviews (labeled "D"). However, we decided to exclude the transcript for D1 from the dataset due to poor audio quality. Then, the team used the MAXQDA qualitative analysis software[6] to iteratively develop a codebook and code the transcripts, meeting frequently to review codes and code summaries and to discuss emerging similarities and differences among the data [173,212].

[3] https://www.qualtrics.com/
[4] https://otter.ai/
[5] https://zoom.us/
[6] https://www.maxqda.com/

In parallel, one member of the study team iteratively diagrammed the apparent relationships among the similarities and differences (Figure 9). This method of synthesizing data into a coherent set of relationships is common to both social science [139] and to design [58,98]. The entire team discussed the final diagrams, with two team members returning to the data to extract relevant quotes and to check how well the diagrammed relationships matched the data. The team also identified relevant prior work that matched the findings and added certainty that the results were valid.

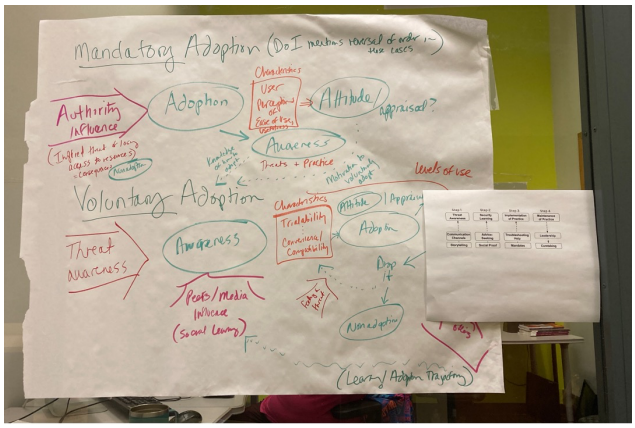

Figure 10: Examples of Phase 1 iterations of the steps diagramming, drawn from interview codes and notes.

This process resulted in a synthesis of the steps of security behavior adoption that were common among participants. See Appendix D for our interview codebook, which includes sources for some code definitions and lists the steps of participants' security practice adoption that we associated with codes.

4.2 Results

In Phase 1, I found that interview participants' narratives of security practice adoption had four steps in common. These are Threat Awareness (Step 1), Security Learning (Step 2), Security Practice Implementation (Step 3), and Security Practice Maintenance (Step 4). Furthermore, I identified step-specific social influences and obstacles to moving forward, which are detailed below.

4.2.1 Sample Characteristics

I received *N*=588 screener responses that I judged reliable and valid, from which I computed an overall Security Score and three composite scores for Awareness, Adoption, and Attitudes toward general security practices. Descriptive statistics are displayed in Table 4.

Table 4: Most participants in our Phase 1 screener survey (*N*=588) were aware of at least one security practice, but some reported no adoption of such practices. The Security Score was computed by adding values for answers to point-response sets, while the Awareness, Adoption and Attitudes scores are computed as mean values of the item responses in those specific survey sections.

	Security Score	Awareness	Adoption	Attitudes (SA-6)
Mean	130.38	3.28	3.20	3.82
SD	31.64	0.70	1.41	0.75
Min	52.00	1.08	0.00	1.33
1Q	109.75	2.85	2.08	3.33
2Q	135.00	3.46	3.46	3.83
3Q	155.00	3.92	4.38	4.33
Max	182.00	4.00	5.00	5.00

For the N=17 interview participants whose data is included in the analysis, they completed a five-minute screening survey and a longer interview on Zoom. Interview times ranged between 45 and 90 minutes. See Tables 5-7 and Figures 11-12 for their sample characteristics.

Table 5: Profile of N=17 participants in Phase 1 whose data was used in the study analysis. Data from one recruit, D1, was removed because of poor audio in the remote interview and resulting recording file.

ID	Description	Security Score	Score Group
C1	College-level lecturer in foreign languages	158	High
C2	Administrative assistant for a government agency	169	High
C3	Financial and patient services for a dental school	145	Middle
D2	Security worker for private companies	152	High
D3	Accountant and parent in a large metro area	147	Middle
D4	Recent college graduate working in finance	126	Middle
D5	Householder and computer gig worker	141	Middle
D6	Freelance worker in information technology	149	Middle
D7	Accountant and parent in a large metro area	128	Middle
D8	Former teacher and computer gig worker	117	Low
D9	Recent college graduate working a mix of jobs	129	Middle
D10	Independent contractor for medical scheduling	118	Low
D11	Physical education teacher and parent in small city	82	Low
D12	Musician and gamer married to security worker	178	High
D13	Householder and computer gig worker	82	Low
D14	Householder and graduate student	127	Middle
D15	Full-time worker in information technology	110	Low

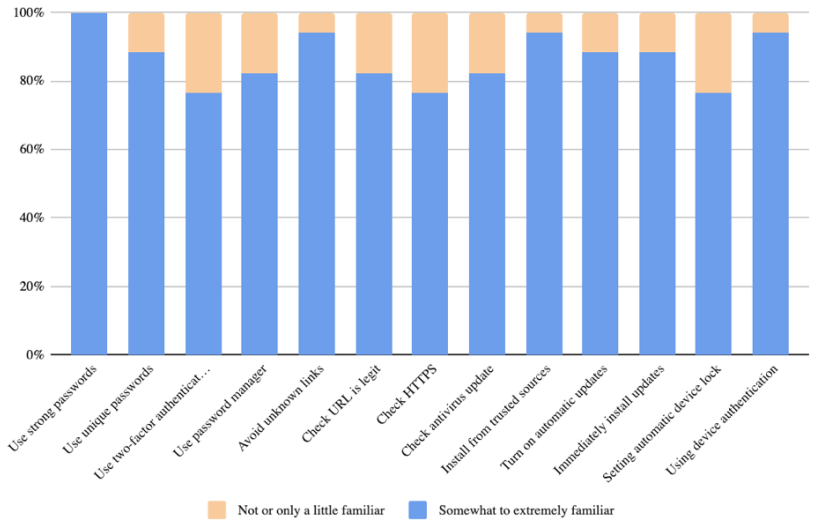

Figure 11: Of our Phase 1 interviewees (*N*=17), most were "Somewhat Familiar" to "Extremely Familiar" with all 13 of the security practices that our screener surveyed them about.

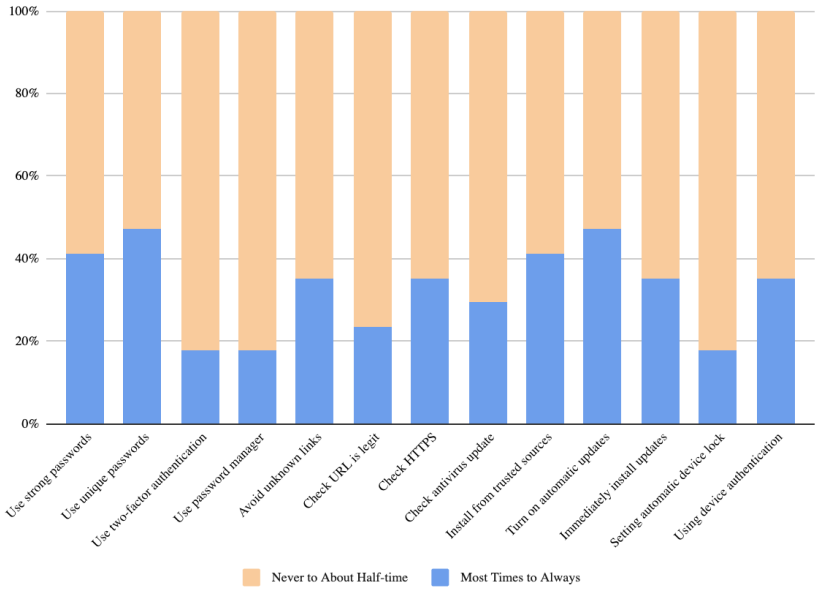

Figure 12: Of our Phase 1 interviewees (N=17), only a minority reported using any of 13 security practices "Most Times" to "Always."

Table 6: Demographics of Phase 1 interview participants (N=17).

Age		Gender		Hispanic/Latinx		Race/ethnicity		Household size	
7	18-29	10	Male	1	Yes	5	White or Caucasian	2	Only them
3	30-39	7	Female	15	No	4	Black or African American	3	Two
5	40-49	0	Nonbinary	1	Prefer not to say	1	Native American or Alaska Native	3	Three
1	50-59					4	Asian - East or Central	5	Four
1	60 or older					1	Asian - South, Southeast, or Southwest	1	Five or more
						1	Native Hawaiian or Pacific Islander	3	Did not say
						0	Middle Eastern or North African		
						1	Prefer to self-describe: Caucasian/Latino		

Table 7: Socio-economic metrics and relevant prior experiences for Phase 1 interview participants (N=17). "SD" stands for Sensitive Data, which, in the U.S., is governed by regulations such as HIPAA or FERPA.

Income		Education		Exp. Working w/ SD		Computer/Information Science Experience	
2	Up to $25,000	0	Some high school	4	None at all	10	I both earned a degree in such a field and have worked or am working in it.
8	$25,000 to $49,999	0	H.S. degree or equivalent	2	A little	2	I earned a degree in such a field, but never worked in it.
2	$50,000 to $74,999	2	Some college /associate's	5	A moderate amount	3	I did not earn a degree in such a field, but I have worked or am working in one.
4	$75,000 to $99,999	11	Bachelor's degree	4	A lot	2	I did not earn a degree in such a field, nor did I ever work in one.
1	$100,000 or more	4	Graduate/ professional	2	A great deal		

4.2.2 Interview Findings and Insights

I found that participants' common narratives of security behavior adoption followed these steps (Figure 13): Threat Awareness (Step 1), Security Learning (Step 2), Security Practice Implementation (Step 3), and Security Practice Maintenance (Step 4). Steps 1 and 2 appeared both common and necessary to people's security narratives: Step 1 because it introduced a cyber threat that participants would need protection from (such as a breach of an important online account), and Step 2 because it introduced a computational tool or a cognition-based practice for providing that protection (such as using a password manager to generate and store hard-to-crack passwords, or knowing how to manually create a password that is difficult to guess). However, these steps were not sufficient to move participants to adoption. Participants reported moving to Step 3 and, later, Step 4 because of the *trialability* of a security practice and because they had access to *troubleshooting* help. Authorities sometimes jump-started the process at Step 3 by mandating a participant's use of a security practice (such as two-factor authentication) for an organizational or business account. This caused at least one participant to go back to Step 2 to learn about that practice, and then to voluntarily adopt it for other accounts.

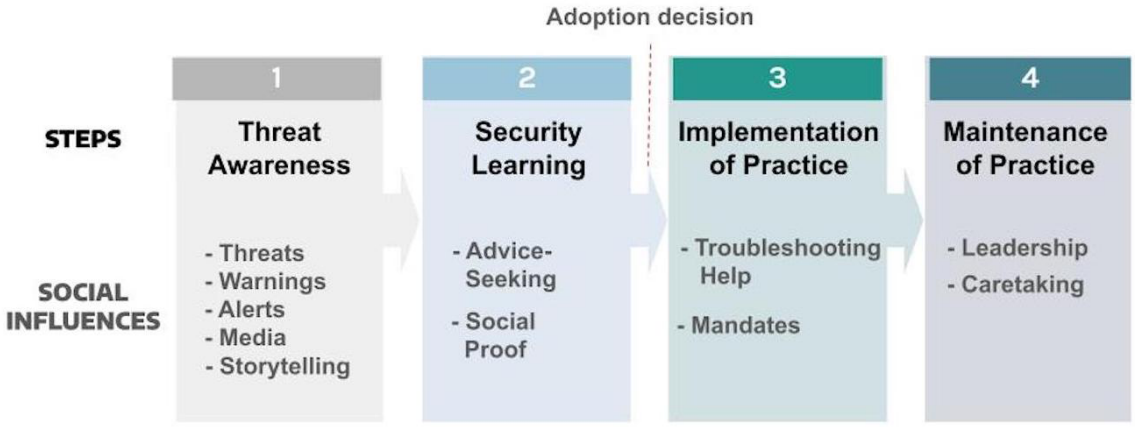

Figure 13: A linear diagram of the common narrative of security practice adoption from *N*=17 Phase 1 participants, with the associated social influences. The direction of association for Steps 1-3 (where social influences lead to Threat Awareness, Security Learning, and Security Practice Implementation, respectively) is reversed for Step 4 (where Security Practice Maintenance leads to adoption leadership and to caretaking behaviors).

Social influences affect these steps through communication channels and storytelling (Step 1), advice-seeking and social proof (Step 2), troubleshooting and mandates (Step 3), and leadership and caretaking (Step 4). While Threat Awareness (Step 1) found them almost without their looking for it, participants often had to seek information and sort through Security Learning (Step 2) on their own; in fact, they reported using time in their day or over several days to figure out how to respond to a given threat. For this Step 2 process, participants appeared to focus on one or two trusted sources (such as a friend in a similar situation, a family authority figure, a tech-savvy coworker, or a brand-name news organization or tech publication) to teach them how to deal with a given threat and to help them work through their uncertainties. In Step 3, for voluntary adoption, the same or similar source would show participants how to try out the security practice and was their go-to for troubleshooting help. Finally, participants who made it to Step 4 voluntarily would then feel motivated by self-identity and an obligation of reciprocity to educate others who are still in Steps 1, 2 or 3, becoming themselves a social influence.

Details on each of the four steps are available in Table 8 and in Sections 4.2.2.1-4.2.2.4.

Table 8: Summary of Phase 1 participants' common security narratives (*N*=17)

Step	Description	Associated Social Influences	Obstacle(s) to Moving Forward
Threat Awareness (Step 1), Section 4.2.2.1	- Mention of threat, risk, harm, or potential harm related to security; stated evaluation of the degree to which an event has significant implications for their security. - Examples: Receiving a threatening email, reacting to media reports, suspecting that your smartphone was illicitly accessed.	- Communication channels. - Storytelling.	- No awareness of a given security practice or other technology.
Security Learning (Step 2), Section 4.2.2.2	- Knowledge of existence of a given security practice or other technology (acquiring knowledge and skills, moving from a state of uncertainty to a state of certainty), but no enactment of that practice. - Examples: Hearing about secure messaging, finding out how others verify a job ad, being told to update software.	- Advice-seeking. - Social proof.	- Not feeling a threat (skipped Step 1). - Rejecting adoption before it is tried.
Security Practice Implementation (Step 3), Section 4.2.2.3	- Acting to test the security practice to evaluate its usefulness; acting to put the decision to adopt into effect. - Examples: Using a promo code or a free trial offer, playing around with a practice; settling on a security tool, acquiescing to a security policy, following up on Step 2.	- Troubleshooting help. - Mandates.	- Discontinuing adoption after the practice has been used at least once.
Security Practice Maintenance (Step 4), Section 4.2.2.4	- Acting to finalize the decision to use a practice; expanding use of the practice; mention of past implementation. - Examples: Stepping up the frequency of use; making statements like "I still use this" or "I currently use this."	- Leadership. - Caretaking.	- The adoption context becomes obsolete. - Waning effectiveness of the practice.

4.2.2.1 Threat Awareness (Step 1). When asked to think back to a time when they had a security concern, participants recalled negative experiences that happened to themselves, their loved ones, their colleagues, or people they've known closely in the past. Specific threats included a student breaking into the school gradebook [C1], a hacker threatening to leak their private photos [C3], a family member or romantic partner spying on their messaging [D2, D14], a website trying to scam them out of personal information or money [D11], or a company exposing their account data to misuse [D15]. Most participants recalled feeling uncertainty or fear for possible harms at this step. Echoing Ruoti et al. 2017 [170], some felt a sense of inevitability about the prospect of suffering a security breach or an organization exposing their data [C2, D6, D8].

Several participants reported that they repeatedly have been exposed to threats, and that this direct experience helped them to stay alert to more security harms or potential harms:

> At least if I get snookered once every few months or once every six months, then I'm on guard for a while. [D8]

Communication Channels and Storytelling. At Step 1, communication channels were both the way that actual threats reached people and the way that they became aware of threats to others that could potentially also impact them. The channels included emails [C2, D2, D4, D10, D11, D12], text messages [D9, D13], social media posts [D3, D4], IT warnings [C1, D10], news reports [C2, D11, D12], fictional

TV shows [C1], and movies [C1, D6]. Most did not have to put forth effort to become aware of threats, instead receiving the information through their lived experiences of threats, through security alerts or warnings, or through their environments.

As in prior work [42,45,163,203], participants reported hearing or seeing people's stories about security threats either through the above channels or during social interactions, for example, at a work meeting [C1], or in conversation with a friend or family member [D4, D8].

Lived experiences and/or first-person stories of security incidents at this step were most impactful for ingraining threat awareness in participants and moving them forward.

> Yeah, like if you have an experience with it, or you might know somebody that had a bad experience, you're gonna adopt the technology faster than somebody who says "Ah, that'll never happen to me." [C2]

Obstacles to Moving Forward. Some participants reported threat awareness but no corresponding awareness of security practices that could help protect against those threats. They were unaware that certain security practices or recommendations existed until they were forced to adopt a practice by an institution or a service - or until our interview. (For example, many were unaware before the interview that software updates often carry fixes for security flaws and should be installed promptly.) Some felt little motivation to try to deal with threats, due to their feeling of inevitability about being subjected to security breaches [C1, D10].

A few participants also reported cultural or linguistic barriers to learning about or educating others about practices [D12]. This is because interface text or directions are often written in English and in computer security jargon, which is difficult to understand or translate.

> These words individually make sense. But when you put them together, what do they mean? And I'm like, that is "firewall." And [my parents are] like, uh-nuh, you lost me. And I'm just like, you know, just a big sigh. And it goes in circles. [D12]

4.2.2.2 Security Learning (Step 2). Participants reported learning about security practices from peers such as colleagues, friends, and family members, and from authority figures such as professors, parents, elder siblings, training staff and IT departments at work [42,145,155,164,165]. Mandatory cybersecurity practices for an organization (e.g., the workplace) [D4, D11] or service (e.g., a bank account) [D12] also spurred security learning, as did department seminars and workshops on security awareness. Specific media sources mentioned were traditional network news on TV and radio [C2, D11]; platforms such as Google [C1, D3, D8, D12], YouTube [C1, D3], Twitter [C2, D12], Facebook [C2, D3, D4, D8, D11, D13], TikTok [D12], and Reddit [C1, D4]; and fictional movies and TV shows with cybersecurity plotlines [C1, D6].

The motivating factors for participants to decide to try out security features were the advertised trialability of software (free trials, easy setup, etc.) [C2, C3, D6, D14, D15], and seeing encouraging reviews.

> I looked at iMessage. And then I eventually see Signal and I see the features and ... all the reviews. So, I decided to use Signal. [D14]

Advice-Seeking and Social Proof. Participants at this step reported engaging in online information exchanges, but largely seeking information rather than providing it. To judge the credibility of these sources, participants relied on social proof by reading reviews and comments on social media posts to see

how others received that advice. Participants also said that they engaged with these posts (such as commenting on a post that they found useful) so that they would provide a signal of its helpfulness to others [D3, D5].

Among the people in their lives, participants judged whom to seek advice from by what they knew about their background or their knowledge of computer science or information technology [C1, D12, D15], echoing Redmiles et al. [164]. They also relied on social proof to guide their thinking.

> I guess I trust him because he has a degree in Computer Engineering. And because my department head trusts him. The dean of the school trusts him. The president of the school trusts him, so he's a trustworthy person who's been there, I think something like 10 years, long time. [C1]

Obstacles to Moving Forward. When participants hesitated to adopt their sources' recommendations (such as changing their passwords, activating multi-factor authentication, using a password manager or other security apps, and checking a website's safety), it was due to distrust in the technological systems [D12] and/or the security task being too tedious or overwhelming to be worth the protection gained [D4]. Another important factor was the comfort and familiarity with current practices, and the tendency to continue doing what they have been doing [D8, D11] [97]. Their statements echoed findings in prior work about security-convenience tradeoffs [67,135,151,170,222].

> "You can be secure [on] your side, but on the server side, who knows." [D12]

> "It was almost like I was willing to take the small risks that, you know, my data would be compromised, in order to not have to, you know, take that extra five minutes, maybe to put that extra layer of security on it." [D4]

> "I get overwhelmed sometimes, with technology. ... I feel like it's another step I have to learn, and I get used to doing things in a certain way, and I guess I'm stubborn." [D11]

> "It's a nightmare to change your password in Yahoo." [D8]

Participants rejected adoption when they felt that the practice was inconvenient or not really required ("overkill"), or when an app was too expensive for a smaller budget [D6].

Some reported that they did not feel threatened anymore and would not be interested in adopting new behaviors because, they felt, a different security practice put in place after the past incident had taken care of the problem (such as a bank reporting taking actions to strengthen account security) [D12, D14]. Some also did not feel like they would be a target of future security breaches [D12].

4.2.2.3 Security Practice Implementation (Step 3). Some security practices that participants reported implementing were cognition-based, in that they most required the participants to employ facts, information or skills. These included taking more frequent backups (especially if they lost data in the past) [D6], not using the same password everywhere (especially if their account got broken into) [C2], not replying to unknown texts and emails [D2], and otherwise trying to correct the weak points in their current security habits [D5].

The other type of security practice that participants reported implementing was tool-based, involving either devices or software programs. Participants reported varying degrees of difficulty with navigating the technology, struggling when they did not have skills from a technology background [D8] and/or access to help with setting them up or with bugs that cropped up [D13].

Trialability and Troubleshooting. Participants at this step frequently mentioned using free trials of antivirus software [D6, D13], or new messaging platforms (instead of WhatsApp, which participants associated with weak data privacy) [D2, D14], or cryptocurrencies. The trials helped them to test different options and choose what best fit their needs, as well as to familiarize themselves with the designs. A few mentioned that they enjoy trying out new computational tools and will seek out promotional bundles for new experiences [D2, D6].

> I chose to settle with Signal because they have different features that suits my needs. There's no screenshot that can be taken from my chats, and I can disable my keying so that no one can learn what I type. Or that they have an option of making my chats disappear after five seconds. Which is a convenient option for me. [D2]

> Yeah, I've used, I first used the 1Password, and then I switched to Keeper. [D5]

When adoption succeeded, it was often with the help of peers or media for troubleshooting. Such assistance enabled participants to clear their confusion regarding the many brands of software performing the same functions (such as antivirus programs or password managers) [D6, D8], or about how their data would be used or misused [C1, D4, D5, D10]. Participants sometimes got stuck while trying to a security practice [D2], or reported that they could not figure something out, then reached out to either the media or peers who had helped them at Step 2 [C2, D5].

> You call them back at this number for the company. And it's busy. On the company's website. So, I'm after a while, thinking and I called my brother and my friend to help me out of this little jam here. [D8]

With successful troubleshooting, they were able to figure out how to perform these security practices in a particular way and to keep repeating these actions for the future.

Mandates. For some who did not first go through the Security Learning step, mandates spurred their adoption of a security practice (such as two-factor authentication) in a limited way.

> For Amazon and a couple other - my other bank ... FNB, I told you, they ... required it and then they actually shut it off after a while. ... If I'm on my same computer, it knows it's me. But if I go to another computer, like I'm on my work computer, I say, oh, I want to check my bank balance, it makes me do two factor authentication. [C2]

Such automatically applied security practices (another being having a firewall installed) were seen as convenient because they provide protection without much intervention. One participant said they voluntarily implemented two-factor authentication elsewhere after it was required for their bank account [D3]. But a few participants also felt that they didn't have enough autonomy over their function and didn't fully understand how the practices worked [D4].

> I have, I guess what I'm saying is mixed feelings on it. It is very, it is very convenient for me., just, you know, click a button, but sometimes I do think like, you know, I do question it, I guess, sometimes. [D4]

Obstacles to Moving Forward. Participants reported discontinuing a security practice because they remained unsure how their data would be used or misused [C1, D4, D5], or because they could not figure out how to set up the practice or how to use it correctly more than a few times [D6, D8]. Beyond

problems with onboarding, participants also discontinued use of apps if they felt annoyed by repeated email newsletter "spam" or notifications [D7], or if they feared that the app was interfering with the operation of their system [D12]. Examples of the latter are overriding custom settings or causing RAM issues, making it difficult for other software to run on the computer.

4.2.2.4 Security Practice Maintenance (Step 4). To reach maintenance, participants needed not just troubleshooting help, but for the security practice to demonstrate results and to be convenient. Examples of maintained practices include checking on websites' credibility [D6, D12], not answering unknown texts or emails [D4, D6], and using tools such as PayPal (which provides an additional layer of privacy for online banking) [D15], NordPass (a separately installed password manager) [D13], and Signal (which provides encrypted message backups) [D14]. Some reported perceiving an improvement in their security concerns after they started using the practice.

> Yeah, [the password manager] was very useful, because till now, I haven't seen any threat in my mails and or my emails as attacked. [D14]

Others did not personally witness results, but they relied on the credibility of a friend or family member who could testify to its usefulness through lived experience [C3, D10, D14].

Repeated exposure to threats also helped maintaining a security practice to become routine:

> Sometimes, you know, there's some attachments and there's more viruses if you open up the files and cause more problems. ... I've been in the industry so long that I don't even read anything, just delete it. [D6]

Leadership and Caretaking. Of participants who described maintaining security practices, all mentioned that they sought to help others avoid falling victim to scams and to adopt good cybersecurity practices. Common points of education were using strong passwords [D7], safeguarding privacy on social media profiles [D15], and employing general web etiquette [D6]. As in Step 2, participants reported engaging in online information exchanges, but now providing information more than receiving it: adding to comment threads on posts, contributing reviews, and commenting on "clickbait" social media to warn others [D3]. Participants reported telling friends and family member what had worked for them and giving their opinions on what these close ties should be doing to better protect their online data and accounts [C2, D10]. Participants also mentioned that they advise their parents and other older adults on how to protect against spam mail and bank fraud, echoing other findings about informal tech helpers [C2] [125,145,155].

> "My mom, she has a computer. She's a senior citizen, she's older. And she actually consults me before she does anything because she's like, I don't want this to happen to me, what happened to you. So, I help her out a lot. And she don't buy from Amazon. If she wants to buy something, I get it for her." [C2]

> "Hey, you know, do you know your password to this? Did you install this? You do? Would you mind if I borrowed your thumb for a minute?" And you know, did this and, you know, sometimes [my relatives] go with it. [D12]

Obstacles to Continued Maintenance. A few participants said they had stopped using a security practice after some time had passed, either because the adoption context was now obsolete [D13] or because they decided not to keep going with it [D5]. Examples were stopping using antivirus programs because of replacing a PC with an Apple device [D4] and dropping a subscription due to not wanting to pay for software [D6, D10].

4.3 Phase 2 Research Questions and Hypotheses to Test

Going into Phase 2, I formed the following research questions and hypotheses based on the Phase 1 results. These helped guide my creation and programming of the Phase 2 survey instrument.

- ***RQ1-2:*** *Does a survey algorithm exist that can classify participants into one and only one step of security practice adoption?*
- ***RQ2-2:*** *What is the distribution of these steps in a U.S. sample?*
- ***H1-2:*** *Authority influences and peers/media influences will significantly associate with evidence of an adoption decision.*
- ***H2(a)-2:*** *Trialability will be positively associated with adoption of a tool-based security practice.*
- ***H2(b)-2:*** *Troubleshooting help will be positively associated with adoption of a tool-based security practice.*

5. PHASE 2 STUDY (2022): VALIDATING THE PHASE 1 INSIGHTS

In this chapter, I describe the Methods (Section 5.1) and Results (Section 5.2) used for the Phase 2 online questionnaire study.

In this phase, I designed and executed a survey algorithm to classify participants in a nationwide panel by step of adoption of password managers. For the step-classification algorithm, I added two steps that represent obstacles: No Learning or Threat Awareness (Step 0), and Security Practice Rejection (Step X). I found support for hypotheses that trialability and troubleshooting help are associated with adoption, and I determined that lack of internet and security know-how is associated with Step 0 and Step 1.

5.1 Methods

Phase 2 was an online questionnaire study with five rounds of data collection. Only data from the final round is included in the analysis. The goal was to create generalizable knowledge about the prevalence of the Phase 1-identified steps of security practice adoption in the U.S. population and the association of these steps with certain social influences and practice characteristics.

5.1.1 Participants

5.1.1.1 Pilot Testing. I recruited for three pilot rounds in person, on social media channels, and on Amazon Mechanical Turk. My Mturk recruitment posts for a "survey on computing behaviors" qualified those who were U.S. residents 18 or older, who had completed at least 50 jobs, and who had an acceptance rate of 95% or above. Mturk workers were paid $3; all other testers were volunteers.

5.1.1.2 Postcard Recruitment. My first attempt at national data collection was to use the U.S. Postal Service to reach adult U.S. residents who otherwise would not see a survey recruitment in the usual internet locations. I designed and ordered printed 25,000 postcards (Figure 14). These included the

Figure 14: The front of the postcard sent out to advertise the Phase 2 survey included the Carnegie Mellon colors and seal, to bolster its credibility. The backside linked to our website, for those who wanted to check it out further.

Carnegie Mellon logo and briefly described us and our work. A QR code and a short URL were provided for recipients to access the survey file at cmu.qualtrics.com, along with a separate link to view information online at our project website, socialcybersecurity.org, without visiting Qualtrics.

To manage printing and sending the postcards, I contracted with the CMU Print Production Center, also known as Tartan Ink. This qualified us to use the CMU discount rate for bulk mailings. The program that I used to select postal routes is the USPS Every Door Direct Mail service. I used their online portal to obtain a list of postal routes for ZIP codes for each of the 12 Metropolitan Statistical Areas used in Phase 1 (Table 4), then I copied these to a spreadsheet and randomized the list, selecting the first 10-15. Participants who receive the mailing and complete the survey were entered in a drawing for one of five $50 e-gift cards. We estimated a response rate of between 0.5% and 2%, based on marketing experiences and other research.

The postcards were mailed between Jan. 24 and Feb. 25, 2022. For three weeks, the Qualtrics survey received 1-5 responses per day, for a total of N=50 completed responses. This was a response rate of 0.2%, below my target. Many surveys were abandoned partway through. This was evidence to me that the survey was too long. Another factor in the low rate of completed surveys may be the national situation during the time of the mailing. The Omicron variant was causing spikes in COVID-19 cases and hospitalizations, and many households were dealing with uncertain school schedules and managing individual quarantines and sicknesses.

5.1.1.3 Qualtrics Recruitment. Because of the failed postcard recruitment, I contracted with Qualtrics in mid-February to assemble a national survey panel of U.S. residents aged 18 and older. The survey was set up to hit quotas for age, gender, and income levels that match those parameters in the latest U.S. Census data available. The survey was also trimmed down to what was considered the minimum of variables needed to answer the research questions. Compensation was handled indirectly by Qualtrics according to agreements with subcontracted vendors. Responses were collected Feb. 21-28, 2022. After processing, the survey panel resulted in a dataset of N=859 responses, which was sufficient for the analyses.

5.1.2 Procedure

In Phase 2, I designed and executed a survey algorithm to classify participants in a nationwide panel by step of adoption of password managers. I chose password managers because they are not yet in widespread and/or mandatory use, because I had collected data about adoption decisions for them from several Phase 1 participants, and because a recent study, Pearman et al. [151], was available to guide my survey design. See Appendix C for a copy of the final survey and the survey flow.

5.1.2.1 Survey Development. I developed the Phase 2 survey, first, by collecting items and scales from prior work, and second, by writing out and testing new survey items. For the first group, I modified the wording of items from prior work as needed to answer the research questions (such as by adapting the wording to security practices). For the second group, I iteratively tested them with pilot surveys on Amazon Mechanical Turk, in which the crowd workers were asked to comment on the items' clarity and on the flow of the item ordering. I also circulated a Google doc with the lists of candidate survey items to collaborators and to other lab members for comment.

The main survey was designed to be comprehensive, yet able to be answered in 12-15 minutes. For the final version administered to the Qualtrics panel, I also inspected its look and feel on mobile to

ensure that participants could complete it on a phone. It was structured to answer the following research questions and test the following hypotheses:

- ***RQ1-2:*** *Does a survey algorithm exist that can classify participants into one and only one step of security practice adoption?*
- ***RQ2-2:*** *What is the distribution of these steps in a U.S. sample?*
- ***H1-2:*** *Authority influences and peers/media influences will significantly associate with evidence of an adoption decision.*
- ***H2(a)-2:*** *Trialability will be positively associated with adoption of a tool-based security practice.*
- ***H2(b)-2:*** *Troubleshooting help will be positively associated with adoption of a tool-based security practice.*

Pearman [151] makes a distinction between password managers that are separately installed (an add-on app such as 1Password, LastPass, or Keeper) and those that are built-in (such as password memorization and generation features of the Google Chrome web browser or the Apple iOS operating system). I chose to randomly assign participants to either Group A ("a separately installed password manager") or to Group B ("a built-in password manager") to allow me to control for type of password manager and to compare findings between these two groups.

5.1.2.2 Item Tree to Classify Participants. To create a way to classify participants by the steps identified in Phase 1, I looked to the methods used in research guided by the Transtheoretical Model (TTM) and by Diffusion of Innovations (DoI).

Figure 15: The item tree programmed into the Phase 2 Qualtrics survey, to classify participants into steps of adoption of password managers.

For the TTM, studies have commonly used six months as the cutoff between the stages of Action and Maintenance, with less than six months being considered as Action, and six months or more being considered Maintenance [95,119]. I included this as the cutoff in my own tree (Figure 15). The TTM also distinguishes between the stages of Contemplation, when people are hesitant to adopt the action, and

Preparation, when people are willing to adopt but have not yet acted [69]. I included follow-up questions to distinguish these two types of reasons for not yet adopting.

As for DoI, its Innovation-Decision Process Model accounts for non-adoption either before Implementation (termed Rejection) or after Implementation (termed Discontinuance) [168]. I accounted for this distinction with an additional level of the tree for non-adopters that asks if they had ever used password managers before. Based on the Phase 1 interview data, along with my knowledge of usable security and prior research, I created two additional types of non-adoption, Ignorance (when someone does not know about the security practice) and Non-Engagement (when someone knows about the security practice but simply doesn't care about it). The DoI also famously categorizes those who are in Maintenance by their time from Implementation, with the earliest being called Innovators, followed by Early Adopters, Early Majority, Late Majority, and (for the most established innovations) Laggards. I devised an item to ask survey respondents their time from Implementation to approximate this scale.

Finally, I added items that were not considered in TTM or DoI research: about participants' perceptions of harms that password managers may pose [6], along with threats that password managers can guard against. The item tree is summarized in Figure 15 (above), and the items are listed in Table 9.

Table 9: The exact questions used in the Phase 2 Qualtrics survey to split people into steps. The program code snippet `${e://Field/PM_type}` is used in the text where the program inserts either the string "a built-in password manager" or the string "a separately installed password manager," depending on their random group assignment.

Classification step	Item(s)	Text of item(s)	Response(s)
Step 3: Practice Implementation	Q5.1	Currently, are you using `${e://Field/PM_type}`?	Yes (1)
(Adoption within last six months)	Q6.1	How long have you been using `${e://Field/PM_type}`?	Less than six (6) months
Step 4: Practice Maintenance	Q5.1	Currently, are you using `${e://Field/PM_type}`?	Yes (1)
(Adoption for six months or longer)	Q6.1	How long have you been using `${e://Field/PM_type}`?	Six (6) months or longer (2)
Step X: Practice Rejection (a)	Q5.1	Currently, are you using `${e://Field/PM_type}`?	No (2)
(Discontinuance)	Q5.2	Have you ever used `${e://Field/PM_type}`?	Yes (1)
Step X: Practice Rejection (b)	Q5.1	Currently, are you using `${e://Field/PM_type}`?	No (2)
	Q5.2	Have you ever used `${e://Field/PM_type}`?	No (2)
(Decision not to adopt)	Q5.3	Which statement best fits your situation?	I have heard of `${e://Field/PM_type}`, but I decided not to use it (4)
Step 2: Security Learning	Q5.1	Currently, are you using `${e://Field/PM_type}`?	No (2)
	Q5.2	Have you ever used `${e://Field/PM_type}`?	No (2)
(No decision about adoption)	Q5.3	Which statement best fits your situation?	I have heard of `${e://Field/PM_type}` and am willing to use it, but so far have not put it into practice (2)
			I have heard of `${e://Field/PM_type}`, but I am hesitant to use it (3)

Classification step	Item(s)	Text of item(s)	Response(s)
Step 1: Threat Awareness	Q5.1	Currently, are you using `${e://Field/PM_type}`?	No (2)
	Q5.2	Have you ever used `${e://Field/PM_type}`?	No (2)
(Not thinking about adoption)	Q5.3	Which statement best fits your situation?	I never heard of `${e://Field/PM_type}` before this survey (1)
			I have heard of `${e://Field/PM_type}`, but I forgot it existed until now (5)
(Aware of threats that the practice guards against)	Q7.6	Are you aware of any threats to your online data or accounts that can be dealt with by using `${e://Field/PM_type}`?	Yes (1)
Step 0: No Learning or Threat Awareness	Q5.1	Currently, are you using `${e://Field/PM_type}`?	No (2)
	Q5.2	Have you ever used `${e://Field/PM_type}`?	No (2)
(Not thinking about adoption)	Q5.3	Which statement best fits your situation?	I never heard of `${e://Field/PM_type}` before this survey (1)
			I have heard of `${e://Field/PM_type}`, but I forgot it existed until now (5)
(Not aware of threats that it guards against)	Q7.6	Are you aware of any threats to your online data or accounts that can be dealt with by using `${e://Field/PM_type}`?	No (2)

5.1.2.3 Additional Items. To create a way to determine the significant predictors of a step, I asked participants to select all the reasons that applied to why they had answered as they did (Table 10). The closed-ended response set (20 for the non-adoption stems and 21 for the adoption stems) included items about understanding of the practice, resistance to the practice, perceived usability, trialability, the practice's relative advantage versus other solutions, troubleshooting availability, other social influences such as advice, and the availability of affordances for the practice. The "Other" open-ended response allowed participants to type in something that was not on the list.

Table 10: The exact questions used in the Phase 2 Qualtrics survey to measure covariates for each step. The program code snippet `${e://Field/PM_type}` is used in the text where the program inserts either the string "a built-in password manager" or the string "a separately installed password manager," depending on their random group assignment

Covariate	Item(s)	Text of Item(s)	Response(s)
Understanding/ Know-How	Q5.4	Why do you not currently use it? Check all that apply.	I don't understand how to use it (1)
			I don't understand how it works (2)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	I understand how to use it (1)
			I understand how it works (2)
			Was able to set it up (10)

Covariate	Item(s)	Text of Item(s)	Response(s)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	I understood how to use it (1)
			I understood how it works (2)
			Was able to set it up (10)
Perceived Importance	Q5.4	Why do you not currently use it? Check all that apply.	I don't think it is important (3)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	Because it is important (3)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	Because it is important (3)
Perceived Usability	Q5.4	Why do you not currently use it? Check all that apply.	It's inconvenient (4)
			It's difficult to use (5)
			It doesn't seem currently useful (6)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	It's convenient (4)
			It's easy to use (5)
			It seems useful (6)
			Was able to set it up (10)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	It was convenient (4)
			It was easy to use (5)
			It seemed useful (6)
			Was able to set it up (10)
Relative Advantage	Q5.4	Why do you not currently use it? Check all that apply.	I'm already using something that I like better (7)
			I tried something else I like better (9)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	Better than something else I used to use regularly (8)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	Was better than something else I used to use regularly (8)
Trialability	Q5.4	Why do you not currently use it? Check all that apply.	I tried it and didn't like it (8)
			I tried something else I like better (9)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	I tried it and liked it (7)
			Was able to try it out first (9)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	I tried it and liked it (7)
			Was able to try it out first (9)

Covariate	Item(s)	Text of Item(s)	Response(s)
Troubleshooting Help	Q5.4	Why do you not currently use it? Check all that apply.	I couldn't find someone to help me with it (10)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	Found someone to help me with it (11)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	Found someone to help me with it (11)
Affordance	Q5.4	Why do you not currently use it? Check all that apply.	New computing device doesn't support it (11)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	Computing device supports it (12)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	Computing device supported it (12)
Mandatoriness	Q5.4	Why do you not currently use it? Check all that apply.	I'm not required to use it (12)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	I'm required to keep using it (14)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	I was required to start using it (14)
Received Advice	Q5.4	Why do you not currently use it? Check all that apply.	Someone I trust told me not to use it (13)
			I heard or saw advice not to use it (14)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	Someone I trust told me to keep using it (15)
			I heard or saw advice to keep using it (16)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	Someone I trust told me to start using it (15)
			I heard or saw advice to start using it (16)
Received Reminders	Q5.4	Why do you not currently use it? Check all that apply.	I forgot about it (15)
	Q6.2	Why do you keep using `${e://Field/PM_type}`? Check all that apply.	I get notifications about it (13)
	Q6.4	Why did you start using `${e://Field/PM_type}`? Check all that apply.	I get notifications about it (13)

To create a way to differentiate steps by social influences, I either wrote or adapted existing items from other surveys and published scales that could be computed as interval variables. I wrote items that could be averaged to create an Educating Others scale, based on the Phase 1 interview data, to test caretaking behaviors. I also adapted items from the Rogers Adoption Leader scale [168] to test security leadership behaviors. I adapted items from the Moore-Benbasat scales for perceived innovation characteristics [144] to test perceptions of the image of password managers and of their visibility and availability to try out. I asked questions about whether a close tie had frequently experienced online security breaches in the past year and also whether they had frequently heard or seen news about such

breaches [70]. These tested the influence of these social experiences on their step of adoption of password managers.

To test the influence of individual characteristics on the steps of adoption, I collected the following variables: Internet Know-How [115], age range, gender identity, Hispanic/Latinx/Spanish identity, racial/ethnic identity, household size, income range, level of education, experience working with sensitive data, and their amount of computer science/information science education or job experience.

Finally, I collected responses for the security-adapted University of Rhode Island Change Assessment (URICA) scales. These are used in research motivated by the Transtheoretical Model to assess a person's Stage of Change. I used these to assess the convergent validity of the Step Classification instrument.

5.1.3 Analysis

For the Phase 2 surveys, I downloaded datasets from the Qualtrics online survey software[7]. The collected datasets were cleaned by deleting seemingly bad-faith responses that had not been caught by the programming checks for fraud and low-quality responses. As in Phase 1, bad-faith responses included those to open-ended questions that were gibberish, those that seemed as if they had been copy-pasted from elsewhere, or those that did not follow directions. An attention-check question directed participants to respond with answer 4; all other responses led to rejection of the data. The last step in processing this data was to run a factor analysis and reliability analysis for each set of collected scale items, such as for the Rogers Adoption Leader scale. Items were discarded if they did not factor as expected with the others and/or if the item deletion would improve the Cronbach's alpha of the scale (minimum to include = .70). Scale means were computed only for the sets of items that passed both checks. See Appendix E for the full list of collected scales and their Cronbach's alpha scores.

In the Phase 2 main survey, the Step Classification was computed by using Boolean terms to join answers to specific item questions and then coding the Step Classification as 1 if a number was returned from those terms, else 0. To answer RQ1, I graphed the histogram of the Step Classifications in the sample. To answer RQ2 and to help answer the hypotheses, I then used this Step Classification as a binary "dependent" or "outcome" variable for a series of statistical analyses of their associations with other variables. (Note that this is a cross-sectional study, so there is no ability to test for cause and effect as with a longitudinal study or an experiment.) The goal of the logistic regressions was to determine which selected variables were significantly associated with someone's odds of being classified in each step. I conducted these stepwise, first testing only for the effect of the type of password manager (where 0 = "a built-in password manager" and 1 = "a separately installed password manager") and for awareness of the risks of using password managers (where 0 = not aware of any risks and 1= aware of at least some risks), then adding in the selected variables on the last step. The last-step model was judged better than the previous models if the -2 Log likelihood statistic was the lowest [101]. The goal of the analyses of variance were, first, to determine whether a significance difference exists among means of an interval variable for participants in different steps; and second, to use post-hoc tests to determine which pairwise comparisons were significant (adjusted for multiple comparisons). The same methods were used for hypotheses testing except for H1, which was tested using a check of the survey dataset and an analysis of

[7] https://www.qualtrics.com/

variance of the steps with a scale to measure TTM Action/Maintenance, which I adapted from the University of Rhode Island Change Assessment (URICA).

See Appendix F for the survey codebook, which includes directions for computing the Step Classification and definitions and/or equations for all variables in the dataset.

5.2 Results

To recap from above: In Phase 2, I designed and executed a survey algorithm to classify participants in a nationwide panel by step of adoption of password managers. I chose password managers because they are not yet in widespread and/or mandatory use, because I had collected data about adoption decisions for them from several Phase 1 participants, and because a recent study, Pearman et al. [151], also was available to guide my survey design. For the step-classification algorithm, I added two steps that represent obstacles: No Learning or Threat Awareness (Step 0), and Security Practice Rejection (Step X).

See Section 5.2.1 for the sample characteristics, Section 5.2.2 for results for the two research questions and three hypotheses generated after Phase 1, and Section 5.2.3 for results of the exploratory analyses of step-specific covariate associations and variances.

5.2.1 Sample Characteristics

I received *N*=859 responses from the survey panel that I judged reliable and valid. A little less than half were completed on an iPhone operating system (409), followed by devices running versions of Windows NT (264), Android (250), Macintosh (43), iPad (15), ChromeOS (7), or the "wv" library's cross-platform operating system (1). The top five web browsers in use were Safari iPhone (402), Chrome (345), Edge (42), Safari other than iPhone (30), and Firefox (13). The sample skewed toward higher education and higher education levels, perhaps due to its administration to the Qualtrics third-party panels. This suggests the results will generalize to many corporations and government agencies, but perhaps not for generalizability to people not engaged in white-collar occupations. See Tables 11-12 for the sample's demographics, socio-economic metrics and relevant prior experiences.

Table 11: Demographics of the Phase 2 survey panel participants (*N*=859).

Age		Gender		Hispanic/Latinx		Race/ethnicity		Household size	
192	18-29	406	Male	173	Yes	628	White or Caucasian	122	Only them
220	30-39	443	Female	684	No	100	Black or African American	225	Two
150	40-49	9	Nonbinary	2	Prefer not to say	11	Native American or Alaska Native	171	Three
149	50-59	1	Prefer not to say			16	Asian - East or Central	125	Four
148	60 or older					21	Asian - South, Southeast, or Southwest	95	Five or more
						1	Native Hawaiian or Pacific Islander	121	Did not say
						1	Middle Eastern or North African		
						58	Prefer to self-describe		
						23	Prefer not to say		

Table 12: Socio-economic metrics and relevant prior experiences for the Phase 2 survey panel participants (*N*=859). "SD" stands for Sensitive Data, which, in the U.S., is governed by regulations such as HIPAA or FERPA.

Income		Education		Exp. Working w/ SD		Computer/Information Science Experience	
94	Up to $25,000	19	Some high school	382	None at all	92	I both earned a degree in such a field and have worked or am working in it.
265	$25,000 to $49,999	158	H.S. degree or equivalent	151	A little	61	I earned a degree in such a field, but never worked in it.
195	$50,000 to $74,999	330	Some college /associate's	165	A moderate amount	151	I did not earn a degree in such a field, but I have worked or am working in one.
139	$75,000 to $99,999	230	Bachelor's degree	79	A lot	555	I did not earn a degree in such a field, nor did I ever work in one.
166	$100,000 or more	122	Graduate/ professional	82	A great deal		

5.2.2 Phase 2 Research Questions and Hypothesis Testing

Overall: I confirmed the Phase 1 findings that trialability, troubleshooting help, and mandates are significantly associated with Step 3, and that leadership and caretaking are significantly associated with Step 4. I found that peer and media influences are significantly associated with Step X. Table 13 and Table 14 summarize these results, along with the sub-sections where the findings are detailed.

Table 13: Based on the results of the quantitative analysis of Phase 2 survey data, both research questions from Phase 1 were answered, and all three hypotheses from Phase 1 were retained.

Research Question or Hypothesis from Phase 1	ID	Results	Sub-section
Does a survey algorithm exist that can classify participants into one and only one step of security practice adoption?	RQ1-2	Answered.	5.2.2.1
What is the distribution of these steps in a U.S. sample?	RQ2-2	Answered.	5.2.2.2
Authority influences and peers/media influences will significantly associate with evidence of an adoption decision.	H1-2	Retained.	5.2.2.3
Trialability will be positively associated with adoption of a tool-based security practice.	H2(a)-2	Partly Retained.	5.2.2.4
Troubleshooting help will be positively associated with adoption of a tool-based security practice.	H2(b)-2	Retained.	5.2.2.5

5.2.2.1 Algorithm to Classify Participants by PM Adoption Step. I found that the survey participants (*N*=589) could be classified into six steps according to the item tree (Figure 16), with no person classified into two steps at once or lacking a step classification. In the item tree, the first question sorts people into two groups: adopters and non-adopters. From there, adopters are classified in Step 4: Maintenance or Step 3: Implementation, according to whether they have adopted the practice earlier than six months. Non-adopters are grouped into Step X: Rejection if they indicate that they decided not to use the security practice, either before or after using it at least once. Those who have reached no decision yet on adoption, stating that they are either willing to act or hesitant to act, are classified in Step 2: Security Learning. Finally, those who give ignorance or non-engagement as a reason that they haven't acted are classified either in Step 1: Threat Awareness or Step 0: No Learning or Threat Awareness, according to whether they are aware of threats that the security practice guards against.

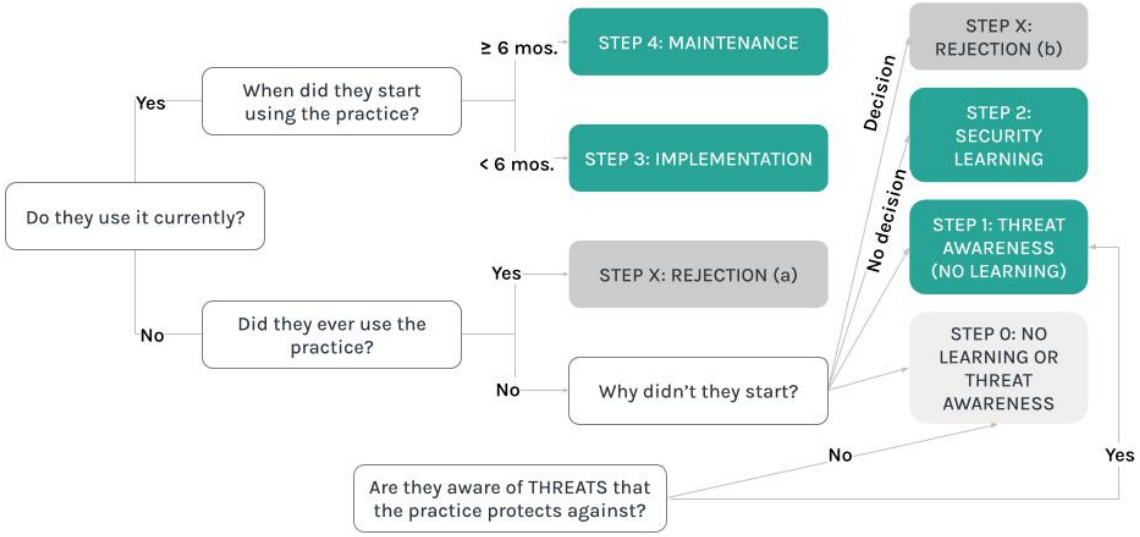

Figure 16: The final item-tree diagram showing how Phase 2 participants were classified into each step.

A two-step cluster analysis of the tree items (excluding Threat Awareness) found very similar results, showing (1) that the single item asking adopters whether their start was at least six months ago was a good fit to segment those participants into an optimal two clusters, and (2) that the first two items asked of non-adopters were a good fit to segment those into an optimal three clusters.

I also tested the association of the step levels with mean scores on scales adapted from the University of Rhode Island Change Assessment (URICA) to classify participants by Stage of Change in the Transtheoretical Model (TTM). An analysis of variance shows that a significant difference exists among mean scores by step on the adapted URICA scale for TTM Action/Maintenance (Figure 17): $F(5,853) = 44.915$, $p<.001$. Further, an estimated 20.8% of the variance in the TTM Action/Maintenance scale is accounted for by the six-level step classification variable: $\eta^2=.208$ (95% CI: .159, .250) [101]. A significant difference among mean scores by step also exists for the composite URICA scale, which includes items for TTM Precontemplation and Contemplation/Preparation (Figure 18): $F(5,853) = 12.964$, $p<.001$, $\eta^2=.071$ (95% CI: .037, .101). For both measures, the direction of association is positive overall.

- ***The step-classification algorithm demonstrates reliability and convergent validity.***

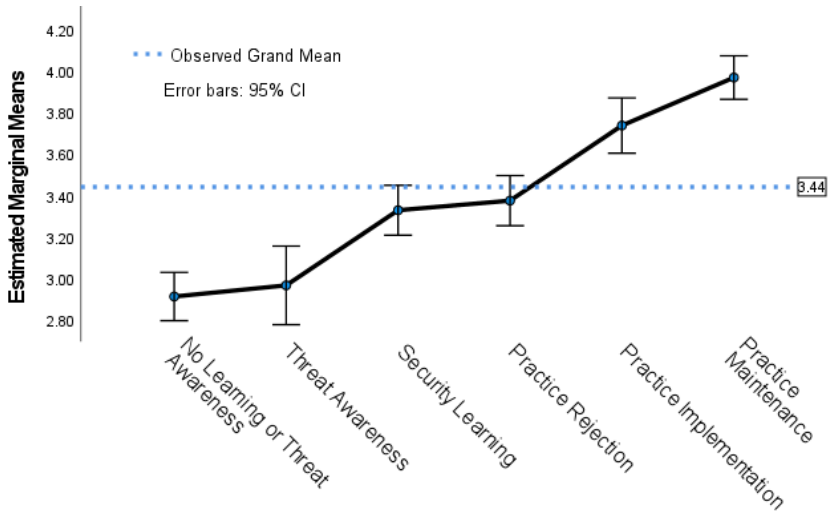

Figure 17: Estimated marginal means of the URICA scale for TTM Action/Maintenance. This represents the URICA mean for each level of the ordinal variable representing the Steps of Security Behavior Adoption. Scores on this scale increase with Steps 0-4 (i.e., all except for Practice Rejection). This is expected and evidence of the Step Classification algorithm's validity.

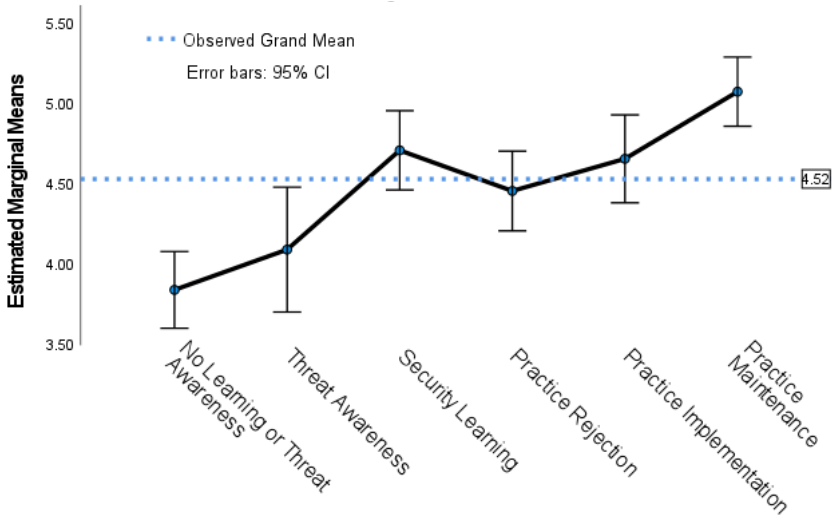

Figure 18: Estimated marginal means of the composite URICA scale for each level of the ordinal variable representing the Steps of Security Behavior Adoption. This URICA scale adds items for TTM Precontemplation and Contemplation/Preparation to TTM Action/Maintenance. Scores on this scale increase with Steps 0-2 before the adoption decision (No Learning or Threat Awareness, Threat Awareness, and Security Learning) and rise again afterward consistent with increases in use duration for Steps X, 3 and 4 (Practice Rejection, then Practice Implementation and Practice Maintenance).

5.2.2.2 Distribution of PM Adoption Steps. About two in five participants (*n*=327, 38.1%) were classified into Step 3 (*n*=125) or Step 4 (*n*=202), indicating that they are currently using a password manager (either built-in or separately installed). One in four participants (*n*=216, 25.1%) fell into pre-adoption, Step 1 (*n*=62) and Step 2 (*n*=154). One in five (*n*=164, 19.1%) had not entered the adoption process, being in Step 0. The rest (*n*=152, 17.7%) had rejected adoption, Step X. See Figure 19 for the comparison by step.

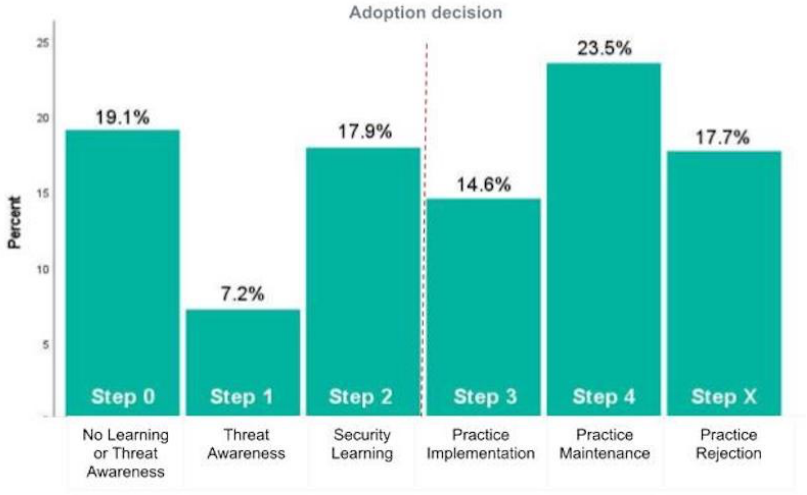

Figure 19: A chart of the step distribution in the Phase 2 Qualtrics survey panel (*N*=859, *M* = 2.69, *Mdn* = 3.00, *SE* = 0.06). Those in Step 4 are the largest subset, followed by those in Step 0. Relatively few are classified in Step 1, perhaps reflecting that Threat Awareness rapidly leads to other steps.

5.2.2.3 Social Influences Significantly Associate with Steps 3-4, X. I next tested H1-2: "Authority influences and peers/media influences will significantly associate with evidence of an adoption decision," using logistic regression. For "evidence of an adoption decision," I used participants' classification into either Step 3: Practice Implementation, Step 4: Practice Maintenance, or Step X: Practice Rejection. Unless otherwise noted, I controlled for the type of password manager (either built-in or separately installed) and for whether they perceived risks in using password managers (such as establishing a single point of failure).

For Steps 3-4: Those with high scores on the Moore-Benbasat "Image" scale, adapted to password managers, were 1.4 times more likely to be in adoption, either Step 3 or Step 4 (OR = 1.366 [95% CI: 1.172, 1.593], p<.001, Nagelkerke R^2 = .134). Participants were 4.5 times more likely to be in Step 3 if they were "required to start using it [a password manager]" (OR = 4.500 [95% CI: 1.761, 11.501], p=.002, Nagelkerke R^2= .031), as were those with high scores on the Moore-Benbasat "Visibility/Trialability" scale (OR = 2.160 [95% CI: 1.693, 2.757], p<.001, Nagelkerke R^2 = .085) and those who "found someone to help me with it" (OR = 8.023 [95% CI: 2.099, 30.664], p=.002, Nagelkerke R^2= .031). Participants were significantly more likely to be in Step 4 if they "heard or saw advice to start using it" or if they were "required to start using it" (Overall model $x^2(19)$ =684.422, p<.001, Nagelkerke R^2= .827).

For Step X: Participants were 4.1 times more likely to reject adoption of a password manager (either before or after Step 3) if they selected that "someone I trust told me not to use it" (OR = 4.125 [95% CI: 1.351, 12.591], p=.013, Nagelkerke R^2=.030). They also were 2.6 times more likely to do so if they selected "I'm not required to use it" (OR = 2.634 [95% CI: 1.610, 4.310], p<.001, Nagelkerke R^2=.044), and 5.9 times more likely if they selected "I couldn't find someone to help me with it" (OR = 5.913 [95% CI: 2.335, 14.976], p<.001, Nagelkerke R^2=.044). Participants were 7.1 times more likely to reject

adoption before Step 3 if they "heard or saw advice not to use it" (OR = 7.104 [95% CI: 1.393, 36.232], p=.018, Nagelkerke R^2=.036).

These results lead me to REJECT the null hypothesis that no such association exists among social influences and evidence of an adoption decision.

- ***H1-2 is Retained.***

5.2.2.4 Trialability Significantly Associates with Steps 3, X. I next tested H2(a)-2: "Trialability will be positively associated with adoption of a tool-based security practice," using logistic regression. For "adoption," I used participants' classification into Step 3: Practice Implementation. I also tested the relationship of the Phase 2 covariates that mention trialability with Step X: Practice Rejection. In this case, the covariates help determine support for the null hypothesis that a positive association exists between trialability and *non*-adoption. Unless otherwise noted, I controlled for the type of password manager (either built-in or separately installed) and for whether they perceived risks in using password managers (such as establishing a single point of failure).

For Step 3: Participants with high scores on the Moore-Benbasat "Visibility/Trialability" scale, adapted to password managers, were 2.2 times more likely to have adopted them (OR = 2.160 [95% CI: 1.693, 2.757], p<.001, Nagelkerke R^2 = .085).

For Step X: Participants were 79.9 times more likely to reject adoption of a password manager (either before or after Step 3) if they selected that "I tried it and didn't like it" (OR = 79.864 [95% CI: 18.667, 341.681], p<.001, Nagelkerke R^2=.174), and 15.5 times more likely if they selected "I tried something else I like better" (OR = 15.452 [95% CI: 4.150, 57.531], p<.001, Nagelkerke R^2=.058).

These results lead me to REJECT the null hypothesis that no association exists between trialability and adoption of a tool-based security practice. However, I found support for the null hypothesis that a positive association exists between trialability and (non)adoption of a tool-based security practice. This indicates that, in this survey panel, trialability needs usability and relative advantage present to be predictive of adoption. It also supports that trialability is useful for moving people beyond Step 2: Security Learning, to an adoption decision.

- ***H2(a)-2 is Partly Retained.***

5.2.2.5 Troubleshooting Help Significantly Associates with Steps 3, X. Lastly, I tested H2(b)-2: "Troubleshooting help will be positively associated with adoption of a tool-based security practice," using logistic regression. For "adoption," I used participants' classification into Step 3: Practice Implementation. I also tested the relationship of the Phase 2 covariates for troubleshooting help with Step X: Practice Rejection. In this case, the covariates help determine support for the alternative hypothesis by representing the inverse of H2(b)$_2$: that a *lack* of troubleshooting help will be positively associated with *(non)*adoption. Unless otherwise noted, I controlled for the type of password manager (either built-in or separately installed) and for whether they perceived risks in using password managers (such as establishing a single point of failure).

For Step 3: Participants were 8.0 times more likely to have adopted a password manager if they "found someone to help me with it" (OR = 8.023 [95% CI: 2.099, 30.664], p=.002, Nagelkerke R^2 = .031).

For Step X: Participants were 5.9 times more likely to have rejected adopting a password manager if they "couldn't find someone to help me with it." (OR = 5.913 [95% CI: 2.335, 14.976], p<.001, Nagelkerke R^2=.044).

These results lead me to REJECT the null hypothesis that no association exists between troubleshooting help and adoption of a tool-based security practice. I also REJECT the null hypothesis that a non-positive association exists between a lack of troubleshooting help and (non)adoption of a tool-based security practice. This indicates that, in this survey panel, the existence of troubleshooting help is predictive of adoption, and that the lack of such help is predictive of the rejection of adoption.

- ***H2(b)-2 is Retained.***

5.2.3 Step-Specific Exploratory Findings and Insights

I next computed the step-specific models of logistic regression for each collection of covariates or "reasons given." I also analyzed the associations and variances among each step and the other interval and categorical variables. The results are summarized in Table 13.

Table 14: For each listed Phase 2 covariate, the practical significance of the step-specific statistical analysis is summarized as either a Decreased amount of data is significantly associated with the step, or an Increased amount of data is significantly associated with the step. Where (n.s.) is indicated, no statistically significant association was detected.

		Non-Adoption				Adoption	
Sub-section	Covariates	Step 0	Step 1	Step 2	Step X	Step 3	Step 4
Reasons Given, 5.2.3.1 and 5.2.3.2	Understanding / Know-How	Decreased	Decreased	Decreased	Increased	Increased	Increased
	Perceived Importance	(n.s.)	(n.s.)	(n.s.)	Decreased	Increased	Increased
	Perceived Usability	(n.s.)	(n.s.)	(n.s.)	Decreased	Increased	Increased
	Relative Advantage	(n.s.)	(n.s.)	(n.s.)	Decreased	(n.s.)	(n.s.)
	Trialability	(n.s.)	(n.s.)	(n.s.)	Increased	Increased	Increased
	Troubleshooting Help	(n.s.)	(n.s.)	(n.s.)	Decreased	Increased	Increased
	Affordance	(n.s.)	(n.s.)	(n.s.)	(n.s.)	Decreased	Increased
	Mandatoriness	Decreased	(n.s.)	Decreased	Decreased	Increased	Increased
	Received Advice	(n.s.)	(n.s.)	(n.s.)	Increased	(n.s.)	Increased
	Received Reminders	(n.s.)	(n.s.)	(n.s.)	Decreased	(n.s.)	Decreased
	Other	Increased	Increased	(n.s.)	Increased	(n.s.)	(n.s.)
Social Factors, 5.2.3.3	Adoption Leader	Decreased	Decreased	(n.s.)	(n.s.)	Increased	Increased
	Educating Others	Decreased	Decreased	(n.s.)	(n.s.)	Increased	Increased
	Image	(n.s.)	(n.s.)	(n.s.)	(n.s.)	Increased	(n.s.)
	Visibility/Trialability	Decreased	Decreased	Decreased	(n.s.)	Increased	Increased
	Breach Exposure - Personal	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)
	Breach Exposure - Close Tie	Decreased	(n.s.)	(n.s.)	(n.s.)	Increased	(n.s.)
	Breach Exposure - Heard/Seen	Decreased	(n.s.)	(n.s.)	(n.s.)	(n.s.)	Increased
Individual Factors, 5.2.3.4	Internet Know-How	Decreased	Decreased	(n.s.)	Increased	Increased	Increased
	Age Under 40	(n.s.)	Decreased	Decreased	(n.s.)	Increased	Increased
	Female Identity	Increased	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)
	Hispanic/Latinx/Spanish Identity	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)
	Non-White and/or Non-Caucasian	Increased	(n.s.)	(n.s.)	(n.s.)	Decreased	(n.s.)
	3 or More in Household	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)
	Income Below $25,000/Year	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)
	4-year College Degree or More	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)	(n.s.)
	No Experience Working with Sensitive Data	Increased	Increased	(n.s.)	(n.s.)	Decreased	Decreased
	No Experience with Computer or Info. Science	Increased	Increased	(n.s.)	(n.s.)	Decreased	Decreased

NOTE: Social Factors adjusted alpha for pairwise comparisons set at 0.01, Individual Factors adjusted alpha for pairwise comparisons set at 0.005.

5.2.3.1 Reasons Given for Non-Adoption. All participants who were classified into Steps 0-2 and X were asked (1) to select all that applied from the same set of 20 possible reasons for not using a password manager, including an "Other" write-in option, and then (2) to select which was the most important reason for their non-adoption. Using the first set of reasons, I computed logistic regressions to determine which of the selected reasons were significantly associated with being classified in each step of non-adoption, controlling first for type of password manager and for awareness of usage risks. The results are summarized below, with tables shortened to only the control variables and the significant predictors.

Step 0: No Learning or Threat Awareness. The variable most strongly and significantly positively associated with Step 0 was "I don't understand how to use it," which 60 in Step 0 also cited as the most important reason they didn't use password managers (Figure 20). For "Other," 17 participants said that they were not aware of password managers. Participants were less likely to be in Step 0 if they perceived risks in using password managers, perhaps because this implies that they had learned enough to have progressed to a different step. Table 15 model statistics: x^2 (18) = 173.471, p<.001, Nagelkerke R^2 = .294.

- ***Lack of understanding, of mandatoriness, and of awareness of password managers were associated with Step 0.***

Table 15: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 0: No Learning or Threat Awareness. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	0.074	0.202	0.133	1	0.716	1.076	0.725	1.599
PM risk perception(1)	-1.864	0.534	12.173	1	<.001	0.155	0.054	0.442
I don't understand how to use it(1)	2.174	0.244	79.263	1	<.001	8.798	5.451	14.199
I'm not required to use it(1)	1.075	0.297	13.09	1	<.001	2.93	1.637	5.245
Other reason:(1)	2.021	0.348	33.669	1	<.001	7.543	3.812	14.926

a. Variable(s) entered on step 1: I don't understand how to use it, I don't understand how it works, I don't think it is important, It's inconvenient, It's difficult to use, It doesn't seem currently useful, I'm already using something that I like better, I tried it and didn't like it, I tried something else I like better, I couldn't find someone to help me with it, New computing device doesn't support it, I'm not required to use it, Someone I trust told me not to use it, I heard or saw advice not to use it, I forgot about it, Other reason:.

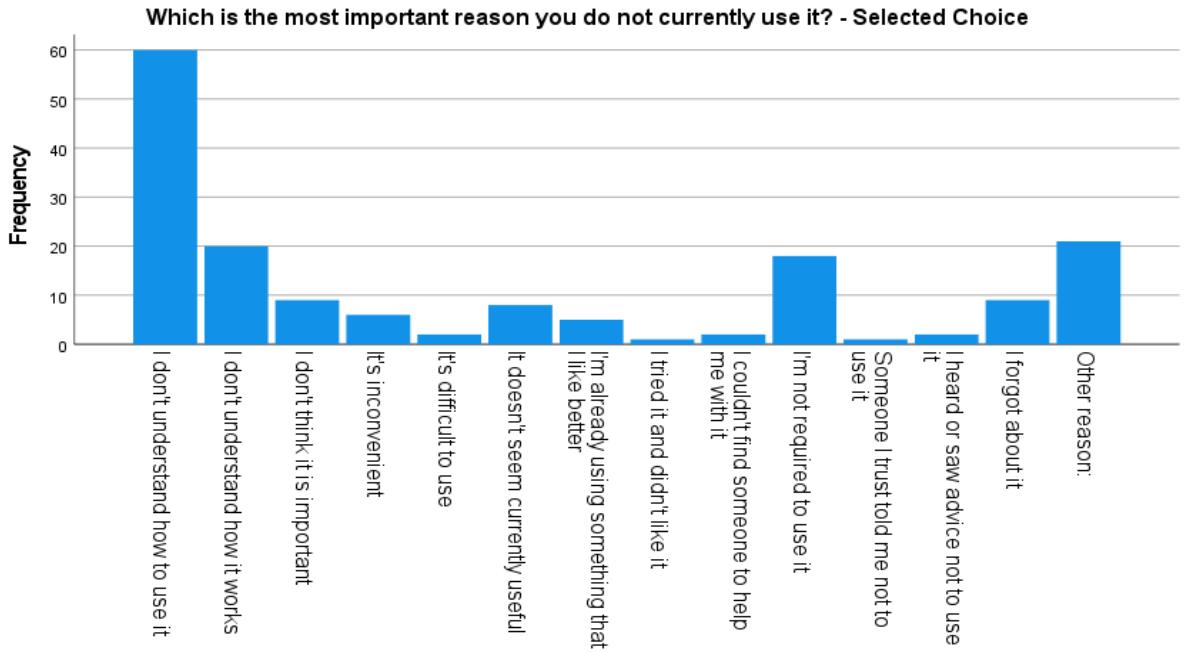

Figure 20: In Step 0, lack of understanding of how to use password managers was the most cited reason for not using them.

Step 1: Threat Awareness. Here again, the variable most strongly and significantly positively associated with Step 1 was "I don't understand how to use it," which 25 people in Step 1 also cited as the most important reason they didn't use password managers (Figure 21). For "Other," 7 participants said that they were not aware of password managers. These results are consistent with the idea that these participants need help to move to Step 2 and learn about the security practice. Table 16 model statistics: x^2 (18) = 88.503, p<.001, Nagelkerke R^2 = .242.

- ***Lack of understanding and of awareness of password managers were associated with Step 1.***

Table 16: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 1: Threat Awareness. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-0.787	0.623	1.598	1	0.206	0.455	0.134	1.542
PM risk perception(1)	0.266	0.294	0.82	1	0.365	1.305	0.734	2.321
I don't understand how to use it(1)	1.814	0.338	28.825	1	<.001	6.133	3.163	11.891
I don't understand how it works(1)	1.076	0.349	9.519	1	0.002	2.933	1.481	5.81
Other reason:(1)	1.722	0.469	13.457	1	<.001	5.597	2.23	14.048

a. Variable(s) entered on step 1: I don't understand how to use it, I don't understand how it works, I don't think it is important, It's inconvenient, It's difficult to use, It doesn't seem currently useful, I'm already using something that I like better, I tried it and didn't like it, I tried something else I like better, I couldn't find someone to help me with it, New computing device doesn't support it, I'm not required to use it, Someone I trust told me not to use it, I heard or saw advice not to use it, I forgot about it, Other reason:.

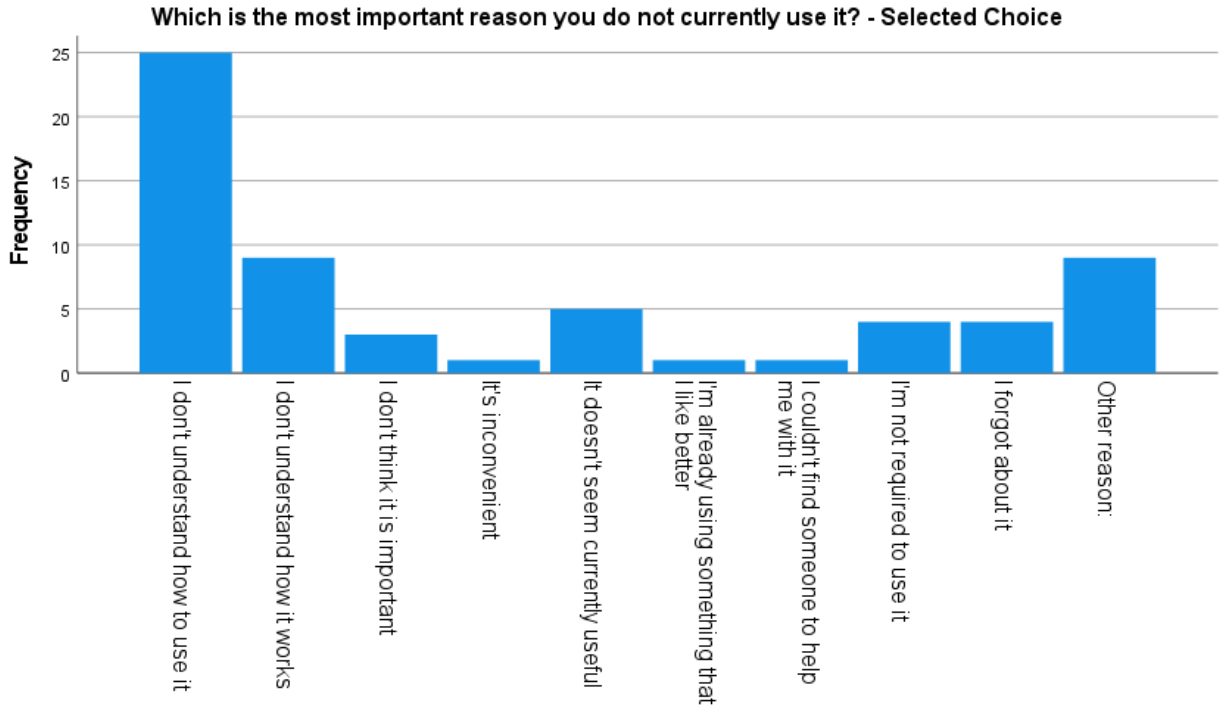

Figure 21: In Step 1, lack of understanding of how to use password managers was the most cited reason for not using them.

Step 2: Security Learning. The variable most strongly and significantly positively associated with Step 2 was "I don't understand how it works," which 60 people in Step 2 also cited as the most important reason they didn't use password managers (Figure 22). Participants were also significantly more likely to be in Step 2 if they perceived risks in using password managers. These two variables together suggest that a lack of trust in password managers holds them back from Step 3: Implementation. Table 17 model statistics: x^2 (18) = 41.581, p<.001, Nagelkerke R^2 = .124.

- ***Lack of understanding and of mandatoriness were associated with Step 2.***

Table 17: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 2: Security Learning. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-0.154	0.468	0.108	1	0.743	0.858	0.343	2.146
PM risk perception(1)	0.854	0.309	7.61	1	0.006	2.348	1.28	4.307
I don't understand how it works(1)	1.377	0.378	13.242	1	<.001	3.962	1.887	8.316
I'm not required to use it(1)	0.827	0.392	4.441	1	0.035	2.286	1.06	4.932

a. Variable(s) entered on step 1: I don't understand how to use it, I don't understand how it works, I don't think it is important, It's inconvenient, It's difficult to use, It doesn't seem currently useful, I'm already using something that I like better, I tried it and didn't like it, I tried something else I like better, I couldn't find someone to help me with it, New computing device doesn't support it, I'm not required to use it, Someone I trust told me not to use it, I heard or saw advice not to use it, I forgot about it, Other reason:.

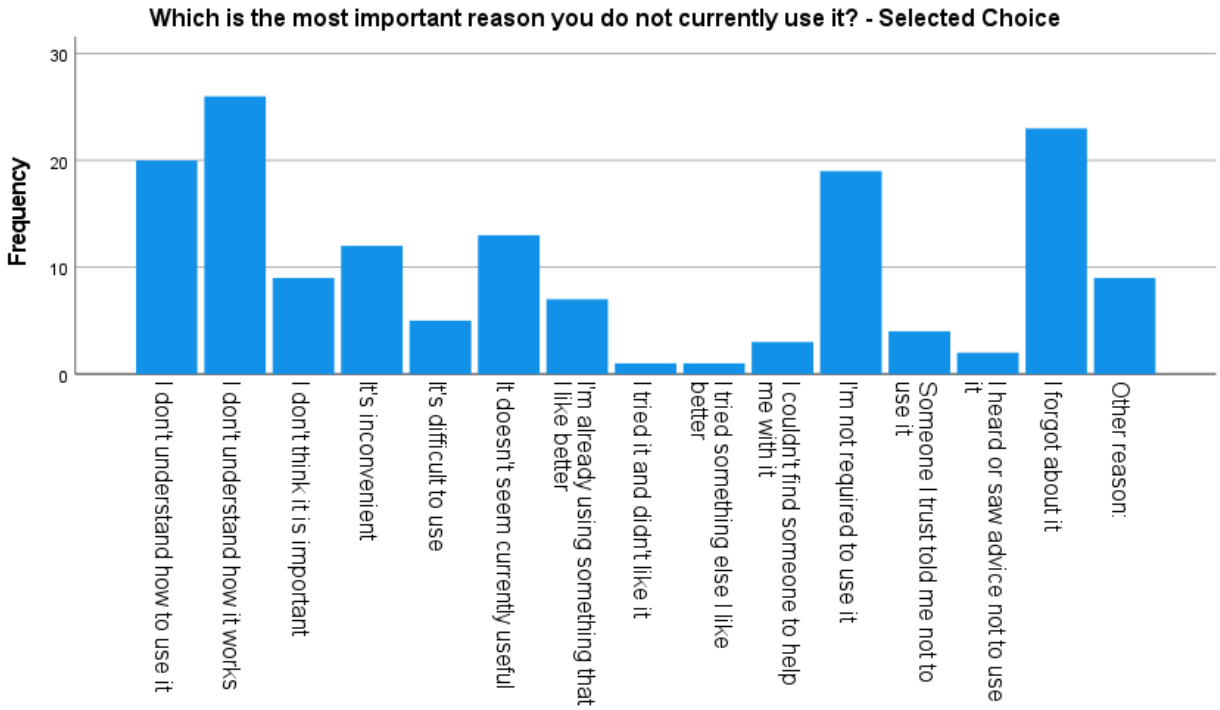

Figure 22: In Step 2, lack of understanding of how password managers work was the most cited reason for not using them.

Step X: Practice Rejection. The variable most strongly and significantly positively associated with Step X was "I tried it and didn't like it," which 16 in Step X also cited as the most important reason they didn't use password managers (Figure 23). "I tried something else I like better" was among the next-most strongly and significantly positively associated variables, as were "I couldn't find someone to help me with it," "I forgot about it," and "I heard or saw advice not to use it." However, the variable "I'm not

required to use it" was both significantly positively associated with Step X and the reason most often cited (19) as the most important reason for non-adoption, suggesting that some in this group would use a password manager if forced to. For "Other," 7 participants said that they do not trust password managers or that they do not like the technology. Participants were significantly less likely to be in Step X if they selected "I don't understand how it works." Table 18 model statistics: x^2 (18) = 262.600, p<.001, Nagelkerke R^2 = .434.

- ***Lack of mandatoriness, of a pleasing and trouble-free user experience, and of trust in password managers were associated with Step X.***

Table 18: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step X: Practice Rejection. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	0.209	0.234	0.8	1	0.371	1.233	0.779	1.951
PM risk perception(1)	0.829	0.313	7.016	1	0.008	2.291	1.241	4.231
I don't understand how it works(1)	-1.285	0.559	5.289	1	0.021	0.277	0.093	0.827
I don't think it is important(1)	1.531	0.411	13.851	1	<.001	4.623	2.064	10.354
It's inconvenient(1)	1.092	0.401	7.43	1	0.006	2.981	1.359	6.537
It doesn't seem currently useful(1)	1.162	0.391	8.848	1	0.003	3.195	1.486	6.868
I tried it and didn't like it(1)	4.912	0.787	38.986	1	<.001	135.878	29.077	634.955
I tried something else I like better(1)	3.434	0.728	22.262	1	<.001	30.99	7.444	129.026
I couldn't find someone to help me with it(1)	2.724	0.658	17.127	1	<.001	15.245	4.196	55.392
I'm not required to use it(1)	1.493	0.313	22.729	1	<.001	4.451	2.409	8.223
I heard or saw advice not to use it(1)	1.835	0.819	5.021	1	0.025	6.264	1.258	31.182
I forgot about it(1)	1.997	0.343	33.943	1	<.001	7.368	3.763	14.425
Other reason:(1)	1.151	0.42	7.495	1	0.006	3.16	1.387	7.202

a. Variable(s) entered on step 1: I don't understand how to use it, I don't understand how it works, I don't think it is important, It's inconvenient, It's difficult to use, It doesn't seem currently useful, I'm already using something that I like better, I tried it and didn't like it, I tried something else I like better, I couldn't find someone to help me with it, New computing device doesn't support it, I'm not required to use it, Someone I trust told me not to use it, I heard or saw advice not to use it, I forgot about it, Other reason:.

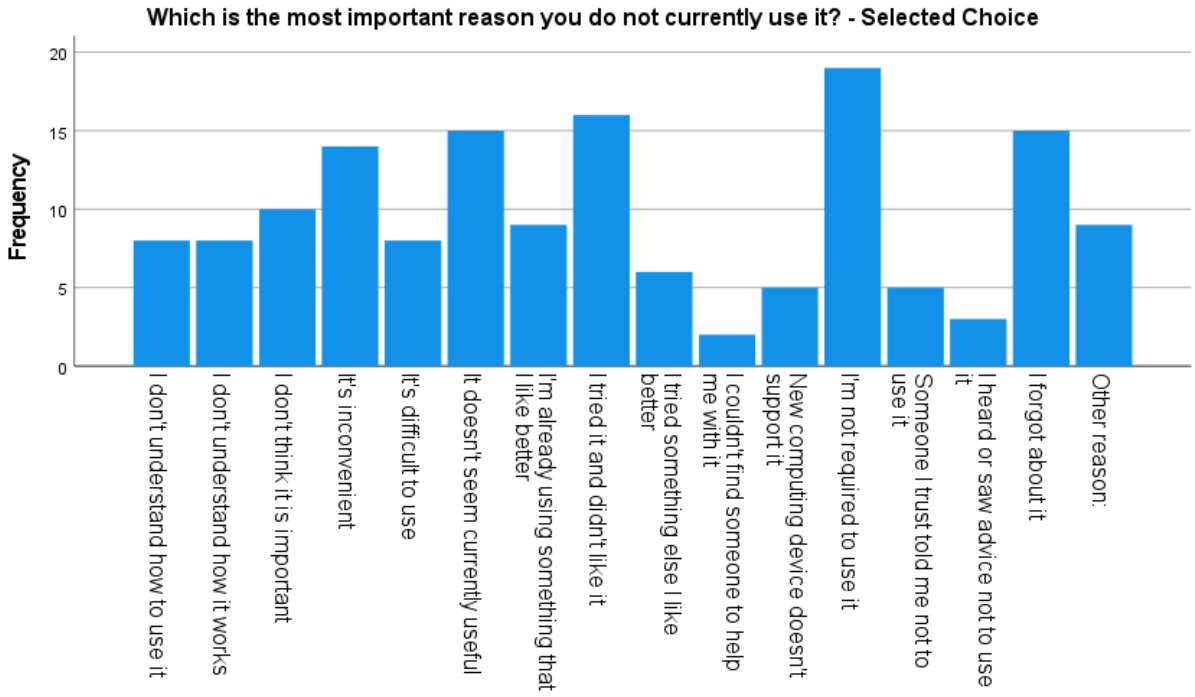

Figure 23: In Step X, not being required to use them was the most cited reason for not using a password manager.

5.2.3.2 Reasons Given for Adoption. All participants who were classified into Steps 3-4 were asked (1) to select all that applied from the same set of 21 possible reasons that they started using a password manager, including an "Other" write-in option, and (2) to select the most important reason. Step 4 participants were also asked the same questions about why they keep using a password manager. Using the "select all" reasons, I computed logistic regressions to determine which of the selected reasons were significantly associated with being classified in each step of non-adoption, controlling first for type of password manager and for awareness of usage risks. The results are summarized below, with tables shortened to only the control variables and the significant predictors.

Step 3: Practice Implementation. This group of participants started using password managers only within six months of the time that they survey was administered. The two variables most strongly and significantly positively associated with their decision to start using a password manager were social: "Found someone to help me with it," followed by "I was required to start using it." However, the variable "It was convenient" was both significantly positively associated with Step 3 and the reason most often cited (31) as the most important reason for adoption in Step 3 (Figure 24). This is evidence that the characteristics of this security practice are more salient in participants' minds than the social influences on initial adoption. Participants were significantly less likely to be in Step 3 if they selected "Computing device supported it" or "I tried it and liked it." Table 19 model statistics: x^2 (19) = 181.269, p<.001, Nagelkerke R^2 = .337.

- ***Convenience, troubleshooting help and mandatoriness were associated with Step 3.***

Table 19: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 3: Practice Implementation. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation [a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM type(1)	-0.329	0.24	1.882	1	0.17	0.72	0.45	1.151
PM risk perception(1)	-0.1	0.316	0.101	1	0.75	0.904	0.487	1.679
I understood how to use it(1)	1.492	0.346	18.633	1	<.001	4.447	2.258	8.755
Because it is important(1)	1.267	0.304	17.353	1	<.001	3.551	1.956	6.446
It was convenient(1)	1.002	0.294	11.637	1	<.001	2.723	1.531	4.842
It seemed useful(1)	1.435	0.327	19.266	1	<.001	4.199	2.213	7.969
I tried it and liked it(1)	-1.266	0.437	8.414	1	0.004	0.282	0.12	0.663
Found someone to help me with it(1)	2.349	0.742	10.011	1	0.002	10.471	2.444	44.854
Computing device supported it(1)	-1.519	0.504	9.09	1	0.003	0.219	0.082	0.588
I was required to start using it(1)	1.823	0.527	11.972	1	<.001	6.193	2.205	17.395

a. Variable(s) entered on step 1: I understood how to use it, I understood how it works, Because it is important, It was convenient, It was easy to use, It seemed useful, I tried it and liked it, Was better than something else I used to use regularly, Was able to try it out first, Was able to set it up, Found someone to help me with it, Computing device supported it, I get notifications about it, I was required to start using it, Someone I trust told me to start using it, I heard or saw advice to start using it, Other:.

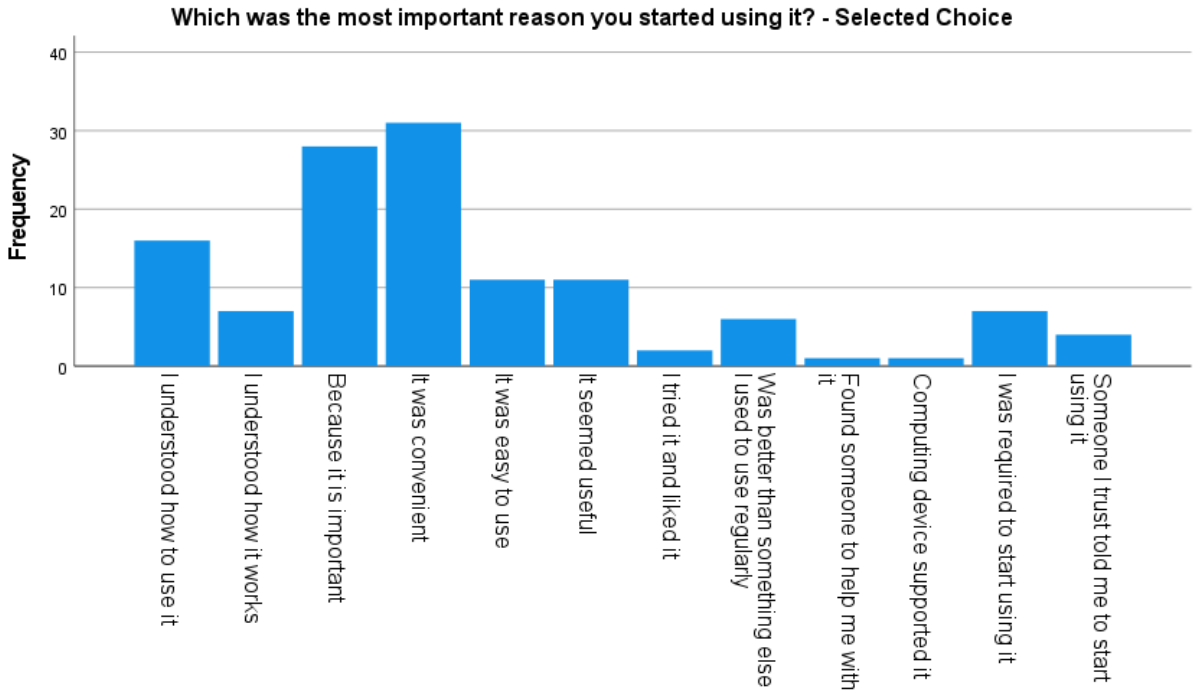

Figure 24: Convenience was cited most often by participants in Step 3 as the most important reason why they started using a password manager, closely followed by "Because it is important."

Step 4: Practice Maintenance. This group of participants started using password managers at least six months or earlier from the time that they survey was administered. Looking first at initial adoption: the variable most strongly and significantly positively associated with Step 4's decision to start using a password manager was "I was required to start using it," followed by "It was convenient." Convenience was also the reason most often cited (61) as the most important for initial adoption by those in Step 4 (Figure 25). Participants were significantly less likely to be in Step 4 if they were asked about using a separately installed password manager or if they said they were aware of risks of using password managers. Table 20 model statistics: x^2 (19) = 684.422, p<.001, Nagelkerke R^2 = .827.

- ***Convenience and mandatoriness were associated with initial adoption for Step 4.***

Table 20: For initial adoption, Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 4: Practice Maintenance. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM type(1)	-0.551	0.212	6.736	1	0.009	0.720	0.380	0.874
PM risk perception(1)	0.757	0.263	8.313	1	0.004	0.904	1.274	3.569
Because it is important(1)	1.128	0.302	13.952	1	<.001	3.089	1.709	5.582
It was convenient(1)	1.848	0.26	50.621	1	<.001	6.345	3.814	10.555
It was easy to use(1)	0.651	0.308	4.469	1	0.035	1.918	1.049	3.508
I tried it and liked it(1)	1.029	0.39	6.950	1	0.008	2.799	1.302	6.017
Computing device supported it(1)	1.697	0.454	14.001	1	<.001	5.459	2.244	13.28
I was required to start using it(1)	2.103	0.527	15.931	1	<.001	8.190	2.916	23.003
I heard or saw advice to start using it(1)	1.424	0.703	4.096	1	0.043	4.152	1.046	16.484

a. Variable(s) entered on step 1: I understood how to use it, I understood how it works, Because it is important, It was convenient, It was easy to use, It seemed useful, I tried it and liked it, Was better than something else I used to use regularly, Was able to try it out first, Was able to set it up, Found someone to help me with it, Computing device supported it, I get notifications about it, I was required to start using it, Someone I trust told me to start using it, I heard or saw advice to start using it, Other:.

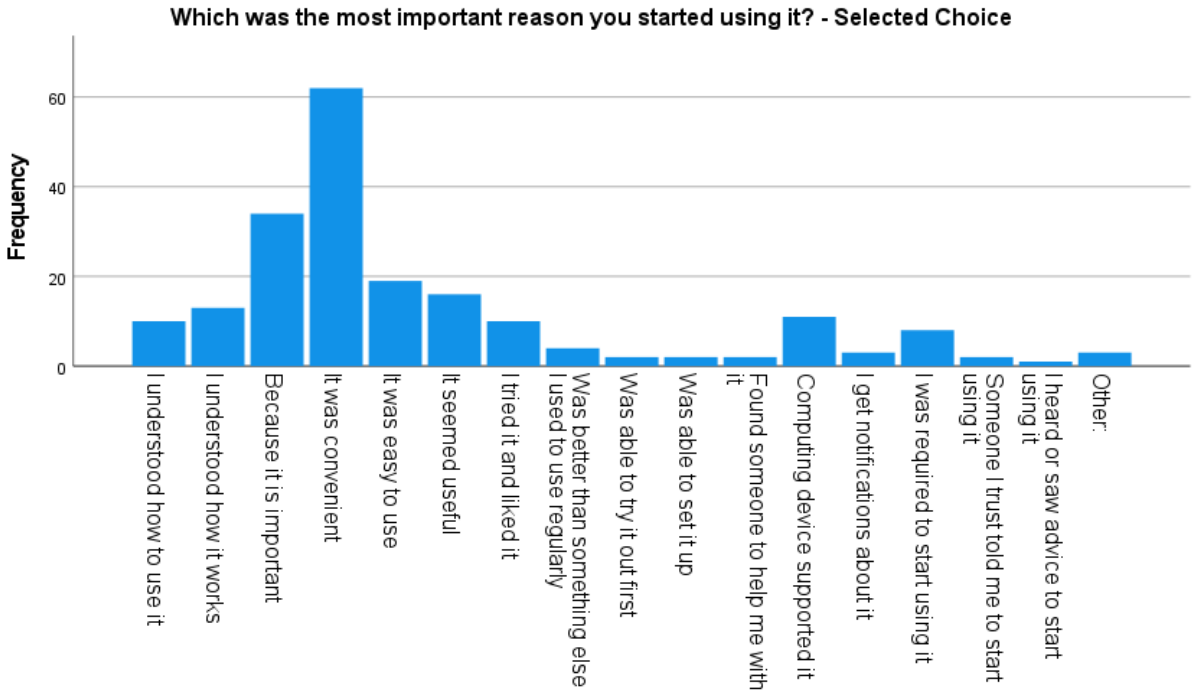

Figure 25: Convenience was cited most often by participants in Step 4 as the most important reason why they first started using a password manager, followed distantly by "Because it is important."

Looking next at continually maintained adoption: the variable most strongly and significantly positively associated with Step 4's decision to keep using a password manager was "It seems useful," followed by "It's convenient." Convenience was also the reason most often cited (90) as the most important for maintained adoption by those in Step 4 (Figure 26). Participants were significantly less likely to be in Step 4 if they selected "Found someone to help me with it" or "I get notifications about it" as reasons they keep using a password manager. Table 21 model statistics: x^2 (19) = 287.552, p<.001, Nagelkerke R^2 = .428.

- ***Convenience and usefulness were associated with continued adoption for Step 4.***

Table 21: For continually maintained adoption: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 4: Practice Maintenance. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in Step 0, all other variables being held constant, while a higher odds ratio indicates more likelihood.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM type(1)	-0.129	0.372	0.120	1	0.729	0.879	0.424	1.822
PM risk perception(1)	0.728	0.483	2.269	1	0.132	2.070	0.803	5.335
I understand how to use it(1)	2.909	0.620	22.020	1	<.001	18.340	5.441	61.814
Because it is important(1)	3.385	0.593	32.645	1	<.001	29.528	9.245	94.316
It's convenient(1)	4.681	0.544	74.077	1	<.001	107.854	37.146	313.156
It seems useful(1)	5.485	1.196	21.024	1	<.001	241.158	23.119	2,515.558
Found someone to help me with it(1)	-12.199	2.583	22.310	1	<.001	0.000	0.000	0.001
Computing device supports it(1)	4.277	1.113	14.764	1	<.001	72.011	8.128	638.012
I get notifications about it(1)	-5.497	1.364	16.229	1	<.001	0.004	0.000	0.059
I'm required to keep using it(1)	3.437	0.911	14.221	1	<.001	31.100	5.211	185.610

a. Variable(s) entered on step 1: I understand how to use it, I understand how it works, Because it is important, It's convenient, It's easy to use, It seems useful, I tried it and liked it, Better than something else I used to use regularly, Was able to try it out first, Was able to set it up, Found someone to help me with it, Computing device supports it, I get notifications about it, I'm required to keep using it, Someone I trust told me to keep using it, I heard or saw advice to keep using it, Other:.

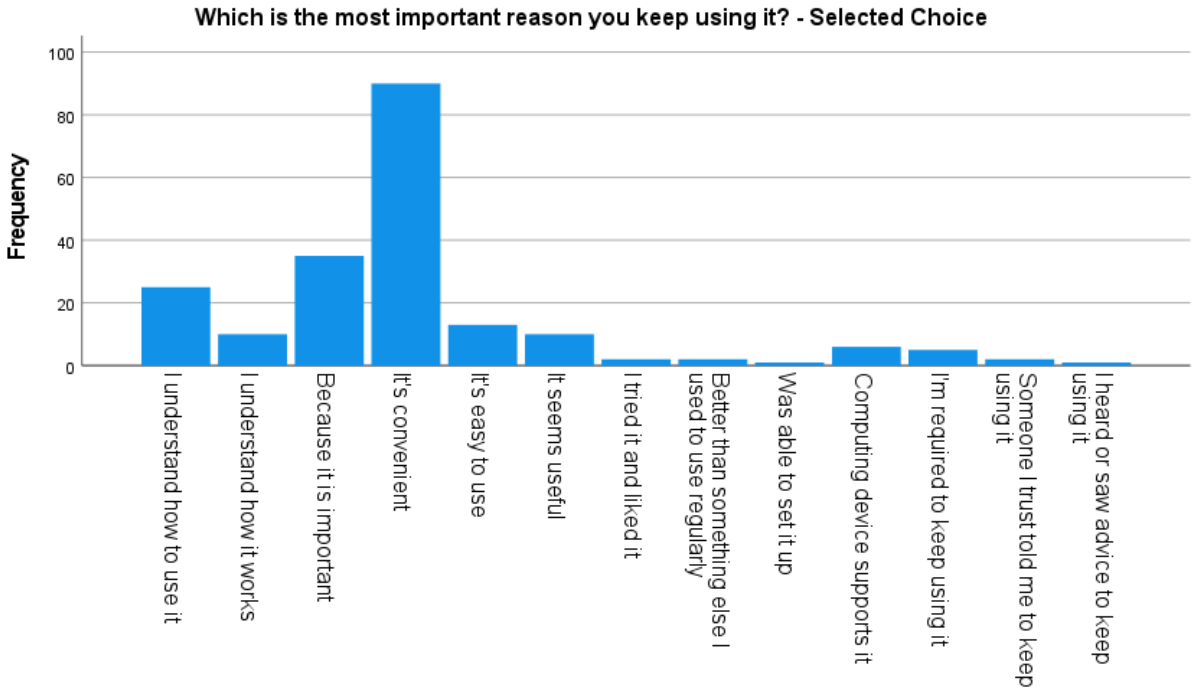

Figure 26: Convenience was cited most often by participants in Step 4 as the most important reason why they keep using a password manager, followed distantly by "Because it is important."

5.2.3.3 Differentiating Social Factors. To follow up on the above analysis, I sought to discover whether social factors would differ significantly according to step classification, as suggested by the Phase 1 results. The goal of these analyses of variance were, first, to determine whether a significance difference exists among means of an interval variable for participants in different steps; and second, to use post-hoc tests to determine which pairwise comparisons were significant (adjusted for multiple comparisons). If a significant difference was detected, a logistic regression then determined the odds that someone would be classified as an adopter given a one-unit increase in the social factor and the two control variables: type of password manager, and perception of usage risks.

Leadership and Caretaking Behaviors. An analysis of variance shows that a significant difference exists among mean scores by step on the adapted Rogers "Adoption Leader" scale (Figure 27): F (5,853) = 38.571, p<.001. Further, an estimated 18.4% of the variance in the Rogers Adoption Leader scale is accounted for by the six-level step classification variable: η^2=.184 (95% CI: .137, .226) [101]. A Tukey HSD post-hoc test found that the value for Step 4: Practice Maintenance (M=3.36, SD = 0.07) was significantly higher than for all others except Step 3: Practice Implementation (M=3.37, SD = 0.08). A logistic regression determined that a participant with a high score on this assessment of security leadership was 130.9% more likely to have adopted a password manager (Steps 3-4). Table 22 model statistics: x^2 (3) = 181.768, p<.001, Nagelkerke R^2 = .259.

- ***Those in Step 3 and Step 4 scored significantly higher on the Adoption Leader scale.***

Table 22: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-1.092	.160	46.479	1	<.001	.336	.245	.459
PM risk perception(1)	.865	.220	15.533	1	<.001	2.375	1.545	3.652
Adoption Leadership	.837	.087	91.902	1	<.001	2.309	1.946	2.740

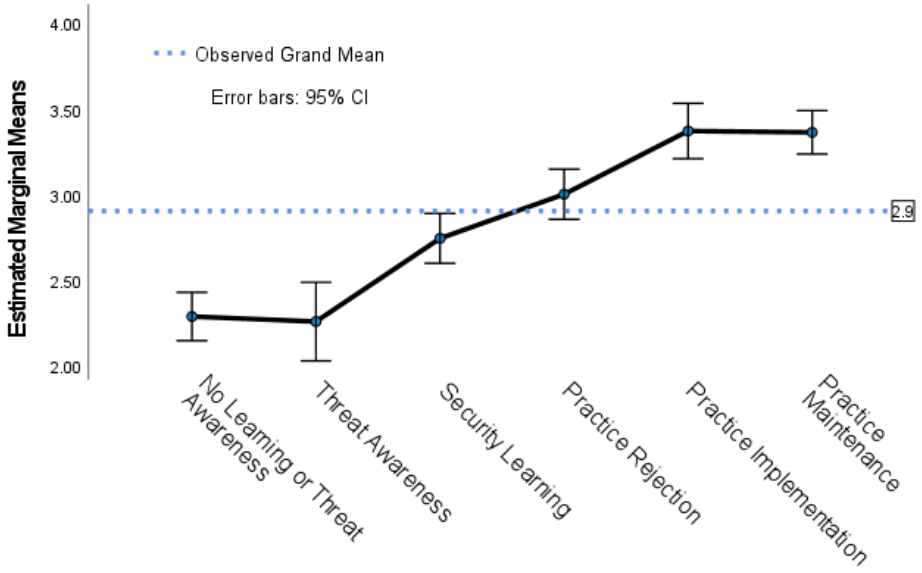

Figure 27: A post-hoc analysis found a significant difference in Rogers Adoption Leader scale means between Step 4: Practice Maintenance (far right) and all other steps except Step 3: Practice Implementation (second from right).

A second analysis of variance shows that a significant difference exists among mean scores by step on the Educating Others scale (Figure 28): F (5,853) = 32.370, p<.001. Further, an estimated 15.9% of the variance in the Educating Others scale is accounted for by the six-level step classification variable: η^2=.159 (95% CI: .114, .199) [101]. A Tukey HSD post-hoc test found that the value for Step 4: Practice Maintenance (M=3.58, SD = 0.98) was significantly higher than for all others except Step 3: Practice Implementation (M=3.47, SD = 0.90). A logistic regression determined that a participant with a high score on this assessment of security caretaking was 115.7% more likely to have adopted a password manager (Steps 3-4). Table 23 model statistics: x^2 (3) = 181.768, p<.001, Nagelkerke R^2 = .259.

- ***Those in Step 4 scored significantly higher on the Educating Others scale.***

Table 23: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-1.094	.160	47.037	1	<.001	.335	.245	.458
PM risk perception(1)	.945	.221	18.260	1	<.001	2.573	1.668	3.970
Educating Others	.769	.083	85.725	1	<.001	2.157	1.833	2.538

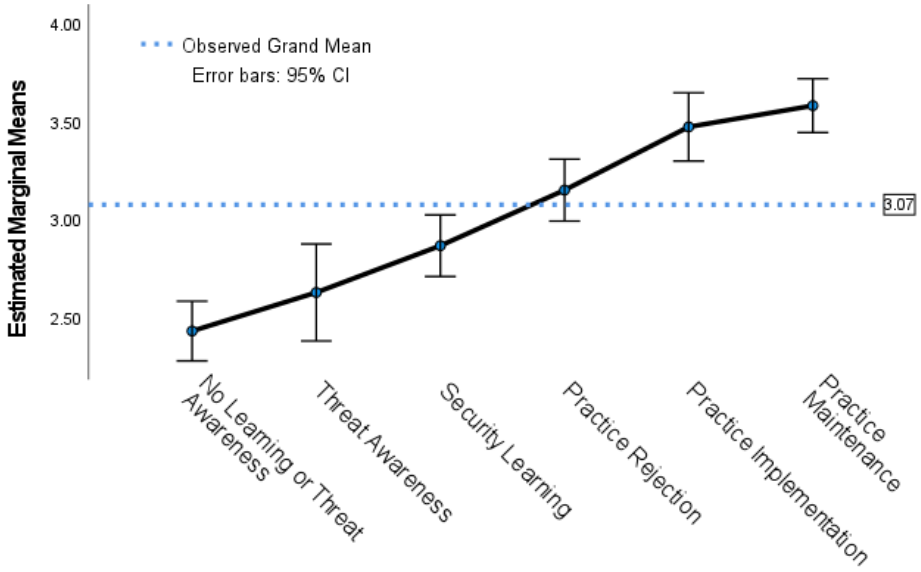

Figure 28: A post-hoc analysis found a significant difference in Educating Others scale means between Step 4: Practice Maintenance (far right) and all other steps except Step 3: Practice Implementation (second from right).

Persuasive Characteristics of Password Managers. An analysis of variance shows that a significant difference exists among mean scores by step on the Moore-Benbasat "Image" scale, with wording adapted to the password manager type asked about in the survey (Figure 29): F (5,853) = 4.032, p<.001. An estimated 2.3% of the variance in the PM Image scale is accounted for by the six-level step classification variable: η^2=.023 (95% CI: .004, .041) [101]. A Tukey HSD post-hoc test found that the value for Step 3: Practice Implementation (M=2.90, SD = 0.95) was significantly higher than for others except Step 4: Practice Maintenance (M=2.70, SD = 1.03) and Step 2: Threat Awareness (M=2.65, SD = 0.76). A logistic regression determined that a participant with a high score on this assessment of positive image of password managers was 36.6% more likely to have adopted a password manager (Steps 3-4). Table 24 model statistics: x^2 (3) = 88.964, p<.001, Nagelkerke R^2 = .134.

- ***Those in Step 3 rated password managers significantly higher on the Image scale than those in Step X, Step 2, or Step 0.***

Table 24: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-.953	.149	40.684	1	<.001	.386	.288	.517
PM risk perception(1)	1.134	.208	29.706	1	<.001	3.109	2.068	4.675
PM Image	.312	.078	15.871	1	<.001	1.366	1.172	1.593

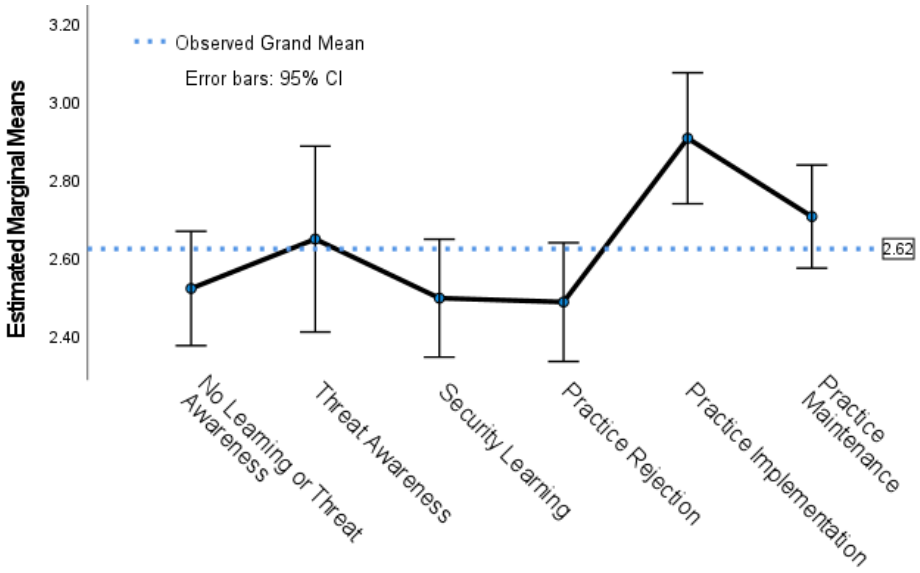

Figure 29: A post-hoc analysis found a significant difference in PM Image scale means between Step 3: Practice Implementation (second from right) and other steps except Step 4: Practice Maintenance (far right) and Step 2: Threat Maintenance (second from left).

A second analysis of variance shows that a significant difference exists among mean scores by step on the condensed Moore-Benbasat Visibility/Trialability scale, with wording adapted to the password manager type asked about in the survey (Figure 30): F (5,853) = 36.747, p<.001. An estimated 17.7% of the variance in the PM Visibility/Trialability scale is accounted for by the six-level step classification variable: η^2=.177 (95% CI: .130, .218) [101]. A Tukey HSD post-hoc test found that the value for Step 3: Practice Implementation (M=3.44, SD = 0.07) was significantly higher than for all others except Step 4: Practice Maintenance (M=3.38, SD = 0.06). A logistic regression determined that a participant with a high score on this assessment of high visibility and availability of password managers to try out was 93.5% more likely to have adopted a password manager (Steps 3-4). Table 25 model statistics: x^2 (3) = 194.734, p<.001, Nagelkerke R^2 = .276.

- ***Those in Step 3 or Step 4 rated password managers significantly higher on the Visibility/Trialability scale than those in any non-adoption step (0, 1, 2, and X).***

Table 25: Significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-1.016	.161	39.956	1	<.001	.362	.264	.496
PM risk perception(1)	.918	.221	17.173	1	<.001	2.503	1.622	3.863
PM Visibility/Trialability	1.077	.109	97.990	1	<.001	2.935	2.372	3.633

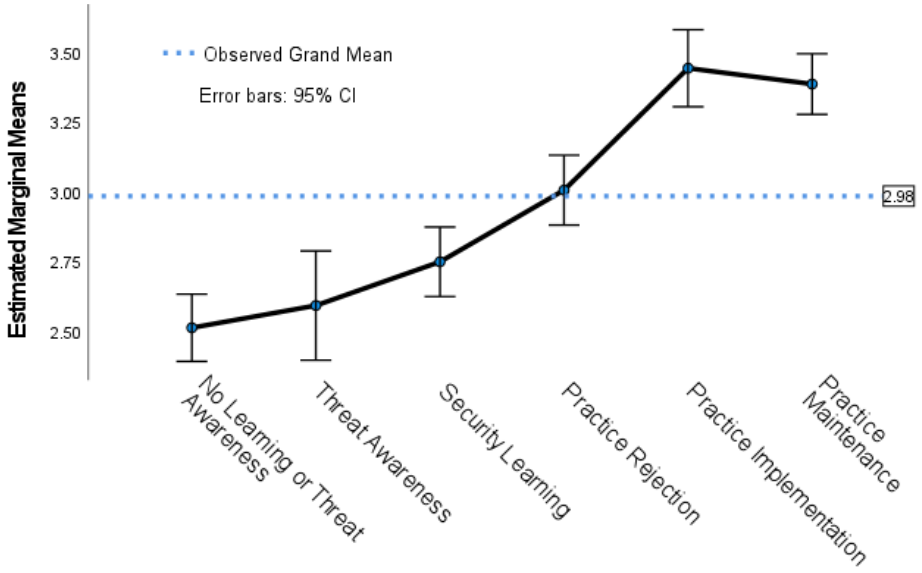

Figure 30: A post-hoc analysis found a significant difference in PM Visibility/Trialability scale means between Step 3: Practice Implementation (second from right) and all others except Step 4: Practice Maintenance (far right).

Exposure to Security Breach Experiences. A logistic regression determined that a participant who reported a close tie being a frequent victim of security breaches in the past year was 26.8% more likely to have adopted a password manager (Steps 3-4). The same test determined that a participant who frequently hearing or seeing news about security breaches in the past year was 46.7% more likely to have adopted a password manager (Steps 3-4). However, participants who themselves had frequently experienced security breaches in the past year showed no significant change in adoption likelihood. Table 26 model statistics: x^2 (5) = 114.596, p<.001, Nagelkerke R^2 = .170.

Table 26: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM type(1)	-0.972	0.152	40.720	1	<.001	0.378	0.281	0.510
PM risk perception(1)	0.989	0.212	21.724	1	<.001	2.688	1.774	4.074
Personally frequent victim of an online security breach (e.g., account hacking, viruses, malware or theft of your personal data)	-0.067	0.094	0.511	1	0.475	0.935	0.777	1.124
Close tie (e.g., spouse, family member or close friend) frequent victim of an online security breach	0.237	0.095	6.252	1	0.012	1.268	1.053	1.527
Frequently heard or read about such breaches	0.383	0.077	24.678	1	<.001	1.467	1.261	1.707

Subsequently, I averaged together the two items about social exposure to security breach experiences to create one interval variable. An analysis of variance shows that a significant difference exists among mean scores by step on this averaged variable (Figure 31): F (5,853) = 12.854, p<.001. An estimated 7% of the variance in the mean is accounted for by the six-level step classification variable: η^2=.070 (95% CI: .037, .100) [101]. A Tukey HSD post-hoc test found that the value for Step 4: Practice Maintenance (M=2.80, SD = 0.06) was significantly higher than for others except Step 3: Practice Implementation (M=2.78, SD = 0.07) and Step X: Practice Rejection (M=2.57, SD = 0.07).

- ***No association existed between a participant's individual frequency of experiencing security breaches and their likelihood of being in adoption (Step 3 or Step 4).***

- ***Those with frequent social exposure to breaches (through a close tie or media/peers) were significantly more likely to be in Step 3 or Step 4 than in a pre-decision step (0, 1, or 2).***

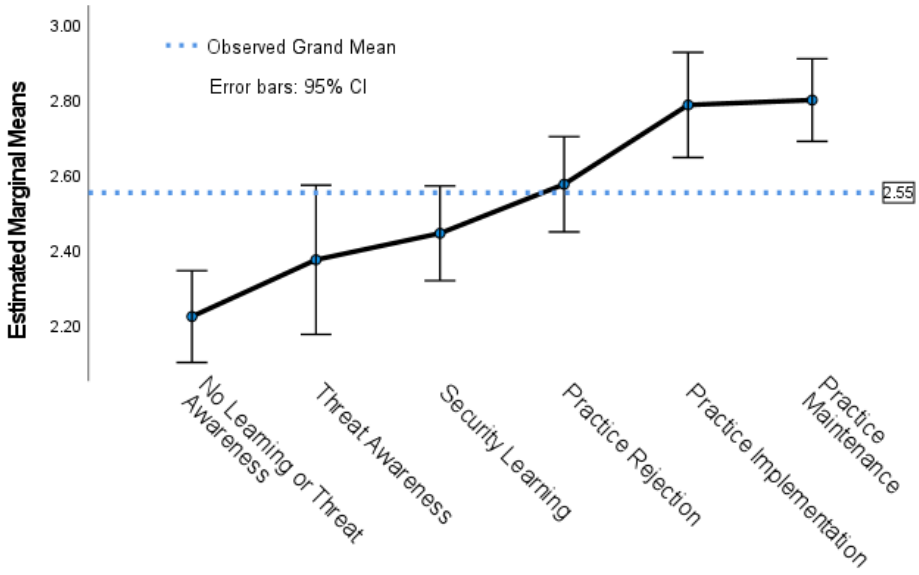

Figure 31: A post-hoc analysis found a significant difference in means for Social Exposure to Security Breach Experiences between Step 4: Practice Maintenance (far right) and other steps except Step 3: Practice Implementation (second from right) and Step X: Practice Rejection (third from right).

5.2.3.4 Differentiating Individual Factors. Lastly, I tested how adoption varies among the collected individual variables: Internet Know-How, Age Range, Gender Identity, Hispanic/Latinx/Spanish Identity, Racial/Ethnic Identity, Household Size, Income Range, Level of Education, Experience Working with Sensitive Data, and Computer/Information Science Experience. To simplify the analysis, I converted all the categorical variables into binary variables based on their median values or another natural cut-off point (such as household income of $25,000, close to the U.S. poverty level of $23,030 for a household of 3). As Internet Know-How is known to vary with other individual characteristics [70,115], I started with its analysis and then added it as a third control variable (along with type of password manager asked about and perception of usage risks) in subsequent logistic regressions.

Internet Know-How. An analysis of variance shows that a significant difference exists among mean scores by step on the Internet Know-How scale (Figure 32): F (5,853) = 37.403, p<.001. An estimated 18% of the variance in the this scale is accounted for by the six-level step classification variable: η^2=.180 (95% CI: .132, .221) [101]. A Tukey HSD post-hoc test found that the value for Step 4: Practice Maintenance (M=3.64, SD = 0.83) was significantly higher than for others except Step 3: Practice Implementation (M=3.55, SD = 0.85) and Step X: Practice Rejection (M=3.50, SD = 0.07). A logistic regression determined that a participant with a high score on this assessment of internet knowledge was 99.0% more likely to have adopted a password manager (Steps 3-4). Table 27 model statistics: x^2 (3) = 130.981, p<.001, Nagelkerke R^2 = .192.

- ***Those with a high score on Internet Know-How were significantly more likely to be aware of password managers (Steps 2, X, 3, or 4).***

Table 27: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-1.027	.154	44.256	1	<.001	.358	.264	.484
PM risk perception(1)	.805	.218	13.664	1	<.001	2.237	1.460	3.429
Internet Know-How	.688	.095	52.982	1	<.001	1.990	1.653	2.395

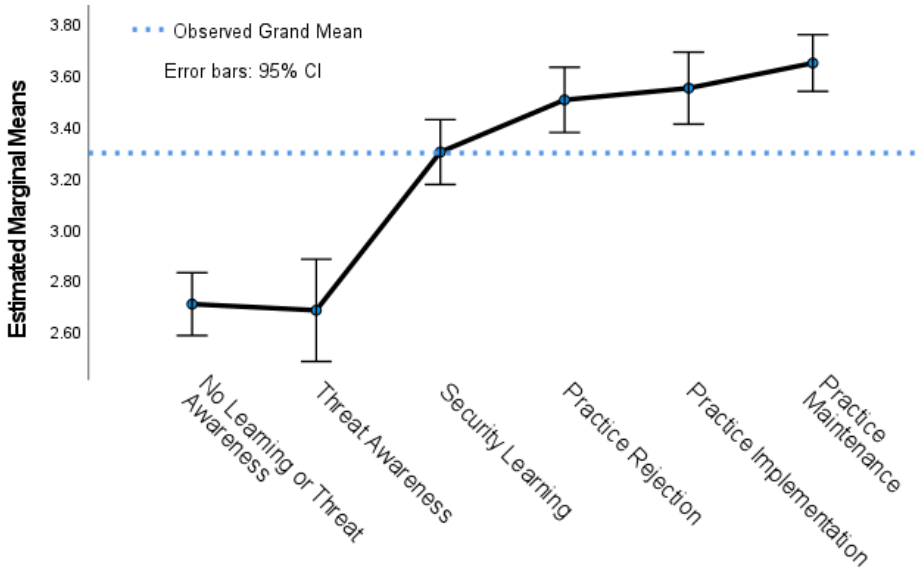

Figure 32: A post-hoc analysis found a significant difference in means for Internet Know-How between Step 4: Practice Maintenance (far right) and other steps except Step 3: Practice Implementation (second from right) and Step X: Practice Rejection (third from right). The biggest difference is between Step 1: Threat Awareness and Step 2: Security Learning.

Other Variables Associated with Adoption. I added in the other individual variables and reran the logistic-regression model. The -2 Log likelihood statistic changed from 1010.511 with just the three above variables to 949.378 with all the individual variables in the model. This represents an improved fit to the data that is not due solely to the inclusion of Internet Know-How. This model determined participants under 40 were 76.9% more likely to have adopted a password manager (Steps 3-4); that participants without a CS/IS education or job history were 48.4% less likely to have adopted a password manager, and that those with no experience working with sensitive data were 38.2% less likely to have adopted one. All other added variables were nonsignificant. Table 28 model statistics: x^2 (12) = 192.050, p<.001, Nagelkerke R^2 = .273.

- ***Those under 40 were significantly more likely to be in Step 3 or Step 4.***

- ***Those without any experienced with computer science, information science, or sensitive data were significantly less likely to be in Step 3 or Step 4.***

Table 28: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in adoption (Steps 3-4). All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-1.093	0.162	45.445	1	<.001	0.335	0.244	0.461
PM risk perception(1)	0.716	0.228	9.834	1	0.002	2.046	1.308	3.201
Internet Know-How	0.457	0.105	18.926	1	<.001	1.580	1.286	1.941
Under 40(1)	0.57	0.168	11.524	1	<.001	1.769	1.273	2.459
Never worked with sensitive data(1)	-0.481	0.177	7.394	1	0.007	0.618	0.437	0.874
No CS/IS experience(1)	-0.661	0.181	13.284	1	<.001	0.516	0.362	0.737

a. Variable(s) entered on step 1: Female, Under 40, Never worked with sensitive data, No CS/IS experience, Income under $25K, 4-year college degree, 3 or more in household, Non-White and/or Non-Caucasian, Hisp./Latin./Sp..

There were two surprises when looking at the logistic regressions by Step Classification for these individual variables. First, the last-step model was nonsignificant for Step X: Practice Rejection, implying that individual variables do not account for variance in Step X. Second, participants who identified as Non-White and/or Non-Caucasian were 92.0% more likely to be classified in Step 0: No Learning or Threat Awareness (Table 29 model statistics: x^2 (12) = 144.953, p=.017, Nagelkerke R^2 = .249), and 44.4% less likely to be classified in Step 3: Practice Implementation (Table 30 model statistics: x^2 (12) = 55.355, p=.009, Nagelkerke R^2 = .111). This implies that security education about tools such as password managers is reaching these populations less than they are reaching White and/or Caucasian populations.

- ***Those who identified as non-White and/or non-Caucasian were significantly more likely to be in Step 0 and significantly less likely to be in Step 3.***

Table 29: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 0: No Learning or Threat Awareness. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	.313	.192	2.646	1	.104	1.367	.938	1.992
PM risk perception(1)	-1.519	.531	8.194	1	.004	.219	.077	.620
Internet Know-How	-.817	.130	39.488	1	<.001	.442	.342	.570
Never worked with sensitive data(1)	.599	.210	8.133	1	.004	1.821	1.206	2.749
Non-White and/or Non-Caucasian(1)	.652	.273	5.712	1	.017	1.920	1.125	3.278

a. Variable(s) entered on step 1: Female, Under 40, Never worked with sensitive data, No CS/IS experience, Income under $25K, 4-year college degree, 3 or more in household, Non-White and/or Non-Caucasian, Hisp./Latin./Sp..

Table 30: Phase 2 significant variables and control variables in the regression equation predicting a participant's likelihood of being in Step 3: Practice Implementation. All the tested variables are listed in footnote a; those that do not appear in the table were non-significant. The beta (B) indicates the direction of prediction, and the Exp(B) is equivalent to the odds ratio. A lower odds ratio indicates less likelihood that a person would be in adoption, all other variables being held constant, while a higher odds ratio indicates more likelihood. PM_type(1) = a separately installed password manager.

							95% C.I. for Exp(B)	
Variables in the Equation[a]	B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
PM_type(1)	-.511	.204	6.282	1	.012	.600	.403	.895
PM risk perception(1)	-.009	.275	.001	1	.974	.991	.579	1.698
Internet Know-How	.160	.133	1.432	1	.231	1.173	.903	1.524
Never worked with sensitive data(1)	-.636	.242	6.899	1	.009	.530	.330	.851
No CS/IS experience(1)	-.549	.233	5.567	1	.018	.577	.366	.911
Non-White and/or Non-Caucasian(1)	-.587	.224	6.854	1	.009	.556	.358	.863

a. Variable(s) entered on step 1: Female, Under 40, Never worked with sensitive data, No CS/IS experience, Income under $25K, 4-year college degree, 3 or more in household, Non-White and/or Non-Caucasian, Hisp./Latin./Sp..

6. PHASE 3 (2022): TRIANGULATION AND INTEGRATION

This chapter sums up analyses of data collected in Phases 1-2 to answer the following question:

- **RQ-0:** *What stages do people go through in adoption (or non-adoption) of cybersecurity behaviors?*

First, I describe the algorithm that other researchers can use to classify participants into the appropriate step of the security adoption process (Section 6.1). Next, I provide the integrated path diagram of how people move through the steps if the adoption is voluntary vs. mandatory (Section 6.2). Finally, I triangulate and integrates these findings with prior work to produce a summary table of each of the final six steps' description, associated social influences, and obstacles to moving forward (Section 6.3). These are intended to help other researchers to use this work for classifying participants by step, for formulating hypotheses and explaining relationships among the variables, and for designing effective interventions.

6.1 Survey Items to Reproduce the Step-Classification Algorithm

To classify participants into the model's steps of adoption, I created and tested the following survey algorithm, which sorted each participant into one and only one step of security practice adoption.

1. Are you currently using [the security practice]?

   Binary response set: Yes/No

2. [If Yes] When did you start using [the security practice]?

   Binary response set: Up to 6 months ago/6 months ago or longer

   a. [If <6] STEP 3: IMPLEMENTATION

   b. [If >=6] STEP 4: MAINTENANCE

3. [If No] Did you ever use [the security practice]?

   Binary response set: Yes/No

   a. [If Yes] STEP X: REJECTION(a)

4. [If No] What best fits your situation regarding [the security practice]?

   Multiple-choice response set: I am aware of it but decided not to use it/I am aware of it and willing to start using it, but haven't yet/I am aware of it but hesitant to start using it/I am not aware of [the security practice]/I forgot about [the security practice]

   a. [If Decision] STEP X: REJECTION(b)

   b. [If No Decision, but Aware] STEP 2: SECURITY LEARNING

5. [If Not Aware or Forgot] Do you know of any threats to your online data or accounts that use of [the security practice] will guard against?

   Binary response set: Yes/No

   a. [If Yes] STEP 1: THREAT AWARENESS

   b. [If No] STEP 0: NO LEARNING OR THREAT AWARENESS

6.2 Data-Informed Diagram of the Steps of Security Adoption

Integrating Phase 2 data into the Phase 1 diagram of the steps of security practice adoption, I have revised my diagram of how the steps relate to each other (Figure 33). This diagram adds the two steps of non-adoption documented in Phase 12 – Step 0: No Learning or Threat Awareness, and Step X: Practice Rejection. It also accounts for the findings in Phase 1 that mandates cause some people go straight to Step 3: Practice Implementation (such as for a bank forcing a customer to use two-factor authentication), and that a change in technology or circumstances cause some who are in Step 4: Practice Maintenance to then discontinue use (such as dropping use of antivirus software when switching from a PC to a Mac). Finally, it adds a path straight from Step 0 to Step 3 through Step 2: Security Learning, skipping Step 1: Threat Awareness. The Phase 2 data show that only 10.4% of those in Step 3: Practice Implementation said that they were aware of threats that use of a password manager would guard against (Figure 34).

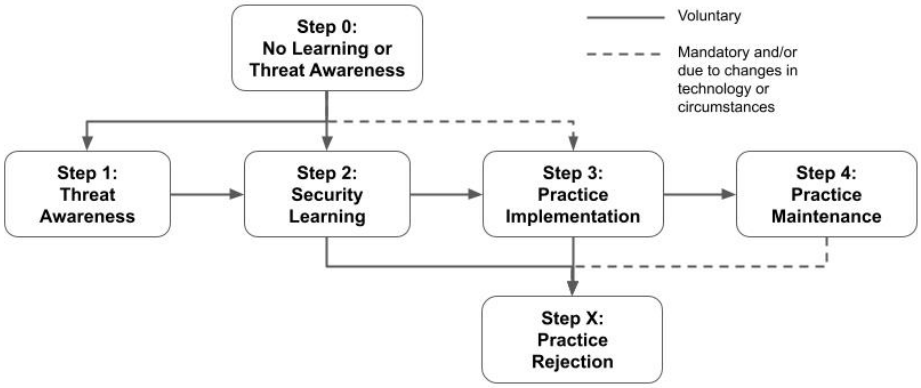

Figure 34: The revised diagram of the steps of security practice adoption. This diagram adds paths leading from Step 0: No Learning or Threat Awareness, and paths to Step X: Practice Rejection. Dotted paths indicate a forced change between steps.

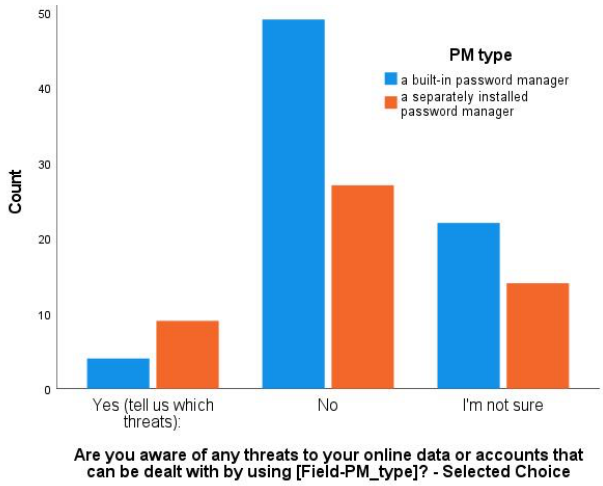

Figure 33: Most people who said they had started using a password manager within the previous six months also indicated that they were not aware of threats that the password manager guards against ("No" or "I'm not sure"). Each saw the same question, but with [Field-PM_type] replaced by either "a built-in password manager" or "a separately installed password manager."

6.3 Step-Specific Descriptions, Associated Social Influences, and Obstacles to Moving Forward

Next, I integrated the Phase 2 data, along with Phase 1 interview data coded as Unawareness and Non-Adoption, into a revised chart of each step's description, associated social influences, and obstacle(s) to moving forward (Table 31). The biggest change is the addition of Step 0 and Step X and their descriptions, associated social influences, and obstacle(s) to moving forward. I then examine these in more depth for all but Step 2, for which this data confirms insights from prior empirical studies and Bandura's theories of social cognition and social learning [12,13] that learning diffuses through social means such as social proof, storytelling, and advice-seeking [42,44,162–165,202].

Table 31: The revised chart adds Step 0 and Step X to the summary of findings about each step.

Step	Description	Associated Social Influences	Obstacle(s) to Moving Forward
No Learning or Threat Awareness (Step 0)	- Lack of understanding about a recommended security practice or the importance of guarding against the specific threats it protects against. - Examples: No knowledge of where to go for security advice, ignorance that software updates are for security.	- No person or source to help them with security. - No authority mandating security awareness training.	- Cultural differences. - Fear of creating tech headaches through changes. - Lack of interest.
Threat Awareness (Step 1)	- Mention of threat, risk, harm, or potential harm related to security; stated evaluation of the degree to which an event has significant implications for their security. - Examples: Receiving a threatening email, reacting to media reports, suspecting that your smartphone was illicitly accessed.	- Threats. - Warnings. - Alerts. - Media. - Storytelling.	- No awareness of a given security practice or other technology.
Security Learning (Step 2)	- Knowledge of existence of a given security practice or other technology (acquiring knowledge and skills, moving from a state of uncertainty to a state of certainty), but no enactment of that practice. - Examples: Hearing about secure messaging, finding out how others verify a job ad, being told to update software.	- Advice-seeking. - Social proof.	- Not feeling a threat (skipped Step 1). - Rejecting adoption before it is tried.
Security Practice Implementation (Step 3)	- Acting to test the security practice to evaluate its usefulness; acting to put the decision to adopt into effect. - Examples: Using a promo code or a free trial offer, playing around with a practice; settling on a security tool, acquiescing to a security policy, following up on Step 2.	- Troubleshooting help. - Mandates.	- Discontinuing adoption after the practice has been used at least once.
Security Practice Maintenance (Step 4)	- Acting to finalize the decision to use a practice; expanding use of the practice; mention of past implementation. - Examples: Stepping up the frequency of use; making statements like "I still use this" or "I currently use this."	- Leadership. - Caretaking.	- The adoption context becomes obsolete. - Waning effectiveness of the practice.
Security Practice Rejection (Step X)	- Either discontinuing adoption of a security practice or deciding not to implement the security practice. - Examples: Stopping after a few uses; making statements like "It felt like overkill" or "Effort is too much for the benefit."	- Receiving advice not to use it. - Lack of troubleshooting help. - Lack of mandates.	- Forgetfulness. - Lack of trust in efficacy or privacy. - Inconvenience. - Difficulty of use.

6.3.1 Insights for Step 0 and Step 1

Lack of understanding was a key obstacle for those in Step 0: No Learning or Threat Awareness and in Step 1: Threat Awareness. In Step 0, the Phase 2 covariate analyses and open-ended responses indicated that participants lacked sufficient understanding of what to do about security or what specific threats exist, evidence that they lacked a person or source to help them with security. Some indicated they were not required to improve their security, with no authority in their lives mandating that they attend security awareness training. In Step 1, in each phase, the participants reported the same lack of understanding of how security practices worked or how to use them. However, they reported becoming aware of a threat through a direct security incident occurring, or because of media or peer storytelling about threats. Internet Know-How mean scores for Step 0 and for Step 1 were significantly lower than for other steps (overall model $x^2(3) = 130.981$, $p<.001$, Nagelkerke $R^2 = .192$). Also, those who had never worked with sensitive data and those who identified as non-White and/or non-Caucasian were significantly more likely to be in Step 0, controlling for Internet Know-How (overall model $x^2(12) = 144.953$, $p<.001$, Nagelkerke $R^2 = .249$).

These findings resonated with Phase 1 interviews with the less tech-savvy and with people from non-White backgrounds. In those sessions, cultural differences emerged as an obstacle, from data that people who are not native English speakers struggle with computer security jargon, and that non-White and/or non-Caucasians were more likely to be classified in this step. Consistent with prior work [170,202], some participants also expressed a fear of changing anything about their technology setups to avoid creating problems, and a lack of interest in security.

- ***Recommendation: To move people out of Stage 0 and Stage 1, security know-how needs to reach broader segments of society.***

6.3.2 Insights for Step X

Those in Step X: Security Practice Rejection cited a host of reasons for rejecting adoption, some of which were social and some of which were usability-related or cognitive. In Phase 2, participants reported receiving advice *not* to use the practice; they were *not* able to find someone to help them with it, and they were *not* required to use it. They also reported that using password managers didn't seem important, that they tried them and didn't like them, that they forgot about them, that they were inconvenient, and that they didn't seem currently useful. These Phase 2 participants rated password managers significantly lower on the "Image" scale, and in open-ended responses, they expressed a lack of trust specifically in password managers to safeguard their passwords, but also in the security practices' efficacy and in providers' trustworthiness to protect their data privacy.

Phase 1 participants who reported rejecting or discontinuing security practices cited similar reasons: a lack of interest in expending effort to implement them, their perception that the benefits gained were not worth the risks of problems such as receiving annoying notifications, and their fears for their data privacy if they trust companies with their account details. These are consistent with rationales found in prior work on non-adoption [151,222].

- ***Recommendation: Soften the stances of those in Step X with transparency, increased usability, and on-demand support.***

6.3.3 Insights for Step 3

This research contributes an emphasis on trialability as a characteristic of tool-based security practices that is associated with adoption. Once the Phase 1 interview participants had resolved their uncertainties about a security practice, trialability provided a specific path for them to move forward from Security Learning (Step 2) to Security Practice Implementation (Step 3). For interview participants with negative attitudes toward cybersecurity, trialability eased them out of the "comfort zone" that they had had with their current (or lack of) security practices. The Phase 2 survey participants were found to be significantly more likely to have adopted a password manager if they rated password managers highly on the Moore-Benbasat Visibility/Trialability scale [144] (p<.001), indicating that they are visible and available to try out. Trialability had previously been identified in Diffusion of Innovations as a characteristic that makes innovations more likely to diffuse through a population [168]. It has been a significant component for marketing funnels in computing, such as for anti-spyware software [221] and web servers [83]. However, other characteristics are still necessary to move people toward long-term adoption. Prior studies in end-user cybersecurity have tended to focus on other characteristics of security practices, such as usability and convenience [147,151,222]. My survey participants also were significantly more likely to have adopted password managers (Step 3 or Step 4) and to maintain adoption (Step 4) if they said that they were "convenient" (p<.001), and to maintain adoption (Step 4) if they found password managers "useful" (p<.001). I found relative advantage to be significantly associated with non-adoption, with participants more likely to have rejected password managers if they said they had "tried something else I like better" (p<.001). The importance of relative advantage echoes Diffusion of Innovations [168].

This research also underlines the role of troubleshooting help as a social influence associated with adoption. Less-savvy Phase 1 interview participants reported getting stuck on installation or setup of tools such as password managers, but they got over these obstacles with the assistance of peers or media content. For adopters who had lingering confusion or doubts about the security practices, these sources helped them to clear their confusion regarding the many brands of software performing the same functions or about how their data would be used or misused. I found troubleshooting in these Step 3 contexts to evolve from advice-seeking and social proof that operated at Step 2, because interview participants often reported going back to the same source that helped them learn about the security practice (such as a trusted friend or a tech website) to help them overcome their implementation blockers. These results provide troubleshooting as a behavior that explains the association of advice-seeking [161,164,165] and social proof [42,44] with not just awareness but also adoption of security practices. The importance of troubleshooting for adoption was backed up by findings in the Phase 2 survey study. "Found someone to help me with it" was significantly positively associated with starting use of a password manager in the previous six months (Step 3, p=.002), while "I couldn't find someone to help me with it" was significantly positively associated with rejecting use of a password manager (Step X, p<.001). This type of social influence echoes the Transtheoretical Model's Processes of Change, specifically the behavioral process of Helping Relationships/Get Support, in which people call on others as they attempt to change a problem behavior [69,241]. It also echoes the findings in Poole et al.'s work on the difficulties of home networking [154,156] and to Vaniea and Rashidi's description of the software update process [194].

- ***Recommendation: Providing troubleshooting help should go together with improving usability so that those who try out security practices will not reject them.***

6.3.4 Insights for Step 4

Social influence flows outward in Step 4: Security Practice Maintenance. The Phase 2 findings validated those in Phase 1 that people in long-term adoption seem drawn to adoption leadership and to educating others on security. Participants with high scores on the Rogers Adoption Leader scale were significantly more likely to be in Step 4 than not (OR = 1.882 [95% CI: 1.581, 2.241], $p<.001$, Nagelkerke R^2 =.096), as were those with high scores on the Educating Others scale (OR = 1.913 [95% CI: 1.610, 2.272], $p<.001$, Nagelkerke R^2 =.107). This suggests a natural pairing with those in Step 2: Securing Learning or in Step X: Security Practice Rejection. Those in Step 2 are either hesitant or willing to act, yet something is stopping them. The data in Phase 1 and Phase 2 show that they may act if trusted sources resolve their doubts and troubleshoot their problems with implementing security practices such as password managers. Those in Step X have decided against the security practices they were asked about, such as using a password manager, but they might be open to accepting other security practices. The data shows that they react to social influences and that mandates might be effective.

- ***Recommendation: To intervene with those in Step 2 or in Step X, make use of opinion leaders who are in Step 4.***

7. DISCUSSION

As described so far, my research has yielded a preliminary model of people's security adoption journeys from no awareness to long-term adoption, focused on password managers. I synthesized survey data with interview data and prior work covering a range of security practices (Chapters 2-5). The resulting diagram and table of constructs (Chapter 6) brings structure to the existing literature on security practice adoption, and it contributes insights about which areas to focus on for research and design to boost end-user cybersecurity.

In the present chapter, I follow up on the results already documented to discuss four topics: how security researchers and practitioners can apply this work (Section 7.1), its contributions to existing theoretical models (Section 7.2), the limitations of this thesis (Section 7.3), and implications and future work (Section 7.4).

7.1 How Security Researchers and Practitioners Can Apply This Thesis Now

The step-classification algorithm (Section 6.1), data-informed step diagram (Section 6.2), and summary of step-specific social influences and obstacles (Section 6.3) are immediately useful for anyone working to improve usable security.

7.1.1 Ideas for Security Researchers

For password managers, but also security tools such as Virtual Private Networks (VPNs) and Two-Factor Authentication (2FA), this model can help answer research questions such as: *How many people are aware of, motivated, and/or knowledgeable about each tool? How much do social influences and voluntariness weigh in the decision to adopt? Why do people stop using the tools, once adopted?* For knowledge-based practices such as judging the legitimacy of websites or applying software updates in a timely fashion, this can help answer research questions such as: *How many people are aware of which practices have merit, and when? Which cognitions or contexts cue them to act out practices? What defeats their intention to act out practices?*

Other researchers can make use of the preliminary conceptual model to create testable hypotheses, such as what kind of intervention is more likely to work in Step 0 vs. in Step 3 to remove obstacles to adoption. The survey items in Section 6.1 can be adapted to other contexts and deployed as a pre- and post-intervention measurement in future research studies, to determine the distribution of the steps in each sample and to test whether participants move closer to long-term adoption after the deployment of the intervention. (See Fish'N'Steps for an example intervention using a similar algorithm for measurement [128] and Faklaris et al. 2022 for messaging and a short survey to measure use of two-step authentication among Amazon Mechanical Turk workers [72].)

The survey items can be used as a covariate in quantitative cross-sectional studies, to control for a person's step of security practice adoption or to test whether their step classification is significantly associated with other collected variables (such as data privacy concerns or general security attitudes).

Lastly, the survey items are short enough to be adapted and deployed across an entire population to assess the state of people's cybersecurity adoption for several recommended practices. A coupon code could be used to incentivize people to take these quick surveys via text message, webpage, social media, or email.

7.1.2 Ideas for Security Designers

Product and service designers will benefit from the conceptual model (Section 6.2) and summary descriptions of the steps and their social influences and obstacles (Section 6.3). They can make use of the diagram as a starting point for their own visualizations of customer journeys and to spark ideas of the relevant stakeholders in any security service. The noted social influences and obstacles can help with ideating new programs for security awareness or exploring alternatives for authentication methods and data flows. For example, the insight that people are likely to take advice from others in their social circles could be used to design a "share this" button for promoting the security practice, or the knowledge that a group of roommates has of each other could be used to create "challenge questions" that would replace passwords as the authentication method for a shared home network.

Working with researchers, designers also can use the survey items to identify participants who are in a particular stage, such as Step 0: Threat Awareness, to help inform the designs and evaluate the resulting products and services. These methods will help them to better understand their target users by step classification and to envision a "preferred future" for the product or service experience [57,183].

7.1.3 Ideas for Security Sales and Marketing

My data underline the importance that any developer or company that produces tools for end-user cybersecurity plan affordances for potential users to try out the tool. With software, this can be accomplished through promoting free trials and offering promotional bundles; some Phase 1 interview participants mentioned these as bonuses that they looked out for, although they were technology enthusiasts and less savvy users are not likely to enjoy testing out new apps. For reaching people with more negative attitudes toward cybersecurity specifically and/or technology in general, it may be necessary to bring the trial to them in person. One of our more-savvy participants said they would like to open a retail store where members of the public can come in and play around with security tools and practices the way that they do at home. Two variants of this idea would be to open an interactive display at a local science museum that lets people try out security practices, or to launch a kiosk with computers and cubbies stocked with different types of software and tools for the public to test out.

7.1.4 Ideas for Security Managers

Effective management, in security as in other domains, requires that managers be able to assess the effectiveness of their policies and their effect on employees and other stakeholders [17]. The step-classification algorithm (Section 6.1) and the other example materials from these studies (Appendices) can be adapted for the "productive security" processes in large multinational corporations. Such "passive" activities consist of iterative cycle of interviews, scenario development, surveys, and analysis [17], very similar to the research design used in this thesis. In smaller companies, the step-classification algorithm itself could be used to assess uptake of one security practice that management wants to increase adoption of, such as a multi-factor authentication app, with the resulting distribution used for helping to more accurately forecast the budget and staff time needed to train those who are not aware of the technology and to identify which employees will not need additional security training. Those non-IT workers identified in Step 4 could be recruited to help evangelize the security practice among those who are not convinced and to help troubleshoot implementation issues among their colleagues. Those who are IT workers could be enlisted as liaisons or "cybersecurity buddies" for non-IT departments [201].

7.1.5 Ideas for Security Executives and Policymakers

For C-level executives and policymakers, this thesis gives ideas at the high-level view of security improvements. The step-level insights (Section 6.3) are the following: (6.3.1) to move people out of Stage 0 and Stage 1, security know-how needs to reach broader segments of society; (6.3.2) soften the stances of those in Step X with transparency, increased usability, and on-demand support; (6.3.3) providing troubleshooting help should go together with improving usability so that those who try out security practices will not reject them; and, (6.3.4) to intervene with those in Step 2 or in Step X, make use of opinion leaders who are in Step 4. Mandates, unfortunately, will be part of the security policy menu for some time to come, but they can be avoided or softened by first trying out the use of opinion leaders to diffuse knowledge of security practices and to help make their use a social norm. These would act subtly on others akin to social media influencers, and so they must be cast carefully for likeability and for image (think of Kim Kardashian or Kendall Jenner as similar types of aspirational figures, who have massive global influence for fashion, beauty, and events). Hiring external influencers or sponsoring social media posts would help to communicate risks among those who ordinarily would not be sitting in a security awareness seminar and connect the dots with the preventive measures that all people can take for improving network security (using strong and unique passwords, securing devices, staying proactive for scams and false news, and quickly installing software updates). Planning out these messages for text and visual content would also help to reduce the possibility of spreading misinformation, because there will be time to vet them for accuracy and for realism.

Finally, those at the higher levels of companies, non-profits, and governments should make every effort and set aside budget to get the needed security tools into more people's hands without them paying for them. Given that cost was a concern for Phase 1 interview participants, for example, purchasing a university-wide password manager would help to encourage voluntary adoption of these for securely creating and sharing account passwords [201].

7.2 Contributions to Existing Theoretical Models in the Literature

My thesis contributes a description of the cybersecurity adoption process that identifies specific social influences at each step and that is driven by a mix of qualitative and quantitative data. None of the four behavior models that I primarily draw on – Protection Motivation Theory, the Technology Acceptance Model, the Transtheoretical Model, and Diffusion of Innovations – accounts for social influences by construct or by stage (Table 32).

Table 32: How my data-informed diagram compares with corresponds with constructs in four established models

My Results	Protection Motivation Theory	Technology Acceptance Model	Transtheoretical Model	Diffusion of Innovations
No Learning or Threat Awareness (Step 0)	(not mentioned)	External factors	Precontemplation	(not mentioned)
Threat Awareness (Step 1)	Threat appraisal; Protection motivation	External factors	(not mentioned)	(not mentioned)
Security Learning (Step 2)	Coping appraisal	Perceived ease of use; Perceived usefulness; Attitude toward behavior; Behavior intention	Contemplation; Preparation	Knowledge; Persuasion; Decision
Security Practice Implementation (Step 3)	(not mentioned)	Behavior	Action	Implementation
Security Practice Maintenance (Step 4)	(not mentioned)	(not mentioned)	Maintenance	Confirmation
Security Practice Rejection (Step X)	(not mentioned)	(not mentioned)	Relapse	Decision; Discontinuance

For Protection Motivation Theory, my thesis extends the model by specifying a path (represented by Step 2: Security Learning, and the trialability characteristic) between protection motivation (Step 1: Threat Awareness) and action (Step 3: Practice Implementation). I have identified the influence of advice-seeking, social proof, troubleshooting help, and mandates on moving people from protection motivation to action. Further, I have gathered data about those in Step 0: No Learning or Threat Awareness that suggests those identifying as Non-White and/or Non-Caucasian are not receiving information that would move them toward protection motivation, nor are those who do not work with sensitive data. Differences in language and culture also were found to be obstacles to those who are non-native English speakers being able to sufficiently understand computer security jargon.

For the Technology Acceptance Model and related frameworks, my thesis adds to what is known about the motivation to continue using a technology after the novelty wears off [191] and to how usability supports long-term adoption. A study of long-term use of activity trackers [182] found that, after curiosity had faded about three months in, a mix of awareness of health issues and social motivations such as relatedness kept people using their trackers. In my research, participants who adopted security practices also reported wanting to protect against threats, in this context, to their online data and accounts rather than to their health. Additionally, for a few interviewees who were forced to adopt practices, such as 2FA for a bank account, the action drove them to learn more the practice and then to voluntarily adopt it in other areas of their lives. Among interviewees who were long-term adopters, the social motivations of being seen as a security leader and caretaking for others helped to keep them engaged in security practices. For survey participants, usefulness and convenience were significantly positively associated with long-term adoption of password managers (Step 4), as was seeing their use as important (all $p<.001$).

For the Transtheoretical Model, my thesis contributes specific social influences that can help move people among the Stages of Change that correspond to the data-derived steps in Table 26. The Experiential Processes of (1) Consciousness Raising/Get the Facts and (2) Dramatic Relief/Pay Attention to Feelings seem likely to be encoded more strongly in people's memories if these facts and emotional stories are told by a peer or trusted media source. The Behavioral Processes of (8) Helping

Relationships/Get Support and (10) Stimulus Control/Manage Your Environment are also more likely to succeed if structured to involve trusted security leaders among friends, family, and work acquaintances. My data also show unequivocally that people's security behaviors are significantly associated with authorities mandating their use.

For Diffusion of Innovations, my thesis explicitly connects reaching the stage of confirmation of the adoption decision (represented by Step 4: Practice Maintenance) with people becoming opinion and adoption leaders in their social circles. While DoI research recognizes adoption leaders as a prominent influence on diffusion, it tends to identify these leaders by the time since they first adopted the innovation (with earlier times corresponding to the label "Innovators" or "Early Adopters"), rather than by their stage reached in the innovation-decision process. My thesis also adds details on how the process unfolds for adoption of preventive innovations [167,168], such as peers specifically providing troubleshooting help and spreading awareness and knowledge of security practices.

Like the thinkers who created models, however, I am simplifying a complex reality to tease apart specific factors at points in time, with the goal of changing people's thoughts and behaviors. My results – the diagram and the summary of each step's attributes, the step-associated social influences, and the step-associated obstacles to adoption -- will better help security researchers and designers to determine which social influences to incorporate in interventions to move people along the security adoption process. The next phase of this research will be a longitudinal survey study and/or controlled experiment so that I can test the timing piece of this thesis: to see, first, whether people are observed moving from one step to another through time, and, second, to determine whether the timing and the match to a particular step it will make a difference for the success of interventions such as awareness messaging or troubleshooting help with security tools.

7.3 Limitations of This Thesis

The part of my thesis statement that so far is unaddressed is the timing aspect. To investigate this will require a longitudinal survey study and/or controlled experiment, neither of which was possible in the time and budget constraints of this thesis work. A longitudinal survey study would document whether participants are observed moving from one step to another at specific points in time. A controlled experiment would determine whether the timing of step-matched interventions will make a difference for the success of interventions such as awareness messaging or troubleshooting help with security tools. This will help provide convincing evidence of the validity of the model and shed insights on how the process unfolds in real life, similar to studies such as Kelly et al.'s application of Diffusion of Innovations theory for spreading knowledge of HIV prevention among gay men [117].

My interview study yielded data for understanding the commonalities in stories of a wide range of behaviors within a small and nonrandom sample of adult U.S.-based survey respondents. Future work can follow up with quantitative surveys informed by these results to determine its representativeness and to help correct for any biases introduced by our targeted recruitment. Second, while I and the study team felt that we reached data saturation with our interview sample, i.e., participants began to simply repeat the same issues and offer no unique insights, I recognize that we likely have missed important voices and perspectives. Third, my approach introduces a pro-practice bias, in that it assumes that adopting a given security practice is the best course of action. Fourth, it also introduces recall bias, as participants' memories of their past thoughts, feelings, behaviors are suspect. Future work can follow up with an observational or diary study that tracks people's journey through the adoption process as it happens.

My survey research was designed to be correlational, which does not allow me to draw causal inferences. Future work will experimentally investigate the degree to which stage-matched interventions are associated with adoption of either a tool or a knowledge-based practice, versus interventions that are not stage-matched, and the degree to which participants are likely to maintain these security practices within one year. Also, the tight timeline did not allow me to fully investigate how this and/or other stage models, such as Diffusion of Innovations, can be adapted for enterprise teams. I see promise for comparing our model with models of behavior such as DoI and with process models such as the Software Engineering Institute's Capability Maturity Model Integration.

Finally, this thesis suggests one possible framework for security practice adoption. It identifies Diffusion of Innovations as the model that most closely fits the data, and elements of that prior work have been incorporated into the study design and the analysis and discussion. This thesis also identifies Protection Motivation Theory, the Technology Acceptance Model, and the Transtheoretical Model as three other models of particular importance for understanding security behaviors, and it draws from elements of this prior work as well. A sustained program of research will be needed to reach a definitive empirical understanding of the security adoption process and to identify which elements of prior work are essential to that understanding. This program of work will also need to identify whether the same model holds for cybersecurity in the context of the workplace as well as in the home or other personal contexts.

7.4 Implications and Future Work

A broader implication of this research is that individual decisions are only part of the story; social situations and social influences must be part of understanding and changing people's security behaviors. Below and in Table X, I list motivations and details for future work that would further advance this social perspective.

7.4.1 Social and Individual Factors in Adoption Decisions

The process of applying this thesis for further research into tool-based security practices such as password managers appears straightforward. What remains to be investigated is the degree to which the step model applies when other security practices besides consumer password managers are mandatory vs. voluntary, and whether they depend more on correctly implementing a tool vs. correctly implementing cognitive knowledge. As noted in Chapter 2, cybersecurity is incredibly layered and complex. Remote work and the proliferation of social devices have led to an increase in the amount of tech infrastructural competence that any one person has to manage [201], and this cognitive load may affect the process of security adoption and hamper the development of effective mental models of security. It is also unclear how much adoption of one specific security practice is influenced by a person's general disposition toward security engagement [70], or whether people's adoption tends to increase for security practices as a group; the Phase 2 survey followed the pattern of other recent studies in usable security by focusing on one specific security practice. Finally, researchers and practitioners have yet to fully leverage social influence in the design of security interventions.

Additional theories from psychology and other social sciences may also yield insights for cybersecurity behavior adoption that can be used in combination with the insights of this thesis. Festinger's theory of cognitive dissonance [100], for example, predicts that people will align their behaviors to prevent this dissonance so that if they change one behavior in a domain, they are more likely to change others. Similarly, Cialdini's theory of social influence [28,29] predicts that people who make a

first commitment to an action will follow through on it. His theory also predicts that they will change behaviors to conform to what they see as the norm around them or to what seems to hold more prestige.

A key assumption that my thesis research shares with the Transtheoretical Model (TTM), the Theory of Reasoned Action/Theory of Planned Behavior, and other behavior models is that people are not inherently motivated to act without an external prompt or nudge, and that they need help in gaining the necessary ability or affordance for effective action. The TTM Stages of Change (SoC) suggest that my step model can be used to better match a prompt or helpful tool with the point in time when the individual is primed to receive it. As with the SoC, those who are in Step 0 or Step 1, for instance, may be uninformed about the consequences of their lack of action, and are more likely to respond to *awareness-oriented* informational campaigns than promotions [157]. Step 3 may be more likely to respond to *action-oriented* interventions such as promotions that help them to act on knowledge [157].

Cybersecurity should also embrace the movement toward increasing diversity, equity, and inclusion (DEI), not just for help in recruiting workers, but also simply for spreading security awareness and increasing adoption. Cultural differences and ethnic and racial differences also emerged as an obstacle for people to enter the security adoption pathway. In Phase 1, I found that people who are not native English speakers struggle with computer security jargon. In Phase 2, I found that non-White and/or non-Caucasian participants were more likely to be classified in Step 0: No Learning or Threat Awareness.

The above discussion suggests the following research questions and study designs (Table 33).

Table 33: Research questions for further exploring social and individual factors in adoption decisions.

Sub-Section	Research Questions
7.4.1.1 Exploring the Impact of Cognitive Dissonance	To what extent is adoption of one security practice (Steps 3-4) associated with adoption of a group of such practices?
	To what extent does No Threat Awareness or Security Learning (Step 0) OR Threat Awareness (Step 1) lead directly to adoption of one security practice (Steps 3-4) vs. adoption of a group of such practices?
	To what extent does Security Learning (Step 2) lead directly to adoption of one security practice (Steps 3-4) vs. adoption of a group of such practices?
	To what degree is non-adoption (Steps 0-2, X) associated with a high degree of receiving conflicting advice about security practices vs. a high degree of receiving consistent advice?
7.4.1.2 Exploring the Impact of Social Influence In-Person vs. At a Distance	To what extent does adoption of one or more security practices by one person diffuse to their close ties and acquaintances? Does it matter if they have in-person contact, or can it diffuse with only remote or social-media contact?
	To what extent does the perceived prestige of a security practice impact adoption?
7.4.1.3 Exploring the Impacts of Targeting and Timing	For those in Steps 0-1, will exposure to accurate and clear advice information about a given security practice increase progress toward implementing adoption (Steps 2-3)?
	For those in Steps 2-3 and X, will exposure to accurate and clear troubleshooting information about a given security practice increase the number who implement or maintain adoption (Steps 3-4)?
	For those in Steps 2-3, will immediately access to a free trial version of a given security practice increase the number who implement or maintain adoption (Steps 3-4)?
7.4.1.3 Exploring the Adoption Process Among Non-English-Fluent Populations	For those who were raised with Spanish as their first language, what are the specific difficulties to awareness and adoption that derive from English as the main language of cybersecurity practices?
	What is the distribution of the steps of security behavior adoption among those who were raised with Spanish as their first language, vs. those who were raised with English as their first language?

7.4.1.1 Exploring the Impact of Cognitive Dissonance.

- *To what extent is adoption of one security practice (Steps 3-4) associated with adoption of a group of such practices?*
- *To what extent does No Threat Awareness or Security Learning (Step 0) OR Threat Awareness (Step 1) lead directly to adoption of one security practice (Steps 3-4) vs. adoption of a group of such practices?*
- *To what extent does Security Learning (Step 2) lead directly to adoption of one security practice (Steps 3-4) vs. adoption of a group of such practices?*

This suggests conducting a longitudinal study over a period of three months, in which participants who are in Steps 0-1 will, first, be instructed in how to adopt a security practice that is new to them (such as a separately installed password manager) and given an incentive to start and to keep using that practice; those in Steps 2 will only be given the incentive to start and to keep using the practice, and those in Steps 3-4 will be given the incentive with an unrelated rationale ("to thank you for your participation"). Next, all will be enrolled in a weekly survey to ask them about their familiarity with and frequency of using the 13 security practices that Phase 1 participants were queried about, and any security concerns that they have had to deal with. This survey will help track whether they also start using any other security practices and whether events other than the study intervention are influencing their actions. Finally, a random group of participants in each step will be interviewed about their answers, to follow up on how and why they chose their security-related behaviors. The duration of three months will help to dissipate any novelty effects from first enrolling and being guided through the initial adoption of the security practice.

- *To what degree is non-adoption (Steps 0-2, X) associated with a high degree of receiving conflicting advice about security practices vs. a high degree of receiving consistent advice?*

A screening survey will, first, classify potential participants by their step of adoption of one specific security practice (such as a separately installed password manager). Second, they will be asked to identify what advice they have been given about the use of the security practice, in two ways: one, by selecting the sources from a list; and two, by scanning news headlines and marking whether this is advice that they remember previously hearing or seeing. The results will be used to determine the degree to which a recalled conflict between advice is associated with their step vs. the recalled consistent advice.

7.4.1.2 Exploring the Impact of Social Influence In-Person vs. At a Distance.

- *To what extent does adoption of one or more security practices by one person diffuse to their close ties and acquaintances? Does it matter if they have in-person contact, or can it diffuse with only remote or social-media contact?*

For this study, several groups of connected people such as family members, a friend group, or a workgroup will need to be recruited. Ideally, about half will have some weekly in-person contact, and half will only have remote or social-media contact. Members of each group would first be asked to fill out a screening survey consisting of the Phase 1 Security Score questions and the Phase 2 Adoption Leader, Educating Others, and Internet Know-How questions. Then, one person can be randomly chosen to receive training and troubleshooting help in adoption of a given security practice that the group does not already use (such as a separately installed password manager). Each group member then will repeat the screening survey to track the changes over time for a period of six weeks. Finally, group members will be given a

copy of their collected survey responses and interviewed about why they think they responded the way that they did.

- *To what extent does the perceived prestige of a security practice impact adoption?*

Another line of research could manipulate the perceived social prestige of a cybersecurity behavior. Among non-adopters, two groups would be first given a misdirection such as a survey on their security attitudes and behaviors. As part of the post-survey incentive, Group A would be gifted a Yubi key or a separately installed password manager that they are told is a special, sought-after beta or limited-release version, while Group B would be given the same tool and told that it was unwanted overstock from customer returns. After two weeks, each group will be administered the same survey, which will include questions on their use of the given tool and whether they showed it to or discussed it with others. The results for each group will be compared to see if the manipulation led to increased use of the tool by Group A and whether Group A reports sharing information about the tool with others. The data will also be analyzed to see whether groups shared information more often in-person vs. remotely.

7.4.1.3 Exploring the Impacts of Targeting and Timing.

- *For those in Steps 0-1, will exposure to accurate and clear advice information about a given security practice increase progress toward implementing adoption (Steps 2-3)?*
- *For those in Steps 2-3 and X, will exposure to accurate and clear troubleshooting information about a given security practice increase the number who implement or maintain adoption (Steps 3-4)?*

An experiment will help to determine whether matching interventions to the step of security behavior adoption will perform better than interventions that are not stage-matched. This experiment will be best carried out on an existing crowdsourcing platform such as Amazon Mechanical Turk or Prolific, where a large scale can be achieved (N>2000) to detect small effect sizes. Participants would first be qualified for the study by answering a pre-intervention survey to classify their step of adoption of a particular security practice (such as using a password manager to generate strong and unique passwords for more than 10 accounts). They then will be randomly assigned to receive one of two different information sheets: A) information meant to raise awareness, motivation, and knowledge of the given practice among people who have never known of it before, and B) practical troubleshooting information for using a password manager to create and store unique passwords that are difficult to break, aimed at people who are aware of password managers but not using them regularly. The pre-interview survey will then be repeated immediately after and a month afterward. The results will be used to determine whether more people progress along the step path who receive a step-matched intervention, as suggested by this thesis.

- *For those in Steps 2-3, will immediate access to a free trial version of a given security practice increase the number who implement or maintain adoption (Steps 3-4)?*

This study will first require building out a website or cooperating with an existing website that provides information about a given security practice (such as using a separately installed password manager). The website link will be sent to enrolled study participants who are U.S. residents and adult internet users, and they will be surveyed about aspects of the website to confirm that they viewed it. A random subset of visitors to the page will receive a pop-up upon leaving that offers a free download and 30-day trial of the tool. The others will receive the link to the download and 30-day free trial in a post-intervention survey sent about one week afterward. The log data for downloads and for use will record the

study ID of the page visitor, to be able to match it to the survey data, and the time of first click, which will help determine whether the timing affected the interest in and use of the free trial.

7.4.1.3 Exploring the Adoption Process Among Non-English-Fluent Populations.

- *For those who were raised with Spanish as their first language, what are the specific difficulties to awareness and adoption that derive from English as the main language of cybersecurity practices?*
- *What is the distribution of the steps of security behavior adoption among those who were raised with Spanish as their first language, vs. those who were raised with English as their first language?*

This study will require a team member who is of Hispanic, Spanish, or Latino ancestry and also a team member (maybe not the same one) who is fluent in Spanish. The team will, first, translate into Spanish the Phase 1 survey items and those used for the step-classification algorithm. Second, we will identify and work with a local community group such as La Raza to recruit 12-15 participants for a needs-finding interview study. We will use a pre-interview screener and interview protocol based on that used in Phase 1. This will elicit obstacles to cybersecurity adoption that can be compared with the findings in this thesis and in other work. Next, we will ask the interview participants and the affiliated community group to help distribute a link to an online survey, sharing versions in both English and in Spanish, to gauge the distribution of the steps of security behavior change in this population. If possible, we will also mail printed surveys to households in neighborhoods known to be home to many people who grew up speaking Spanish as their first language. The results will be compared against the Phase 2 results from this survey to determine what differences exist in the step distribution.

7.4.2 Interventions that Leverage Social Insights and Platforms

My data suggest that a promising systems intervention could be to create a *crowdsourcing platform* for cybersecurity help, for those who are freelance or small-business workers or who are managing home networks. This platform would help those at the Security Learning step to seek advice about how to act to protect their online data and accounts, while those at the Security Practice Implementation step could get help with troubleshooting practices that they are trying out. People at the Maintenance step would be able to offer their own experiences, skills, and knowledge on the platform. The design should take care to incorporate social proof, such as through a points system for rewarding good advice and downgrading less-good advice, an avatar system to show who is contributing the most time to the platform, or via reviews of advisors to help others to judge their credibility and expertise. Such a platform would need robust moderation and safeguards, however, to prevent trolls or attackers from infiltrating and deliberately misleading those who sought advice from the crowd.

Another social intervention at the organizational level would be to designate tech helper (or some similar title) as an official non-IT job role. These would be akin to the system "superusers" who are given administrator-like access privileges to handle tasks at the workgroup level, with the aim of improving overall workgroup experiences with the system [229,242]. Such helpers would need to be selected for their social capital (likeability and prestige) and for competence with tech tasks, for communication skills, and for their desire to help with cybersecurity. If they possess the right set of personal characteristics, they can help influence people to see the security practices as desirable and not give out incorrect or misleading advice. Existing research on security advice-taking [161,164] and on informal tech helpers for

older adults [125,145] points to the value of selecting people who are already embedded in a social network and who are seen as credible and trustworthy.

This research shows promise to lead to a model that can be used to create a classification algorithm to direct resources and "interventions" (such as security tips or interface nudges) to those most likely to benefit, as predicted by the model. This will boost the effectiveness of cybersecurity risk assessments in resource-tight organizations. It will help those in industry who promote adoption of security practices to sharpen their strategies, building business value for their organizations. For the short-term, I envision creating a system for creating and recording digital cybersecurity markers, similar to the digital biomarkers being developed for health and wellness [27,56,195]. This would incorporate both quick surveys administered via text push or email and back-end logging and monitoring of data from enterprise mobile devices such as laptops and smartphones. The latter would be designed to be minimally privacy-invasive, only collecting metadata about whether apps for security such as VPNs or for sensitive accounts such as banks were turned off or on, and not recording or processing any of the content of the account data. The apps could be used to identify people who may need additional training or perhaps air-gapping of the resources they have access to, to prevent unintentional insider threat from lax security practices.

The above ideas suggest the following research questions and studies to pursue them (Table 34).

Table 34: Research questions for evaluating interventions that leverage social insights and platforms.

Sub-Section	Research Questions
7.4.2.1 Evaluating a Step-Matched Crowdsourcing Platform	To what degree will participation in a crowdsourcing platform lead to adoption of security practices (Steps 3-4) for those in Steps 0-2 vs. those in Step X?
	To what degree will participants classified in Step 4 vs. any other steps find satisfaction in contributing to a crowdsourcing platform?
7.4.2.2 Evaluating a Tech-Helper Program	To what degree will the presence of an official tech helper lead to adoption of security practices (Steps 3-4) for those in Steps 0-2 vs. those in Step X?
	To what degree will participants classified in Step 4 vs. any other steps find satisfaction in the presence of a tech helper?
7.4.2.3 Evaluating the Use of Digital Cybersecurity Markers	Can a system that collects mobile activity traces and survey data accurately predict someone's step classification as laid out in this thesis?
	To what degree will such a system be able to match users with security information that is successful at building their security efficacy and their self-efficacy

7.4.2.1 Evaluating a Step-Matched Crowdsourcing Platform.

- *To what degree will participation in a crowdsourcing platform lead to adoption of security practices (Steps 3-4) for those in Steps 0-2 vs. those in Step X?*
- *To what degree will participants classified in Step 4 vs. any other steps find satisfaction in contributing to a crowdsourcing platform?*

For this study, the platform will be configured to securely authenticate each user and to assign them a unique study ID. At onboarding, they will be administered a survey to assess their step of adoption for the 13 security practices asked of Phase 1 participants. Some who are security knowledgeable and found to be in Step 4 will be designated as tech helpers; all others will be designated tech seekers. Participants will be

required to interact with the platform, either by posting one question per day (Steps 0-2, X) or by answering or commenting on an already posted answer to one question per day (Step 4). Those in Step 3 will be allowed to post questions or to comment on answers, but not to directly answer questions.

After one week, all participants will be surveyed on their satisfaction with the experience. They will be asked to rate and comment on the platform itself and also on the quality of advice. They also will be asked about specific threads they contributed to.

7.4.2.2 Evaluating a Tech-Helper Program.

- *To what degree will the presence of an official tech helper lead to adoption of security practices (Steps 3-4) for those in Steps 0-2 vs. those in Step X?*
- *To what degree will participants classified in Step 4 vs. any other steps find satisfaction in the presence of a tech helper?*

This study will require the cooperation of a large company that has an interest in boosting adoption of a particular security practice (such as using VPNs on personal devices or using a password manager for securely sharing accounts). The study team will work with the managers to identify employees with sufficient social capital (likeability and prestige), competence with tech tasks, communication skills, and desire to help with cybersecurity. These individuals will be given a special badge and go through a half-day of training to ensure they have accurate, factual knowledge of the practice and to rehearse encounters with other staff who are seeking help or who may be openly resisting the practice. The entire group or department will be given a pre-intervention survey like the Phase 1 screener that includes survey items to classify each by adoption step. For four weeks, the tech helpers will be on call for the staff. They will participate in IT meetings about the rollout or otherwise be seen to be part of the rollout team. The study team will also be on call themselves to assist the tech helpers if needed, and they will meet with them once a week to check in on how things are going and to troubleshoot any problems with the study intervention.

At the end of four weeks, the department will be given a post-intervention survey, identical to the first, with the addition of an open-ended question to ask for comments on the program and another to ask for comments about the tech helpers. Some will be selected for interviews to follow up on their answers. The tech helpers will also be interviewed, as will the IT managers and employees who handled the rollout, to get their feedback about the experience. The interview data will be coded for "satisfaction" vs. "dissatisfaction," and the survey items will be compared to see how many employees progress in the steps over the four weeks. If available, the study team will also use system log data to evaluate whether a change in adoption occurred over the four weeks.

7.4.2.3 Evaluating the Use of Digital Cybersecurity Markers.

- *Can a system that collects mobile activity traces and survey data accurately predict someone's step classification as laid out in this thesis?*
- *To what degree will such a system be able to match users with security information that is successful at building their security efficacy and their self-efficacy?*

This study would involve two phases – a controlled trial and a field trial. The field trial will require the cooperation of a large company that has an interest in boosting adoption of a group of security practices and generally in forestalling unintentional insider threat. It will proceed similarly to the

controlled trial. For the controlled trial, I will recruit up to 500 participants who are adult Android smartphone users located in the United States. Those who answer our ad will be emailed instructions and a link to the study information sheet, the initial questionnaire, and app installation instructions. The study team will offer sessions remotely on Zoom and in person at my university for participants to get help with app installation. Once installed, the study apps will collect data in the background and push notifications of weekly surveys to participants. All participants will be allowed to exit the study at any time by pressing a button in the study app. Those who stay in the study will be entered in weekly drawings for a $50 gift card as an incentive to stay enrolled and to answer weekly surveys. At the end of the study, we will email all participants the directions to uninstall the app.

The collected data will be used to compute descriptive statistics from the initial questionnaire and the weekly surveys. We will correlate these stats with features created from lists of running apps, app versions, Wi-Fi usage and other network activity, number of calls received and made, number of messages received and sent, location data, activity recognition, and ambient light. This will give us objective data on whether participants have a two-factor authentication app installed and in use, whether they have a VPN app installed and in use, whether they are installing needed updates, whether they are using secured networks, and the surrounding context such as communications, location, and time of day. We will run regressions on these features and on collected survey variables such as the SA-6 security attitude scale. We will create visualizations of the collected data and explore the data using available software.

8. CONCLUSION

In my thesis, I used an exploratory sequential mixed-methods approach to specify a preliminary model of cybersecurity behavior adoption. The results are a data-driven diagram and description of the six steps of cybersecurity adoption and a survey-item algorithm for classifying people by adoption step. These steps are 0: No Learning or Threat Awareness, 1: Threat Awareness, 2: Security Learning, 3: Security Practice Implementation, 4: Security Practice Maintenance, and "X": Security Practice Rejection. My Step Classifications exhibited reliability and convergent validity, showing an expected significant variance by steps on mean scores for adapted Transtheoretical Model scales ($p<.001$). The trialability of password managers and the availability of troubleshooting help were significantly positively associated with adoption of password managers (Step 3 and Step 4, $p<.001$), and the lack of troubleshooting help was significantly positively associated with rejection of password managers (Step X, $p<.001$). Other authority influences (mandates, adoption leadership, caretaking) and peer/media influences (advice on password managers, exposure to news of others' security breach experiences) also were significantly associated with adoption decisions.

This work helps move the field of usable security away from "one size fits all" strategies by providing a theoretical basis and a method for segmenting the target audience for security interventions and directing resources to those segments most likely to benefit. It establishes an agenda for future experiments to validate whether specific step-matched interventions influence adoption and are more likely to lead to long-term change. It contributes to the literature on Diffusion of Innovations and extends other established theoretical models, such as Protection Motivation Theory, the Technology Acceptance Model, and the Transtheoretical Model. Finally, it suggests specific design interventions for boosting security adoption. I hope this will be a meaningful step toward reducing the overwhelming amount of human involvement in cybersecurity breaches in the coming years.

BIBLIOGRAPHY

[1] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human–Computer Interact*. 15, 2–3 (September 2000), 179–203. DOI:https://doi.org/10.1207/S15327051HCI1523_5

[2] Icek Ajzen. 1991. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process*. 50, 2 (December 1991), 179–211. DOI:https://doi.org/10.1016/0749-5978(91)90020-T

[3] Icek Ajzen. 2001. Nature and Operation of Attitudes. *Annu. Rev. Psychol*. 52, 1 (2001), 27–58. DOI:https://doi.org/10.1146/annurev.psych.52.1.27

[4] Icek Ajzen and Martin Fishbein. 2000. Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes. *Eur. Rev. Soc. Psychol*. 11, 1 (January 2000), 1–33. DOI:https://doi.org/10.1080/14792779943000116

[5] Ibrahim M. Al-Jabri and M. Sadiq Sohail. 2012. *Mobile Banking Adoption: Application of Diffusion of Innovation Theory*. Social Science Research Network, Rochester, NY. Retrieved October 13, 2021 from https://papers.ssrn.com/abstract=2523623

[6] Nora Alkaldi and Karen Renaud. 2016. Why Do People Adopt, or Reject, Smartphone Password Managers? Retrieved December 24, 2020 from https://www.internetsociety.org/doc/why-do-people-adopt-or-reject-smartphone-password-managers

[7] M. Alotaibi, S. Furnell, and N. Clarke. 2016. Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 352–358. DOI:https://doi.org/10.1109/ICITST.2016.7856729

[8] Mansour Alsaleh, Noura Alomar, and Abdulrahman Alarifi. 2017. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLOS ONE* 12, 3 (March 2017), e0173284. DOI:https://doi.org/10.1371/journal.pone.0173284

[9] Stephen E. Anderson. 1997. Understanding Teacher Change: Revisiting the Concerns Based Adoption Model. *Curric. Inq*. 27, 3 (1997), 331–367. DOI:https://doi.org/10.1111/0362-6784.00057

[10] Young Min Baek, Eun-mee Kim, and Young Bae. 2014. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Comput. Hum. Behav*. 31, Supplement C (February 2014), 48–56. DOI:https://doi.org/10.1016/j.chb.2013.10.010

[11] Sebastian Bamberg. 2003. How does environmental concern influence specific environmentally related behaviors? A new answer to an old question. *J. Environ. Psychol*. 23, 1 (March 2003), 21–32. DOI:https://doi.org/10.1016/S0272-4944(02)00078-6

[12] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychol. Rev*. (1977), 191–215.

[13] Albert Bandura. 2000. SOCIAL COGNITIVE THEORY: An Agentic Perspective. (2000), 28.

[14] John A. Bargh and Katelyn Y. A. McKenna. 2004. The Internet and Social Life. *Annu. Rev. Psychol*. 55, 1 (2004), 573–590. DOI:https://doi.org/10.1146/annurev.psych.55.090902.141922

[15] John A. Bargh, Katelyn Y. A. McKenna, and Grainne M. Fitzsimons. 2002. Can You See the Real Me? Activation and Expression of the "True Self" on the Internet. *J. Soc. Issues* 58, 1 (2002), 33–48. DOI:https://doi.org/10.1111/1540-4560.00247

[16] S. Bartsch and M. A. Sasse. 2012. *How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization*. UCL Department of Computer Science, London, UK. Retrieved April 2, 2019 from http://discovery.ucl.ac.uk/1389948/

[17] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and Angela Sasse. 2016. Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. 253–270. Retrieved April 2, 2019 from https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

[18] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. 2019. Smart Home Bystanders: Further Complexifying a Complex Context. (2019), 6.

[19] Jane T. Bertrand. 2004. Diffusion of Innovations and HIV/AIDS. *J. Health Commun*. 9, sup1 (January 2004), 113–121. DOI:https://doi.org/10.1080/10810730490271575

[20] Denis Besnard and Budi Arief. 2004. Computer security impaired by legitimate users. *Comput. Secur*. 23, 3 (May 2004), 253–264. DOI:https://doi.org/10.1016/j.cose.2003.09.002

[21] Alex Blau. 2017. Better Cybersecurity Starts with Fixing Your Employees' Bad Habits. *Harvard Business Review*. Retrieved December 11, 2017 from https://hbr.org/2017/12/better-cybersecurity-starts-with-fixing-your-employees-bad-habits

[22] Scott Boss, Dennis Galletta, Paul Benjamin Lowry, Gregory D. Moody, and Peter Polak. 2015. *What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors*. Social Science Research Network, Rochester, NY. Retrieved July 18, 2018 from https://papers.ssrn.com/abstract=2607190

[23] US Census Bureau. Metropolitan and Micropolitan Statistical Areas Totals: 2010-2019. *The United States Census Bureau*. Retrieved April 20, 2021 from https://www.census.gov/data/tables/time-series/demo/popest/2010s-total-metro-and-micro-statistical-areas.html

[24] Bernard Burnes and David Bargal. 2017. Kurt Lewin: 70 Years on. *J. Change Manag*. 17, 2 (April 2017), 91–100. DOI:https://doi.org/10.1080/14697017.2017.1299371

[25] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. Retrieved August 29, 2019 from https://www.usenix.org/conference/soups2019/presentation/busse

[26] John T. Cacioppo and Richard E. Petty. 1984. The Elaboration Likelihood Model of Persuasion. *ACR North Am. Adv*. NA-11, (1984). Retrieved March 4, 2019 from http://acrwebsite.org/volumes/6329/volumes/v11/NA-11

[27] Luca Canzian and Mirco Musolesi. 2015. Trajectories of depression: unobtrusive monitoring of depressive states by means of smartphone mobility traces analysis. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (UbiComp '15), Association for Computing Machinery, New York, NY, USA, 1293–1304. DOI:https://doi.org/10.1145/2750858.2805845

[28] Robert B. Cialdini. 2001. *Influence: science and practice* (4th ed ed.). Allyn and Bacon, Boston, MA.

[29] Robert B. Cialdini and Noah J. Goldstein. 2004. Social Influence: Compliance and Conformity. *Annu. Rev. Psychol*. 55, 1 (January 2004), 591–621. DOI:https://doi.org/10.1146/annurev.psych.55.090902.142015

[30] Jason Cipriani. Google signs up 150 million people for two-factor authentication: What it is, how it works. *CNET*. Retrieved January 14, 2022 from https://www.cnet.com/tech/services-and-software/google-signs-up-150-million-people-for-two-factor-authentication-what-it-is-how-it-works/

[31] Anatoli Colicev, Ashish Kumar, and Peter O'Connor. 2019. Modeling the relationship between firm and user generated content and the stages of the marketing funnel. *Int. J. Res. Mark*. 36, 1 (March 2019), 100–116. DOI:https://doi.org/10.1016/j.ijresmar.2018.09.005

[32] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), ACM, New York, NY, USA, 456:1-456:11. DOI:https://doi.org/10.1145/3173574.3174030

[33] Sunny Consolvo, David W. McDonald, and James A. Landay. 2009. Theory-driven Design Strategies for Technologies That Support Behavior Change in Everyday Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '09), ACM, New York, NY, USA, 405–414. DOI:https://doi.org/10.1145/1518701.1518766

[34] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2021. SA-13, the 13-item security attitude scale. Retrieved from https://socialcybersecurity.org/files/SA13handout.pdf

[35] Lorrie Faith Cranor. A Framework for Reasoning About the Human in the Loop. *USENIX*, 15.

[36] Lorrie Faith Cranor and Simson Garfinkel. 2005. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc.

[37] John W. Creswell and Vicki L. Plano Clark. 2017. *Designing and Conducting Mixed Methods Research*. SAGE Publications.

[38] John W. Creswell and J. David Creswell. 2017. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

[39] Reeshad S. Dalal, David J. Howard, Rebecca J. Bennett, Clay Posey, Stephen J. Zaccaro, and Bradley J. Brummel. 2021. Organizational science and cybersecurity: abundant opportunities for research at the interface. *J. Bus. Psychol.* (February 2021). DOI:https://doi.org/10.1007/s10869-021-09732-9

[40] Jonas Dalege, Denny Borsboom, Frenk van Harreveld, Helma van den Berg, Mark Conner, and Han L. J. van der Maas. 2016. Toward a formalized account of attitudes: The Causal Attitude Network (CAN) model. *Psychol. Rev.* 123, 1 (2016), 2–22. DOI:https://doi.org/10.1037/a0039802

[41] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association Berkeley, CA. Retrieved August 28, 2019 from https://www.usenix.org/conference/soups2019/presentation/das

[42] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The effect of social influence on security sensitivity. In *Proceedings of the Symposium on Usable Privacy and Security*, USENIX Association Berkeley, CA. Retrieved from https://www.usenix.org/system/files/conference/soups2014/ soups14-paper- das.pdf

[43] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (CCS '14), ACM, New York, NY, USA, 739–749. DOI:https://doi.org/10.1145/2660267.2660271

[44] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), ACM, New York, NY, USA, 1416–1426. DOI:https://doi.org/10.1145/2675133.2675225

[45] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. *ACM CHI 2018 Conf. Hum. Factors Comput. Syst.* 1, 1 (2018), 2.

[46] Fred D. Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* 13, 3 (1989), 319–340. DOI:https://doi.org/10.2307/249008

[47] Fred D. Davis. 1993. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *Int. J. Man-Mach. Stud.* 38, 3 (March 1993), 475–487. DOI:https://doi.org/10.1006/imms.1993.1022

[48] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. 1989. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Manag. Sci.* 35, 8 (August 1989), 982–1003. DOI:https://doi.org/10.1287/mnsc.35.8.982

[49] Rachel Davis, Rona Campbell, Zoe Hildon, Lorna Hobbs, and Susan Michie. 2015. Theories of behaviour and behaviour change across the social and behavioural sciences: a scoping review. *Health Psychol. Rev.* 9, 3 (August 2015), 323–344. DOI:https://doi.org/10.1080/17437199.2014.941722

[50] James W. Dearing. 2009. Applying Diffusion of Innovation Theory to Intervention Development. *Res. Soc. Work Pract.* 19, 5 (September 2009), 503–518. DOI:https://doi.org/10.1177/1049731509335569

[51] Carlo C. DiClemente and James O. Prochaska. 1998. Toward a comprehensive, transtheoretical model of change: Stages of change and addictive behaviors. In *Treating addictive behaviors, 2nd ed.* Plenum Press, New York, NY, US, 3–24. DOI:https://doi.org/10.1007/978-1-4899-1934-2_1

[52] Carlo C. DiClemente, James O. Prochaska, Scott K. Fairhurst, Wayne F. Velicer, Mary M. Velasquez, and Joseph S. Rossi. 1991. The process of smoking cessation: An analysis of precontemplation, contemplation, and preparation stages of change. *J. Consult. Clin. Psychol.* 59, 2 (1991), 295–304. DOI:https://doi.org/10.1037/0022-006X.59.2.295

[53] Carlo C. DiClemente, James O. Prochaska, and Michael Gibertini. 1985. Self-efficacy and the stages of self-change of smoking. *Cogn. Ther. Res.* 9, 2 (April 1985), 181–200. DOI:https://doi.org/10.1007/BF01204849

[54] Paul DiGioia and Paul Dourish. 2005. Social Navigation As a Model for Usable Security. In *Proceedings of the 2005 Symposium on Usable Privacy and Security* (SOUPS '05), ACM, New York, NY, USA, 101–108. DOI:https://doi.org/10.1145/1073001.1073011

[55] Tamara Dinev and Qing Hu. 2007. The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *J. Assoc. Inf. Syst.* 8, 7 (July 2007), 386–408. DOI:https://doi.org/10.17705/1jais.00133

[56] Afsaneh Doryab, Prerna Chikarsel, Xinwen Liu, and Anind K. Dey. 2019. Extraction of Behavioral Features from Smartphone and Wearable Data. *ArXiv181210394 Cs Stat* (January 2019). Retrieved February 2, 2022 from http://arxiv.org/abs/1812.10394

[57] Hugh Dubberly and Shelley Evenson. 2008. On modelingThe analysis-systhesis bridge model. *Interactions* 15, 2 (March 2008), 57–61. DOI:https://doi.org/10.1145/1340961.1340976

[58] Hugh Dubberly and Shelley Evenson. 2011. Design as learning---or "knowledge creation"---the SECI model. *Interactions* 18, 1 (January 2011), 75–79. DOI:https://doi.org/10.1145/1897239.1897256

[59] Alice H. Eagly and Shelly Chaiken. 1993. *The psychology of attitudes*. Harcourt Brace Jovanovich College Publishers, Orlando, FL, US.

[60] CSRC Content Editor. computer security - Glossary | CSRC. Retrieved May 24, 2022 from https://csrc.nist.gov/glossary/term/computer_security

[61] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), ACM, New York, NY, USA, 5257–5261. DOI:https://doi.org/10.1145/2858036.2858265

[62] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), ACM, New York, NY, USA, 2873–2882. DOI:https://doi.org/10.1145/2702123.2702249

[63] Serge Egelman and Eyal Peer. 2015. The Myth of the Average User: Improving Privacy and Security Systems Through Individualization. In *Proceedings of the 2015 New Security Paradigms Workshop* (NSPW '15), ACM, New York, NY, USA, 16–28. DOI:https://doi.org/10.1145/2841113.2841115

[64] Serge Egelman and Eyal Peer. 2015. Predicting privacy and security attitudes. *ACM SIGCAS Comput. Soc.* 45, 1 (2015), 22–28.

[65] Shelley Evenson and Hugh Dubberly. 2009. Designing for Service: Creating an Experience Advantage. In *Introduction to Service Engineering*, Gavriel Salvendy and Waldemar Karwowski (eds.). John Wiley & Sons, Inc., Hoboken, NJ, USA, 403–413. DOI:https://doi.org/10.1002/9780470569627.ch19

[66] M. Fagan and M. M. Khan. 2018. To Follow or Not to Follow: A Study of User Motivations around Cybersecurity Advice. *IEEE Internet Computing 22*, 25–34. Retrieved October 9, 2018 from doi.ieeecomputersociety.org/10.1109/MIC.2017.3301619

[67] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. 59–75. Retrieved February 10, 2021 from https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan

[68] Cori Faklaris. 2021. Components of a Model of Cybersecurity Behavior Adoption. In *7th Workshop on Security Information Workers (WSIW 2021)*, USENIX Association Berkeley, CA, Virtual event. Retrieved from https://corifaklaris.com/files/Faklaris_WSIW2021_stagemodels.pdf

[69] Cori Faklaris, Laura Dabbish, and Jason Hong. 2018. Adapting the Transtheoretical Model for the Design of Security Interventions. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, Md., USA. Retrieved December 4, 2019 from https://doi.org/10.13140/RG.2.2.15447.57760

[70] Cori Faklaris, Laura Dabbish, and Jason I Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, USENIX Association Berkeley, CA, Santa Clara, CA, 18. Retrieved from https://www.usenix.org/system/files/soups2019-faklaris.pdf

[71] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2022. Do They Accept or Resist Cybersecurity Measures? Development and Validation of the 13-Item Security Attitude Inventory (SA-13). *ArXiv220403114 Cs* (April 2022). Retrieved April 25, 2022 from http://arxiv.org/abs/2204.03114

[72] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2022. *Experimental Evidence for Using a TTM Stages of Change Model in Boosting Progress Toward 2FA Adoption*. arXiv. DOI:https://doi.org/10.48550/arXiv.2205.06937

[73] Michael D Fetters, Leslie A Curry, and John W Creswell. 2013. Achieving Integration in Mixed Methods Designs—Principles and Practices. *Health Serv. Res.* 48, 6 Pt 2 (December 2013), 2134–2156. DOI:https://doi.org/10.1111/1475-6773.12117

[74] Martin Fishbein and Icek Ajzen. 2010. *Predicting and changing behavior: The reasoned action approach*. Psychology Press, New York, NY, US.

[75] B. J. Fogg. BJ Fogg's Behavior Model. Retrieved March 15, 2018 from http://www.behaviormodel.org/

[76] B. J. Fogg and Jason Hreha. 2010. Behavior Wizard: A Method for Matching Target Behaviors with Solutions. In *Persuasive Technology*, Thomas Ploug, Per Hasle and Harri Oinas-Kukkonen (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 117–131. DOI:https://doi.org/10.1007/978-3-642-13226-1_13

[77] B. J. Fogg and Hsiang Tseng. 1999. The elements of computer credibility. ACM Press, 80–87. DOI:https://doi.org/10.1145/302979.303001

[78] B.J. Fogg, David Danielson, and Gregory Cuellar. 2007. Motivating, Influencing, and Persuading Users: An Introduction To Captology. In *The Human-Computer Interaction Handbook*, Andrew Sears and Julie Jacko (eds.). CRC Press, 133–146. DOI:https://doi.org/10.1201/9781410615862.ch7

[79] B.J. Fogg, Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangnekar, John Shon, Preeti Swani, and Marissa Treinen. 2001. *What Makes Web Sites Credible? A Report on a Large Quantitative Study*. CHI '01 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

[80] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc ACM Hum-Comput Interact* 1, CSCW (December 2017), 46:1-46:22. DOI:https://doi.org/10.1145/3134681

[81] Patrícia Pinheiro de Freitas, Mariana Carvalho de Menezes, Luana Caroline dos Santos, Adriano Marçal Pimenta, Adaliene Versiani Matos Ferreira, and Aline Cristine Souza Lopes. 2020. The transtheoretical model is an effective weight management intervention: a randomized controlled trial. *BMC Public Health* 20, 1 (December 2020), 652. DOI:https://doi.org/10.1186/s12889-020-08796-1

[82] Jon Froehlich, Tawanna Dillahunt, Predrag Klasnja, Jennifer Mankoff, Sunny Consolvo, Beverly Harrison, and James A. Landay. 2009. UbiGreen: Investigating a Mobile Tool for Tracking and Supporting Green Transportation Habits. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '09), ACM, New York, NY, USA, 1043–1052. DOI:https://doi.org/10.1145/1518701.1518861

[83] John M. Gallaugher and Yu-Ming Wang. 2002. Understanding Network Effects in Software Markets: Evidence from Web Server Pricing. *MIS Q.* 26, 4 (2002), 303–327. DOI:https://doi.org/10.2307/4132311

[84] Simson Garfinkel, Gene Spafford, and Alan Schwartz. 2003. *Practical UNIX and Internet Security*. O'Reilly Media, Inc.

[85] Shirley Gaw, Edward W. Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '06), Association for Computing Machinery, New York, NY, USA, 591–600. DOI:https://doi.org/10.1145/1124772.1124862

[86] Andrew R. Gillam and W. Tad Foster. 2020. Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Comput. Hum. Behav.* 108, (July 2020), 106319. DOI:https://doi.org/10.1016/j.chb.2020.106319

[87] Karen Glanz and Donald B. Bishop. 2010. The Role of Behavioral Science Theory in Development and Implementation of Public Health Interventions. *Annu. Rev. Public Health* 31, 1 (2010), 399–418. DOI:https://doi.org/10.1146/annurev.publhealth.012809.103604

[88] Karen Glanz, Barbara K. Rimer, and K. Viswanath. 2008. *Health Behavior and Health Education: Theory, Research, and Practice*. John Wiley & Sons.

[89] Frank L. Greitzer, Jeremy R. Strozer, Sholom Cohen, Andrew P. Moore, David Mundie, and Jennifer Cowley. 2014. Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In *2014 IEEE Security and Privacy Workshops*, 236–250. DOI:https://doi.org/10.1109/SPW.2014.39

[90] Andrea Grimes, Vasudhara Kantroo, and Rebecca E. Grinter. 2010. Let's Play!: Mobile Health Games for Adults. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (UbiComp '10), ACM, New York, NY, USA, 241–250. DOI:https://doi.org/10.1145/1864349.1864370

[91] Rebecca E. Grinter, W. Keith Edwards, Marshini Chetty, Erika S. Poole, Ja-Young Sung, Jeonghwa Yang, Andy Crabtree, Peter Tolmie, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2009. The ins and outs of home networking: The case for useful and usable domestic networking. *ACM Trans. Comput.-Hum. Interact.* 16, 2 (June 2009), 8:1-8:28. DOI:https://doi.org/10.1145/1534903.1534905

[92] Martin S. Hagger. 2016. Non-conscious processes and dual-process theories in health psychology. *Health Psychol. Rev.* 10, 4 (October 2016), 375–380. DOI:https://doi.org/10.1080/17437199.2016.1244647

[93] Gene E. Hall. 1974. The Concerns-Based Adoption Model: A Developmental Conceptualization of the Adoption Process Within Educational Institutions. (February 1974). Retrieved May 13, 2022 from https://eric.ed.gov/?id=ED111791

[94] Heesup Han and Hae Jin Yoon. 2015. Hotel customers' environmentally responsible behavioral intention: Impact of key constructs on decision in green consumerism. *Int. J. Hosp. Manag.* 45, (February 2015), 22–33. DOI:https://doi.org/10.1016/j.ijhm.2014.11.004

[95] Ho Han, Kelley Pettee Gabriel, and Harold Willis Kohl Iii. 2017. Application of the transtheoretical model to sedentary behaviors and its association with physical activity status. *PLOS ONE* 12, 4 (April 2017), e0176330. DOI:https://doi.org/10.1371/journal.pone.0176330

[96] Julie Haney, Wayne Lutters, and Jody Jacobs. 2021. Cybersecurity Advocates: Force Multipliers in Security Behavior Change. *IEEE Secur. Priv.* 19, 4 (July 2021), 54–59. DOI:https://doi.org/10.1109/MSEC.2021.3077405

[97] Julie M Haney and Wayne G Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*, USENIX Association Berkeley, CA, Baltimore, Maryland, USA, 16.

[98] Bruce Hanington and Bella Martin. 2012. *Universal Methods of Design: 100 Ways to Research Complex Problems, Develop Innovative Ideas, and Design Effective Solutions*. Rockport Publishers.

[99] Bartlomiej Hanus and Yu "Andy" Wu. 2016. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Inf. Syst. Manag.* 33, 1 (January 2016), 2–16. DOI:https://doi.org/10.1080/10580530.2015.1117842

[100] Eddie Harmon-Jones and Judson Mills. 2019. An introduction to cognitive dissonance theory and an overview of current perspectives on the theory. In *Cognitive dissonance: Reexamining a pivotal theory in psychology (2nd ed.)*., Eddie Harmon-Jones (ed.). American Psychological Association, Washington, 3–24. DOI:https://doi.org/10.1037/0000135-001

[101] Larry Hatcher. 2013. *Advanced statistics in research: Reading, understanding, and writing up data analysis results*. ShadowFinch Media, LLC.

[102] Yasser M. Hausawi and William H. Allen. 2014. An Assessment Framework for Usable-Security Based on Decision Science. In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (eds.). Springer International Publishing, Cham, 33–44. DOI:https://doi.org/10.1007/978-3-319-07620-1_4

[103] Katharine J. Head, Seth M. Noar, Nicholas T. Iannarino, and Nancy Grant Harrington. 2013. Efficacy of text messaging-based interventions for health promotion: A meta-analysis. *Soc. Sci. Med.* 97, (November 2013), 41–48. DOI:https://doi.org/10.1016/j.socscimed.2013.08.003

[104] Hilary Putnam. 1980. The nature of mental states. In *Readings in philosophy of psychology*. 223–231. Retrieved October 7, 2021 from http://www.kaley-bradley.com/McDaniel/courses/spring_2012/MandM/readings/Putnam.PDF

[105] Helge G. Hollmeyer, Frederick Hayden, Gregory Poland, and Udo Buchholz. 2009. Influenza vaccination of health care workers in hospitals—A review of studies on attitudes and predictors. *Vaccine* 27, 30 (June 2009), 3935–3944. DOI:https://doi.org/10.1016/j.vaccine.2009.03.056

[106] Kasper Hornbæk and Morten Hertzum. 2017. Technology Acceptance and User Experience: A Review of the Experiential Component in HCI. *ACM Trans. Comput.-Hum. Interact.* 24, 5 (October 2017), 1–30. DOI:https://doi.org/10.1145/3127358

[107] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. 2012. The Psychology of Security for the Home Computer User. In *2012 IEEE Symposium on Security and Privacy*, 209–223. DOI:https://doi.org/10.1109/SP.2012.23

[108] Matthew Hull, Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. 2021. Understanding individual differences: factors affecting secure computer behaviour. *Behav. Inf. Technol.* 0, 0 (October 2021), 1–27. DOI:https://doi.org/10.1080/0144929X.2021.1977849

[109] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. 327–346. Retrieved March 27, 2020 from https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[110] Mohammad S. Jalali, Maike Bruckes, Daniel Westmattelmann, and Gerhard Schewe. 2020. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *J. Med. Internet Res.* 22, 1 (2020), e16775. DOI:https://doi.org/10.2196/16775

[111] James R Mahalik, Michael Di Bianca, and Michael P Harris. 2021. Men's attitudes toward mask-wearing during COVID-19: Understanding the complexities of mask-ulinity. *J. Health Psychol.* (February 2021). DOI:https://doi.org/10.1177/1359105321990793

[112] Irving L. Janis and Leon Mann. 1977. *Decision making: A psychological analysis of conflict, choice, and commitment*. Free Press, New York, NY, US.

[113] Daniel Kahneman. 2011. *Thinking, Fast and Slow*. Macmillan.

[114] Daniel Kahneman and Amos Tversky. 1979. Prospect Theory: An Analysis of Decision Making Under Risk. *Econometrica* 47, 2 (March 1979), 262–292. Retrieved July 19, 2021 from http://links.jstor.org/sici?sici=0012-9682%28197903%2947%3A2%3C263%3APTAAOD%3E2.0.CO%3B2-3

[115] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association Berkeley, CA, 39–52. Retrieved from https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

[116] Joseph "Jofish" Kaye. 2011. Self-reported Password Sharing Strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), ACM, New York, NY, USA, 2619–2622. DOI:https://doi.org/10.1145/1978942.1979324

[117] J A Kelly, J S St Lawrence, L Y Stevenson, A C Hauth, S C Kalichman, Y E Diaz, T L Brasfield, J J Koob, and M G Morgan. 1992. Community AIDS/HIV risk reduction: the effects of endorsements by popular people in three cities. *Am. J. Public Health* 82, 11 (November 1992), 1483–1489. DOI:https://doi.org/10.2105/AJPH.82.11.1483

[118] Vijay Khatri, Binny M. Samuel, and Alan R. Dennis. 2018. System 1 and System 2 cognition in the decision to adopt and use a new technology. *Inf. Manage.* 55, 6 (September 2018), 709–724. DOI:https://doi.org/10.1016/j.im.2018.03.002

[119] Alison Kirk, Freya MacMillan, and Nikki Webster. 2010. Application of the Transtheoretical model to physical activity in older adults with Type 2 diabetes and/or cardiovascular disease. *Psychol. Sport Exerc.* 11, 4 (July 2010), 320–324. DOI:https://doi.org/10.1016/j.psychsport.2010.03.001

[120] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. 2015. "Shadow Security" As a Tool for the Learning Organization. *SIGCAS Comput Soc* 45, 1 (February 2015), 29–37. DOI:https://doi.org/10.1145/2738210.2738216

[121] Predrag Klasnja, Sunny Consolvo, and Wanda Pratt. 2011. How to Evaluate Technologies for Health Behavior Change in HCI Research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '11), ACM, New York, NY, USA, 3063–3072. DOI:https://doi.org/10.1145/1978942.1979396

[122] Stephen J. Kraus. 1995. Attitudes and the Prediction of Behavior: A Meta-Analysis of the Empirical Literature. *Pers. Soc. Psychol. Bull.* 21, 1 (January 1995), 58–75. DOI:https://doi.org/10.1177/0146167295211007

[123] Matthew W. Kreuter, David W. Farrell, Laura R. Olevitch, Laura K. Brennan, David W. Farrell, Laura R. Olevitch, and Laura K. Brennan. 2013. *Tailoring Health Messages : Customizing Communication With Computer Technology*. Routledge. DOI:https://doi.org/10.4324/9781315045382

[124] Matthew W. Kreuter and Ricardo J. Wray. 2003. Tailored and Targeted Health Communication: Strategies for Enhancing Information Relevance. *Am. J. Health Behav.* 27, 1 (November 2003), 227–232. DOI:https://doi.org/10.5993/AJHB.27.1.s3.6

[125] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J. Wisniewski. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW3 (January 2021), 255:1-255:27. DOI:https://doi.org/10.1145/3432954

[126] Sebastian Kurowski and Heiko Roßnagel. On the diffusion of security behaviours. 14.

[127] C. Lee. 1993. Attitudes, knowledge, and stages of change: a survey of exercise patterns in older Australian women. *Health Psychol. Off. J. Div. Health Psychol. Am. Psychol. Assoc.* 12, 6 (November 1993), 476–480.

[128] James J. Lin, Lena Mamykina, Silvia Lindtner, Gregory Delajoux, and Henry B. Strub. 2006. Fish'N'Steps: Encouraging Physical Activity with an Interactive Computer Game. In *Proceedings of the 8th International Conference on Ubiquitous Computing* (UbiComp'06), Springer-Verlag, Berlin, Heidelberg, 261–278. DOI:https://doi.org/10.1007/11853565_16

[129] Junchao Lin, Jason I. Hong, and Laura Dabbish. 2021. "It's our mutual responsibility to share": The Evolution of Account Sharing in Romantic Couples. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1 (April 2021), 160:1-160:27. DOI:https://doi.org/10.1145/3449234

[130] Yuping Liu and L. J. Shrum. 2009. A Dual-Process Model of Interactivity Effects. *J. Advert.* 38, 2 (July 2009), 53–68. DOI:https://doi.org/10.2753/JOA0091-3367380204

[131] Mary Madden and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance | Pew Research Center. Retrieved February 28, 2019 from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[132] Thomas J. Madden, Pamela Scholder Ellen, and Icek Ajzen. 1992. A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *Pers. Soc. Psychol. Bull.* 18, 1 (February 1992), 3–9. DOI:https://doi.org/10.1177/0146167292181001

[133] James E Maddux and Ronald W Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol.* 19, 5 (September 1983), 469–479. DOI:https://doi.org/10.1016/0022-1031(83)90023-9

[134] Johannes Mander, Martin Teufel, Katharina Keifenheim, Stephan Zipfel, and Katrin Elisabeth Giel. 2013. Stages of change, treatment outcome and therapeutic alliance in adult inpatients with chronic anorexia nervosa. *BMC Psychiatry* 13, (April 2013), 111. DOI:https://doi.org/10.1186/1471-244X-13-111

[135] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 5921–5932. Retrieved August 29, 2021 from https://doi.org/10.1145/2858036.2858051

[136] Katelyn Y. A. McKenna and John A. Bargh. 1999. Causes and Consequences of Social Interaction on the Internet: A Conceptual Framework. *Media Psychol.* 1, 3 (September 1999), 249–269. DOI:https://doi.org/10.1207/s1532785xmep0103_4

[137] Philip Menard, Gregory J. Bott, and Robert E. Crossler. 2017. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *J. Manag. Inf. Syst.* 34, 4 (October 2017), 1203–1230. DOI:https://doi.org/10.1080/07421222.2017.1394083

[138] Tamir Mendel and Eran Toch. 2017. Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '17), Association for Computing Machinery, New York, NY, USA, 581–593. DOI:https://doi.org/10.1145/2998181.2998323

[139] Carol Mershon and Olga Shvetsova. 2019. *Formal Modeling in Social Science*. University of Michigan Press.

[140] Gary Meyer. 2004. Diffusion Methodology: Time to Innovate? *J. Health Commun.* 9, sup1 (January 2004), 59–69. DOI:https://doi.org/10.1080/10810730490271539

[141] Robert J. Meyers, Hendrik G. Roozen, and Jane Ellen Smith. 2011. The Community Reinforcement Approach. *Alcohol Res. Health* 33, 4 (2011), 380–388. Retrieved December 22, 2017 from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3860533/

[142] Susan Michie, Maartje M. van Stralen, and Robert West. 2011. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implement. Sci.* 6, 1 (April 2011), 42. DOI:https://doi.org/10.1186/1748-5908-6-42

[143] Susan Michie, Robert West, Kate Sheals, and Cristina A. Godinho. 2018. Evaluating the effectiveness of behavior change techniques in health-related behavior: a scoping review of methods used. *Transl. Behav. Med.* 8, 2 (March 2018), 212–224. DOI:https://doi.org/10.1093/tbm/ibx019

[144] Gary C. Moore and Izak Benbasat. 1991. Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Inf. Syst. Res.* 2, 3 (September 1991), 192–222. DOI:https://doi.org/10.1287/isre.2.3.192

[145] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1 (April 2021), 1–24. DOI:https://doi.org/10.1145/3449212

[146] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know your enemy: the risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, ACM, 271–280.

[147] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P. Knijnenburg. 2020. Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. *Proc. Priv. Enhancing Technol.* 2020, 1 (January 2020), 83–102. DOI:https://doi.org/10.2478/popets-2020-0006

[148] Seth M. Noar, Christina N. Benac, and Melissa S. Harris. 2007. Does tailoring matter? Meta-analytic review of tailored print health behavior change interventions. *Psychol. Bull.* 133, 4 (2007), 673–693. DOI:https://doi.org/10.1037/0033-2909.133.4.673

[149] Kenneth Olmstead and Aaron Smith. 2017. Americans and Cybersecurity. *Pew Research Center: Internet, Science & Tech*. Retrieved November 6, 2017 from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[150] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, USENIX Association Berkeley, CA, Baltimore, Md., USA, 83–102. Retrieved February 26, 2019 from https://www.usenix.org/conference/soups2018/presentation/park

[151] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. 319–338. Retrieved July 15, 2021 from https://www.usenix.org/conference/soups2019/presentation/pearman

[152] Sandy Kristin Piderit. 2000. Rethinking Resistance and Recognizing Ambivalence: A Multidimensional View of Attitudes Toward an Organizational Change. *Acad. Manage. Rev.* 25, 4 (October 2000), 783–794. DOI:https://doi.org/10.5465/amr.2000.3707722

[153] Ronald C. Plotnikoff and Linda Trinh. 2010. Protection Motivation Theory: Is This a Worthwhile Theory for Physical Activity Promotion? *Exerc. Sport Sci. Rev.* 38, 2 (April 2010), 91–98. DOI:https://doi.org/10.1097/JES.0b013e3181d49612

[154] Erika Shehan Poole, Marshini Chetty, Rebecca E. Grinter, and W. Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems* (DIS '08), Association for Computing Machinery, New York, NY, USA, 455–464. DOI:https://doi.org/10.1145/1394445.1394494

[155] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E. Grinter, and W. Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '09), Association for Computing Machinery, New York, NY, USA, 739–748. DOI:https://doi.org/10.1145/1518701.1518816

[156] Erika Shehan Poole, W Keith Edwards, and Lawrence Jarvis. The Home Network as a Socio-Technical System: Understanding the Challenges of Remote Home Network Problem Diagnosis. 23.

[157] J. O. Prochaska and W. F. Velicer. 1997. The transtheoretical model of health behavior change. *Am. J. Health Promot. AJHP* 12, 1 (October 1997), 38–48.

[158] James O. Prochaska and Carlo C. DiClemente. 1983. Stages and processes of self-change of smoking: Toward an integrative model of change. *J. Consult. Clin. Psychol.* 51, 3 (1983), 390–395. DOI:https://doi.org/10.1037/0022-006X.51.3.390

[159] James O. Prochaska, Julie A. Wright, and Wayne F. Velicer. 2008. Evaluating theories of health behavior change: A hierarchy of criteria applied to the transtheoretical model. *Appl. Psychol. Int. Rev.* 57, 4 (2008), 561–588. DOI:https://doi.org/10.1111/j.1464-0597.2008.00345.x

[160] Leilei Qu, Cheng Wang, Ruojin Xiao, Jianwei Hou, Wenchang Shi, and Bin Liang. 2019. Towards Better Security Decisions: Applying Prospect Theory to Cybersecurity. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI EA '19), ACM, New York, NY, USA, LBW2613:1-LBW2613:6. DOI:https://doi.org/10.1145/3290607.3312782

[161] Christina A. Rader, Richard P. Larrick, and Jack B. Soll. 2017. Advice as a form of social influence: Informational motives and the consequences for accuracy. *Soc. Personal. Psychol. Compass* 11, 8 (August 2017), n/a-n/a. DOI:https://doi.org/10.1111/spc3.12329

[162] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *J. Cybersecurity* 1, 1 (September 2015), 121–144. DOI:https://doi.org/10.1093/cybsec/tyv008

[163] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS '12)*, USENIX Association Berkeley, CA, 1. DOI:https://doi.org/10.1145/2335356.2335364

[164] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*, 272–288. DOI:https://doi.org/10.1109/SP.2016.24

[165] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (CCS '16), ACM, New York, NY, USA, 666–677. DOI:https://doi.org/10.1145/2976749.2978307

[166] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where is the Digital Divide?: A Survey of Security, Privacy, and Socioeconomics. ACM Press, 931–936. DOI:https://doi.org/10.1145/3025453.3025673

[167] Everett M Rogers. 2002. Diffusion of preventive innovations. *Addict. Behav.* 27, 6 (November 2002), 989–993. DOI:https://doi.org/10.1016/S0306-4603(02)00300-3

[168] Everett M. Rogers. 2010. *Diffusion of Innovations, 4th Edition*. Simon and Schuster.

[169] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol.* 91, 1 (September 1975), 93–114. DOI:https://doi.org/10.1080/00223980.1975.9915803

[170] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. 2017. Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture. 211–228. Retrieved February 11, 2021 from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/ruoti

[171] Ismail Sahin. 2005. UNDERSTANDING FACULTY ADOPTION OF TECHNOLOGY USING THE LEARNING/ADOPTION TRAJECTORY MODEL: A QUALITATIVE CASE STUDY. *Turk. Online J. Educ. Technol.* 4, 1 (2005), 10.

[172] Ismail Sahin and Ann Thompson. 2007. Analysis of Predictive Factors That Influence Faculty Members Technology Adoption Level. *J. Technol. Teach. Educ.* 15, 2 (April 2007), 167–190. Retrieved July 28, 2021 from https://www.learntechlib.org/primary/p/18935/

[173] Johnny Saldaña. 2013. *The coding manual for qualitative researchers* (2nd ed ed.). SAGE, Los Angeles.

[174] Malek Ben Salem, Shlomo Hershkop, and Salvatore J. Stolfo. 2008. A Survey of Insider Attack Detection Research. In *Insider Attack and Cyber Security: Beyond the Hacker*, Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith and Sara Sinclair (eds.). Springer US, Boston, MA, 69–90. DOI:https://doi.org/10.1007/978-0-387-77322-3_5

[175] Ayane Sano, Yukiko Sawaya, Akira Yamada, and Ayumu Kubota. 2021. SeBeST: Security Behavior Stage Model and Its Application to OS Update. In *Advanced Information Networking and Applications* (Lecture Notes in Networks and Systems), Springer International Publishing, Cham, 552–566. DOI:https://doi.org/10.1007/978-3-030-75075-6_45

[176] Ayane Sano, Yukiko Sawaya, Akira Yamada, Ayumu Kubota, and Takamasa Isohara. 2021. Designing Personalized OS Update Message based on Security Behavior Stage Model. In *2021 18th International Conference on Privacy, Security and Trust (PST)*, 1–9. DOI:https://doi.org/10.1109/PST52912.2021.9647792

[177] M. A. Sasse, S. Brostoff, and D. Weirich. 2001. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technol. J.* 19, 3 (July 2001), 122–131. DOI:https://doi.org/10.1023/A:1011902718709

[178] Paul van Schaik, Karen Renaud, Jurjen Jansen, and Joseph Onibokun. 2019. Risk as affect: the affect heuristic in cybersecurity. *Comput. Secur.* (October 2019), 101651. DOI:https://doi.org/10.1016/j.cose.2019.101651

[179] Bruce Schneier. 2008. The Psychology of Security. In *Progress in Cryptology – AFRICACRYPT 2008* (Lecture Notes in Computer Science), Springer, Berlin, Heidelberg, 50–79. DOI:https://doi.org/10.1007/978-3-540-68164-9_5

[180] Tara Seals. 2017. Cost of User Security Training Tops $290K Per Year. *Infosecurity Magazine*. Retrieved January 20, 2021 from https://www.infosecurity-magazine.com:443/news/cost-of-user-security-training/

[181] Savannah Wei Shi and Jie Zhang. 2014. Usage Experience with Decision Aids and Evolution of Online Purchase Behavior. *Mark. Sci.* 33, 6 (November 2014), 871–882. DOI:https://doi.org/10.1287/mksc.2014.0872

[182] Grace Shin, Yuanyuan Feng, Mohammad Hossein Jarrahi, and Nicci Gafinowitz. 2019. Beyond novelty effect: a mixed-methods exploration into the motivation for long-term activity tracker use. *JAMIA Open* 2, 1 (April 2019), 62–72. DOI:https://doi.org/10.1093/jamiaopen/ooy048

[183] Herbert A. Simon. 1988. The Science of Design: Creating the Artificial. *Des. Issues* 4, 1/2 (original 1969 1988), 67–82. DOI:https://doi.org/10.2307/1511391

[184] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password Sharing: Implications for Security Design Based on Social Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '07), ACM, New York, NY, USA, 895–904. DOI:https://doi.org/10.1145/1240624.1240759

[185] Zhanna Malekos Smith, Eugenia Lostri, and James A Lewis. 2020. *The Hidden Costs of Cybercrime*. McAfee.

[186] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. *Proc ACM Hum-Comput Interact* 3, CSCW (November 2019), 83:1-83:25. DOI:https://doi.org/10.1145/3359185

[187] Allan Steckler, Robert M. Goodman, Kenneth R. McLeroy, Sonia Davis, and Gary Koch. 1992. Measuring the Diffusion of Innovative Health Promotion Programs. *Am. J. Health Promot.* 6, 3 (January 1992), 214–224. DOI:https://doi.org/10.4278/0890-1171-6.3.214

[188] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proc. Priv. Enhancing Technol.* 2021, 3 (July 2021), 308–333. DOI:https://doi.org/10.2478/popets-2021-0049

[189] B. Studer and S. Knecht. 2016. Chapter 2 - A benefit–cost framework of motivation for a specific activity. In *Progress in Brain Research*, Bettina Studer and Stefan Knecht (eds.). Elsevier, 25–47. DOI:https://doi.org/10.1016/bs.pbr.2016.06.014

[190] Pei-Ju Lucy Ting. 2006. The Transtheoretical Model, Stages of Change and Decisional Balance as Predictors of Behavioural Change in Internet Privacy and Security. Ph.D. University of Manchester. Retrieved February 8, 2018 from http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.603434

[191] Endel Tulving and Neal Kroll. 1995. Novelty assessment in the brain and long-term memory encoding. *Psychon. Bull. Rev.* 2, 3 (September 1995), 387–390. DOI:https://doi.org/10.3758/BF03210977

[192] Wendelien Van Eerde and Henk Thierry. 1996. Vroom's expectancy models and work-related criteria: A meta-analysis. *J. Appl. Psychol.* 81, 5 (1996), 575–586. DOI:https://doi.org/10.1037/0021-9010.81.5.575

[193] Kami E. Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by Updates: How Negative Experiences Affect Future Security. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems* (CHI '14), ACM, New York, NY, USA, 2671–2674. DOI:https://doi.org/10.1145/2556288.2557275

[194] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of Software Updates: The Process of Updating Software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), ACM, New York, NY, USA, 3215–3226. DOI:https://doi.org/10.1145/2858036.2858303

[195] Julio Vega, Meng Li, Kwesi Aguillera, Nikunj Goel, Echhit Joshi, Kirtiraj Khandekar, Krina C. Durica, Abhineeth R. Kunta, and Carissa A. Low. 2021. Reproducible Analysis Pipeline for Data Streams: Open-Source Software to Process Data Collected With Mobile Devices. *Front. Digit. Health* 3, (2021). Retrieved February 2, 2022 from https://www.frontiersin.org/article/10.3389/fdgth.2021.769823

[196] Wayne F. Velicer, Carlo C. DiClemente, James O. Prochaska, and Nancy Brandenburg. 1985. Decisional balance measure for assessing and predicting smoking status. *J. Pers. Soc. Psychol.* 48, 5 (1985), 1279.

[197] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *Manag. Inf. Syst. Q.* 27, 3 (2003), 5.

[198] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True": The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proc ACM Hum-Comput Interact* 2, CSCW (November 2018), 176:1-176:25. DOI:https://doi.org/10.1145/3274445

[199] Emily a Vogels and Monica Anderson. 2019. Americans and Digital Knowledge. *Pew Research Center: Internet, Science & Tech*. Retrieved January 14, 2022 from https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/

[200] V.H. Vroom. 1964. *Work and motivation*. Wiley, Oxford, England.

[201] Serena Wang, Cori Faklaris, Junchao Lin, Laura Dabbish, and Jason I. Hong. 2022. "It's Problematic but I'm not Concerned": University Perspectives on Account Sharing. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1 (March 2022), 1–27. DOI:https://doi.org/10.1145/3512915

[202] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), ACM, New York, NY, USA, 11:1-11:16. DOI:https://doi.org/10.1145/1837110.1837125

[203] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training?: Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), ACM, New York, NY, USA, 492:1-492:12. DOI:https://doi.org/10.1145/3173574.3174066

[204] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. 309–325. Retrieved May 25, 2022 from https://www.usenix.org/conference/soups2015/proceedings/presentation/wash
[205] Steven Weber. 2017. Coercion in cybersecurity: What public health models reveal. *J. Cybersecurity* 3, 3 (November 2017), 173–183. DOI:https://doi.org/10.1093/cybsec/tyx005
[206] Neil D. Weinstein. 1989. Effects of personal experience on self-protective behavior. *Psychol. Bull.* 105, 1 (1989), 31–50. DOI:https://doi.org/10.1037/0033-2909.105.1.31
[207] Neil D. Weinstein. 2007. Misleading tests of health behavior theories. *Ann. Behav. Med.* 33, 1 (February 2007), 1–10. DOI:https://doi.org/10.1207/s15324796abm3301_1
[208] Neil D Weinstein, Judith E Lyon, and Peter M Sandman. 1998. Experimental Evidence for Stages of Health Behavior Change: The Precaution Adoption Process Model Applied to Home Radon Testing. *Health Psychol.* 17, 5 (1998), 445–453. DOI:https://doi.org/10.1037/0278-6133.17.5.445
[209] Neil D. Weinstein, Alexander J. Rothman, and Stephen R. Sutton. 1998. Stage theories of health behavior: Conceptual and methodological issues. *Health Psychol.* 17, 3 (1998), 290–299. DOI:https://doi.org/10.1037/0278-6133.17.3.290
[210] Neil D. Weinstein and Peter M. Sandman. 1992. A model of the precaution adoption process: Evidence from home radon testing. *Health Psychol.* 11, 3 (1992), 170–180. DOI:https://doi.org/10.1037/0278-6133.11.3.170
[211] Dirk Weirich and Martina Angela Sasse. 2001. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (NSPW '01), Association for Computing Machinery, New York, NY, USA, 137–143. DOI:https://doi.org/10.1145/508171.508195
[212] Robert S. Weiss. 1995. *Learning From Strangers: The Art and Method of Qualitative Interview Studies*. Simon and Schuster.
[213] Alma Whitten and J D Tygar. 1999. A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, USENIX Association Berkeley, CA, Washington, DC, US, 169–184.
[214] Emma J. Williams, Jan Noyes, and Bogdan Warinschi. 2018. How Do We Ensure Users Engage In Secure Online Behavior? A Psychological Perspective. DOI:https://doi.org/10.5176/2251-1865_CBP18.49
[215] Jim Witschey, Shundan Xiao, and Emerson Murphy-Hill. 2014. Technical and personal factors influencing developers' adoption of security tools. In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, 23–26.
[216] Jim Witschey, Olga Zielinska, Allaire Welk, Emerson Murphy-Hill, Chris Mayhorn, and Thomas Zimmermann. 2015. Quantifying developers' adoption of security tools. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, ACM, Bergamo Italy, 260–271. DOI:https://doi.org/10.1145/2786805.2786816
[217] Jason S. Wrench, Candice Thomas-Maddox, Virginia Peck Richmond, and James C. McCroskey. 2013. *Quantitative Research Methods for Communication: A Hands-On Approach* (2nd ed.). Oxford University Press, Inc., USA.
[218] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *Proceedings of the 43rd IEEE Symposium on Security & Privacy*, IEEE Computer Society, Oakland, CA, USA, 17. Retrieved from https://sauvikdas.com/uploads/paper/pdf/36/file.pdf
[219] Shundan Xiao, Jim Witschey, and Emerson Murphy-Hill. 2014. Social influences on secure development tool adoption: why security tools spread. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, ACM, Baltimore Maryland USA, 1095–1106. DOI:https://doi.org/10.1145/2531602.2531722
[220] Yen, David C., Wu, Chin-Shan, Cheng, Fei-Fei, and Huang, Yu-Wen. 2010. Determinants of users' intention to adopt wireless technology: An empirical study by integrating TTF with TAM - ScienceDirect. *Comput. Hum. Behav.* 26, 5 (September 2010), 906–915. DOI:https://doi.org/10.1016/j.chb.2010.02.005
[221] Youngwha Lee and Kenneth A. Kozar. 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective - ScienceDirect. *Inf. Manage.* 45, 2 (March 2008), 109–119. DOI:https://doi.org/10.1016/j.im.2008.01.002
[222] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–15. DOI:https://doi.org/10.1145/3313831.3376570
[223] 2002. *Capability Maturity Model® Integration for Software Engineering (CMMI-SW), Version 1.1*. Carnegie Mellon Software Engineering Institute, Pittsburgh, Pennsylvania. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14069.pdf
[224] 2010. Triangulation. In *Encyclopedia of Research Design*. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States. DOI:https://doi.org/10.4135/9781412961288.n469
[225] 2017. Social influence. *Wikipedia*. Retrieved September 13, 2017 from https://en.wikipedia.org/w/index.php?title=Social_influence&oldid=800243709
[226] 2019. *2019 Data Breach Investigations Report*. Verizon Enterprise. Retrieved May 8, 2019 from https://enterprise.verizon.com/resources/reports/dbir/
[227] 2020. *2020 Data Breach Investigations Report*. Verizon Enterprise. Retrieved May 28, 2020 from https://enterprise.verizon.com/resources/reports/dbir/
[228] 2020. Ponemon Report 2020 Cost of Insider Threats: Global. *ObserveIT*. Retrieved May 29, 2020 from https://www.observeit.com/2020costofinsiderthreat/
[229] 2020. Aces in Places: 5 characteristics of a Super User. *Sekoia UK*. Retrieved February 9, 2021 from https://sekoia.co.uk/news/aces-in-places-5-characteristics-of-a-super-user/
[230] 2021. New Year, New Digital You: Consumer Security Findings from McAfee's Latest Report. *McAfee Blogs*. Retrieved September 19, 2021 from https://www.mcafee.com/blogs/internet-security/new-year-new-digital-you-consumer-security-findings-from-mcafees-latest-report/
[231] 2021. List of metropolitan statistical areas. *Wikipedia*. Retrieved July 21, 2021 from https://en.wikipedia.org/w/index.php?title=List_of_metropolitan_statistical_areas&oldid=1034742128
[232] 2021. Making sign-in safer and more convenient. *Google*. Retrieved January 14, 2022 from https://blog.google/technology/safety-security/making-sign-safer-and-more-convenient/
[233] [Tessian Research] The Psychology of Human Error.pdf. Retrieved October 29, 2021 from https://f.hubspotusercontent20.net/hubfs/1670277/%5BTessian%20Research%5D%20The%20Psychology%20of%20Human%20Error.pdf?__hstc=1

70273983.6aa213222a25e91ce29bfd9645578315.1635528205207.1635528205207.1635528205207.1&__hssc=170273983.5.1635528205208&__hsfp=3390846970
[234] Proofpoint's Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click | Proofpoint US. Retrieved October 29, 2021 from https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more
[235] The psychology of cyberthreats. *https://www.apa.org*. Retrieved February 15, 2019 from https://www.apa.org/monitor/2019/02/cyberthreats
[236] 2021 Data Breach Investigations Report. *Verizon Business*. Retrieved September 19, 2021 from https://www.verizon.com/business/resources/reports/dbir/
[237] Capability Maturity Model (CMM). Retrieved February 7, 2018 from http://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model?vgnextfmt=print
[238] Home : Oxford English Dictionary. Retrieved January 15, 2022 from https://www.oed.com/
[239] Less Than 1 in 10 Gmail Users Enable Two-Factor Authentication - Slashdot. Retrieved January 18, 2018 from https://tech.slashdot.org/story/18/01/18/1836259/less-than-1-in-10-gmail-users-enable-two-factor-authentication
[240] What is Usability? *The Interaction Design Foundation*. Retrieved May 24, 2022 from https://www.interaction-design.org/literature/topics/usability
[241] About the TTM - HABITS Lab - UMBC. Retrieved June 25, 2018 from https://habitslab.umbc.edu/the-model/
[242] The Relationship Between Super Users' Attitudes and Employee Experiences With Clinical Information Systems - Jonathon R. B. Halbesleben, Douglas S. Wakefield, Marcia M. Ward, Jane Brokel, Donald Crandall, 2009. Retrieved February 9, 2021 from https://journals.sagepub.com/doi/abs/10.1177/1077558708325984?casa_token=y9eEqs0hv1oAAAAA:P7MawikERAP70REXSfrO7_o_agbTZnHeoF0fzbeSRvmertwIY5uI2m9H2o1R0nh32ODurnp25BUsOQ

APPENDICES

Appendix A: Phase 1 Screener Survey and Scoring Method

A.1 Phase 1 Screener Survey

Q1.1 [Study Information and Consent Form]

[page break]
Q2.1 Before we begin, please enter your email address.
We will use this to send you a gift card for the completed survey and to contact you if we would like to arrange a follow-up interview.

_____

Note that, due to the volume of spam received, this email address is not considered evidence that your completed survey is valid. We may reject your response if the survey metadata reports duplication, low response quality and/or non-U.S. location, if the recorded duration of the survey seems inconsistent with manual human response, or if your response fails attention checks.

[page break]
Q3.1 For each of the following practices, please indicate the statement that best describes your level of awareness of it.
For more explanation of each practice, see this link: http://bit.ly/ITpractices

	I am familiar with this practice. (4)	I am aware of this practice, but not familiar with it. (3)	I am not aware of this practice. (2)	Not sure. (1)	N/A (0)
Using online account passwords that are strong. (1)	○	○	○	○	○
Using online account passwords that are unique. (2)	○	○	○	○	○
Using two-factor authentication (2FA) for online accounts. (3)	○	○	○	○	○
Using a password manager for online accounts. (4)	○	○	○	○	○
Avoiding clicking on links or attachments sent by unknown people. (5)	○	○	○	○	○
Checking the URL before visiting a website, to verify that it is legitimate. (7)	○	○	○	○	○

Checking the URL before visiting a website, to verify that it is using HTTPS. (17)	○	○	○	○	○
Checking that antivirus software is up-to-date. (9)	○	○	○	○	○
Only installing software from trusted sources. (10)	○	○	○	○	○
Keeping automatic software updates turned on. (11)	○	○	○	○	○
Immediately installing needed updates to the operating system and other software. (12)	○	○	○	○	○
Setting your computing devices to automatically lock when you do not use them. (13)	○	○	○	○	○
Using a password, passcode, thumbprint or other method to unlock your computing devices. (14)	○	○	○	○	○

[page break]

Q4.1 Below, we list the practices from the previous page that you indicated you are aware of. For each practice, please indicate which statement most accurately describes your behavior. For more explanation of each practice, see this link: http://bit.ly/ITpractices

[Answer set for next 13 questions:
- o Never (1)
- o Rarely (2)
- o About half the time (3)
- o Most of the time (4)
- o Always (5)]

Display This Question:
If Q3.1 = 1 [3]
Or Q3.1 = 1 [4]

Q4.2 Using online account passwords that are strong.

Display This Question:
If Q3.1 = 2 [3]
Or Q3.1 = 2 [4]

Q4.3 Using online account passwords that are unique.

Display This Question:
If Q3.1 = 3 [3]

Or Q3.1 = 3 [4]

Q4.4 Using two-factor authentication (2FA) for online accounts.

Display This Question:
If Q3.1 = 4 [3]
Or Q3.1 = 4 [4]

Q4.5 Using a password manager for online accounts.

Display This Question:
If Q3.1 = 5 [3]
Or Q3.1 = 5 [4]

Q4.6 Avoiding clicking on links or attachments sent by unknown people.

Display This Question:
If Q3.1 = 7 [3]
Or Q3.1 = 7 [4]

Q4.7 Checking the URL before visiting a website, to verify that it is legitimate.

Display This Question:
If Q3.1 = 17 [3]
Or Q3.1 = 17 [4]

Q4.8 Checking the URL before visiting a website, to verify that it is using HTTPS.

Display This Question:
If Q3.1 = 9 [3]
Or Q3.1 = 9 [4]

Q4.9 Checking that antivirus software is up-to-date.

Display This Question:
If Q3.1 = 10 [3]
Or Q3.1 = 10 [4]

Q4.10 Only installing software from trusted sources.

Display This Question:
If Q3.1 = 11 [3]
Or Q3.1 = 11 [4]

Q4.11 Keeping automatic software updates turned on.

Display This Question:
If Q3.1 = 12 [3]
Or Q3.1 = 12 [4]

Q4.12 Immediately installing needed updates to the operating system and other software.

Display This Question:
If Q3.1 = 13 [3]
Or Q3.1 = 13 [4]

Q4.13 Setting your computing devices to automatically lock when you do not use them.

Display This Question:
If Q3.1 = 14 [3]
Or Q3.1 = 14 [4]

Q4.14 Using a password, passcode, thumbprint or other method to unlock your computing devices.

[page break]
Q5.1 Below, we follow up on one or more of your answers to the preceding questions.
For more explanation of each practice, see this link: http://bit.ly/ITpractice

Display This Question:
If Q4.2 = 1

Q5.2 You say you never use online account passwords that are strong. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I don't have any online accounts that require passwords. (0)

Display This Question:
If Q4.2 = 2
Or Q4.2 = 3
Or Q4.2 = 4
Or Q4.2 = 5

Q5.3 You say you do use online account passwords that are strong. Is this only when they are required?
o Yes, I only use this practice in instances where it is required. (3)
o No, I also use this practice in instances where it is not required. (2)
o Not sure. (1)

Display This Question:
If Q5.3 = 2

Q83 Please describe this briefly:
_____

Display This Question:
If Q4.3 = 1

Q5.4 You say you never use online account passwords that are unique. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I don't have any online accounts that require passwords. (0)

Display This Question:
If Q4.4 = 1

Q5.5 You say you never use two-factor authentication (2FA) for online accounts. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I don't have any online accounts that require passwords. (0)

Display This Question:
If Q4.4 = 2
Or Q4.4 = 3
Or Q4.4 = 4
Or Q4.4 = 5

Q5.6 You say you do use two-factor authentication for online accounts. Is this only when 2FA is required?
o Yes, I only use this practice in instances where it is required. (3)
o No, I also use this practice in instances where it is not required. (2)
o Not sure. (1)

Display This Question:
If Q5.6 = 2

Q85 Please describe this briefly:
_____

Display This Question:
If Q4.5 = 1

Q5.7 You say you never use a password manager for online accounts. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I don't have any online accounts that require passwords. (0)

Display This Question:
If Q4.6 = 1

Q5.8 You say you never avoid clicking on links or attachments sent by unknown people. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I do not use any email or messaging services that allow links or attachments. (0)

Display This Question:
If Q4.7 = 1

Q5.9 You say you never check the URL before visiting a website, to verify that it is legitimate. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I do not visit websites. (0)

Display This Question:
If Q4.8 = 1

Q5.10 You say you never check the URL before visiting a website, to verify that it is using HTTPS. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I do not visit websites. (0)

Display This Question:
If Q4.9 = 1

Q5.11 You say you never check that antivirus software is up to date. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I do not have any antivirus software installed on my devices. (0)

Display This Question:
If Q4.10 = 1

Q5.12 You say you never install software only from trusted sources. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I do not ever install software. (0)

Display This Question:
If Q4.10 = 2
Or Q4.10 = 3
Or Q4.10 = 4
Or Q4.10 = 5

Q5.13 You say you do install software only from trusted sources. Is this only when this is required?
o Yes, I only use this practice in instances where it is required. (3)
o No, I also use this practice in instances where it is not required. (2)
o Not sure. (1)

Display This Question:
If Q5.13 = 2

Q84 Please describe this briefly:
_____

Display This Question:
If Q4.11 = 1

Q5.14 You say you never keep automatic software updates turned on. Did you do so in the past, but then stop?
o Yes, I used this practice in the past but then stopped. (3)
o No, I never used this practice in the past. (2)
o Not sure. (1)
o N/A - I do not use any software. (0)

Display This Question:
If Q4.12 = 1

Q5.15 You say you never immediately install needed updates to the operating system and other software. Did you do so in the past, but then stop?
- o Yes, I used this practice in the past but then stopped. (3)
- o No, I never used this practice in the past. (2)
- o Not sure. (1)
- o N/A - I do not use any software. (0)

Display This Question:
If Q4.13 = 1

Q5.16 You say you never set your computing devices to automatically lock when you do not use them. Did you do so in the past, but then stop?
- o Yes, I used this practice in the past but then stopped. (3)
- o No, I never used this practice in the past. (2)
- o Not sure. (1)
- o N/A - I do not have exclusive use of any computing devices. (0)

Display This Question:
If Q4.14 = 1

Q5.17 You say you never use a password, passcode, thumbprint or other method to unlock your computing devices. Did you do so in the past, but then stop?
- o Yes, I used this practice in the past but then stopped. (3)
- o No, I never used this practice in the past. (2)
- o Not sure. (1)
- o N/A - I do not have exclusive use of any computing devices. (0)

Display This Question:
If Q4.14 = 2
Or Q4.14 = 3
Or Q4.14 = 4
Or Q4.14 = 5

Q5.18 You say you do use a password, passcode, thumbprint or other method to unlock your computing devices. Is this only when this is required?
- o Yes, I only use this practice in instances where it is required. (3)
- o No, I also use this practice in instances where it is not required. (2)
- o Not sure. (1)

Display This Question:
If Q5.18 = 2

Q86 Please describe this briefly:

_____

[page break]
Q6.1 On the next page, we will present a series of statements about the use of security measures. Examples of security measures are laptop or tablet passwords, spam email reporting tools, software updates, secure web browsers, fingerprint ID, and anti-virus software.

For each, please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel right now, not what you have felt in the past or would like to feel.

[Randomize next 13 items, answer set is:
- o Strongly disagree (1)
- o Disagree (2)
- o Neither agree nor disagree (3)
- o Agree (4)
- o Strongly agree (5)]

Q7.1 I seek out opportunities to learn about security measures that are relevant to me.

Q7.2 I am extremely motivated to take all the steps needed to keep my online data and accounts safe.

Q7.3 Generally, I diligently follow a routine about security practices.

Q7.4 I often am interested in articles about security threats.

Q7.5 I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.

Q7.6 I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

Q7.7 I am too busy to put in the effort needed to change my security behaviors.

Q7.8 I have much bigger problems than my risk of a security breach.

Q7.9 There are good reasons why I do not take the necessary steps to keep my online data and accounts safe.

Q7.10 I usually will not use security measures if they are inconvenient.

Q7.11 I want to change my security behaviors to improve my protection against threats (e.g., phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.

Q7.12 I want to change my security behaviors in order to keep my online data and accounts safe.

Q7.13 I worry that I'm not doing enough to protect myself against threats (e.g., phishing, computer viruses, identity theft, password hacking) that are a danger to my online data and accounts.

[page break]
Q8.1 On the final two pages, we want you to tell us more about your background and experiences. Please read each question carefully and choose the response that you feel is the best match.

[page break]
Q9.1 We use this question to discard the answers of people who are not reading the questions. Please select "51% to 75% of the time" (option 4) to preserve your answers.
- o I have never done this. (1)
- o Under 25% of the time. (2)
- o 26% to 50% of the time. (3)
- o 51% to 75% of the time. (4)
- o Over 75% of the time. (5)

Q9.2 How frequently or infrequently have you personally been the victim of a breach of security (e.g., account hacking, viruses, malware or theft of your personal data)?
- o Very infrequently (1)
- o Infrequently (2)
- o Neither infrequently or frequently (3)
- o Frequently (4)
- o Very frequently (5)

Q9.3 To the best of your knowledge, how frequently or infrequently has someone close to you (e.g., spouse, family member or close friend) been the victim of a breach of security (e.g., account hacking, viruses, malware or theft of your personal data)?
- o Very infrequently (1)
- o Infrequently (2)
- o Neither infrequently or frequently (3)
- o Frequently (4)
- o Very frequently (5)

Q9.4 How much have you heard or read about during the last year about online security breaches?
- o None at all (1)
- o Only a little (2)
- o A moderate amount (3)
- o A lot (4)
- o A great deal (5)

Q9.5 What else should we know about how you think about online security?

If nothing comes to mind, please write "Nothing" to preserve your answers.

_____

[page break]

Q10.1 What is your age bracket?
- o 18-29 (1)
- o 30-39 (2)
- o 40-49 (3)
- o 50-59 (4)
- o 60 or older (5)

Q10.2 What is your gender identity?
- o Male (1)
- o Female (2)
- o Nonbinary or gender non-conforming (3)
- o Prefer to self-describe (4) _____
- o Prefer not to say (0)

Q10.3 Are you Hispanic, Latino or Spanish?
- o Yes (3)
- o No (2)
- o Prefer not to say (0)

Q10.4 What is your racial/ethnic identity?
- o White or Caucasian (1)
- o Black or African American (2)
- o Native American or Alaska Native (3)
- o Asian - East or Central Asian (4)
- o Asian - South, Southeast, or Southwest Asian (5)
- o Native Hawaiian or Pacific Islander (6)
- o Middle Eastern or North African (7)
- o Prefer to self-describe (8) _____
- o Prefer not to say (0)

Q10.5 What is your estimated yearly household income?
- o Up to $25,000 (1)
- o $25,000 to $49,999 (2)
- o $50,000 to $74,999 (3)
- o $75,000 to $99,999 (4)
- o $100,000 or more (5)

Q10.6 Including yourself, how many people are in your household currently?

Q10.7 What is the highest level of education that you have completed?
o Some high school (1)
o High school degree or equivalent (2)
o Some college, associate's degree or technical degree (3)
o Bachelor's degree (4)
o Graduate or professional degree (5)

Q10.8 How much experience have you had working with sensitive data (such as government data for which a security clearance is required, health data protected by HIPAA, or education data protected by FERPA)?
o None at all (1)
o Only a little (2)
o A moderate amount (3)
o A lot (4)
o A great deal (5)

Q10.9 Have you earned a degree in and/or worked in the fields of computer science, computer engineering, information science, or information technology?
o I both earned a degree in such a field and have worked or am currently working in one. (4)
o I earned a degree in such a field, but never worked in it. (3)
o I did not earn a degree in such a field, but I have worked or am currently working in one. (2)
o I did not earn a degree in such a field, nor did I ever work in one. (1)

Q10.10 On a scale of 0-10 (0=Cybersecurity Beginner to 10=Cybersecurity Expert), how secure do you think you are?

Cybersecurity Beginner Cybersecurity Expert

0 1 2 3 4 5 6 7 8 9 10

I rate myself as ()

A.2 Scoring Method

Sum the point values from answers to survey blocks 3, 4, and 7, using the values in parentheses.

- Q3.1 matrix: I am familiar with this practice. (4); I am aware of this practice, but not familiar with it. (3); I am not aware of this practice. (2); Not sure. (1); N/A (0)
- Q4.2-Q4.14: Never (1); Rarely (2); About half the time (3); Most of the time (4); Always (5)
- Q7.1-Q7.13: Strongly disagree (1); Disagree (2); Neither agree nor disagree (3); Agree (4); Strongly agree (5)

Appendix B: Phase 1 Detailed Research Sub-Questions and Interview Protocol

B.1 Phase 1 Detailed Research Sub-Questions

1. To what extent are participants aware of, motivated to use and/or knowledgeable about how to deal with their security and privacy concerns?
2. What are the stages of participants' security adoption decision process?
    a. To what extent are participants aware of useful and/or expert-recommended cybersecurity measures?
    b. If aware, what pros or cons do the participants weigh in deciding whether to use each of these measures?
    c. If adopted, why and for how long have they adopted the given measure?
    d. If not adopted, why not - did they never start using the given measure, or did they start using it and then stop?
3. At each stage of the adoption process, to what extent do peers, authorities, or media coverage influence people's thinking about security measures?
    a. To what extent are participants' thought processes about security adoption influenced by peers, authorities, or media coverage?
    b. To what extent do participants influence others' thought processes about security adoption?
    c. To what extent are these external influences associated with a change from one stage of the adoption process to another stage?
4. At each stage of the adoption process, to what extent do perceived characteristics of the security measures influence people's thinking about the measures?

B.1 Phase 1 Interview Protocol

[Once connected on Zoom, start script]
Hello, thank you for joining me for this interview. Do you have any questions before we begin?
[Answer any questions, then continue]
I am going to start recording now.
[Start recording]
Tell me about yourself.
[Make notes of answers that pertain to the topic]

Now, I want you to think back within the last three months, to recall an instance when you had a security or privacy concern. This might be a time that you were worried about the security of your data, or the security of an account. I'll give you a minute to think about it.
[After up to 60 seconds, if hasn't spoken] Do you have something in mind?
[if no] OK, I'd like you to think back further. Take your time.
How long ago was this?
[Q1] What caused your concern?
[Q1] How did you deal with it?
[Q1] [Q3a] Did you get advice about this from anyone?

Tell me more about that.
[Q1] [Q3a] Why did you trust this person?
    [Q3c] Did you find their advice useful? Why?
[Q1] [Q3a] Why did you trust this source?
    [Q3c] Did you find their advice useful? Why?
[Q1] [Q2a] Did this make you aware of any tools or practices that you could use to deal with this concern? What was that?
[Q1] [Q2b] Did this make you consider using any new tools or practices to safeguard your security or privacy?
[Q2d][Q4] [if no] Why do you think that is?
[Q3c] Did you get any advice about this? Did you trust it? Did you find it useful?
[Q2c] [if yes] Did you, in fact, start using any new tools or practices?
[Q2c] [if yes] Are you still using this?
[Q2c] [Q4] [if yes] Why did you keep using it?
[Q2d] [Q4] [if no] Why do you think that is?
[Q1] [Q2b] Did this make you consider stopping anything you do online or with a computing device or account?
[Q4] [if no] Why is that?
[Q3c] Did you get any advice about this?
Did you trust it?
Did you find it useful?
[if yes] What was that?
[Q2c] [Q2d] [Q4] Did you stop? Why?
[Q1] To what extent do you think that this concern is now resolved?
[Q1] [Q3b] Have you given anyone advice about this security and privacy concern?
[if yes] Tell me about how that happened.
Did they trust it, do you think?
Did they find it useful, do you think?
[Q1] Is there anything else that you think I should know about this?

Now I'm going to ask you about other specific measures of interest for our study.
[Q2a] Are you aware of _____? [pick one or more based on time and previous answers]
two-factor authentication, sometimes called two-step or multi-factor authentication?
Something called a password manager?
Methods for installing software updates?
Any type of antivirus protection?
How to create passwords that are strong, in other words, difficult to hack?
Advice not to reuse passwords on different accounts?
Any advice about how to stay alert for phishing and other scam messages in email, texts and social media?
Any advice on how to avoid sites that might contain malware?
Any advice about how to judge whether something is misinformation, sometimes known as "fake news"?
[if not aware, briefly explain what this is]
[If aware, ask whether using it themselves]

[Q2c] [Q4] If using, ask how long and why
[Q3c] Did you get any advice about this? Did you trust it? Did you find it useful?
[Q2b] If not using, ask whether have considered using:
[Q2b] [Q4] If not, why?
[Q2d] [Q4] did you once use it and then stop
Are there other benefits or drawbacks that we haven't covered?
[Q3c] Did you get any advice about this? Did you trust it? Did you find it useful?
[Q2b] If so, why?
[Q2c] [Q4] Do you think you are likely to start using this? When?
[Q3c] Did you get any advice about this? Did you trust it? Did you find it useful?
[Q1] [Q2c] Are there other measures that you use for safeguarding your security and privacy online, that we haven't talked about?
[Q2c] [for each] How long have you used this measure?
[Q2b] [for each] What made you start using this measure? How did you find out about it?
[Q3a] [follow up] Do any family members use this measure?
    [Q3d] Did they give you advice about it? Did you trust it? Did you find it useful?
[Q3a] [follow up] Do any friends use this measure?
    [Q3d] Did they give you advice about it? Did you trust it? Did you find it useful?
[Q3a] [follow up] Did you have any interactions with someone in IT about this?
    [Q3d] Did you trust it? Did you find it useful?
[Q3a] [follow up] Did you learn about this measure from any online sources, such as a news website, a video, a social media platform, or a search engine query?
    [Q3d] Did you trust their advice? Did you find it useful?
Are there any other sources you consulted?
[Q3b] [for each] Have you given anyone advice about using this measure?
[if yes] Tell me about how that happened.
Did they trust it, do you think?
Did they find it useful, do you think?
[Q1] [for each] Is there anything else that you think I should know about this?
[Q2b] Are there other measures that you are aware of but do not use?
[Q4] [for each] Why not?
[Q3c] Did you get any advice about this? Did you trust it? Did you find it useful?
[Q2d] Have you tried to use any other measures and stopped using them?
[Q4] [for each] Why?
[Q3c] Did you get any advice about this? Did you trust it? Did you find it useful?

[Wrap-up]
Is there anything else you think that I should know about these topics, but haven't yet asked?
Is there anyone else whom you think I should speak with?

Appendix C: Phase 2 Final Survey

- Original survey files at https://corifaklaris.com/files/thesis_surveys.zip
- Survey Flow:

Block: Introduction - Consent (2 Questions) **Standard: Demographics (10 Questions)**
BlockRandomizer: 1 - Evenly Present Elements
Group: A
EmbeddedData **PM_type = a built-in password manager**
Standard: Group A: Using a Built-In Password Manager (2 Questions)
Group: B
EmbeddedData **PM_type = a separately installed password manager**
Standard: Group B: Using a Separately Installed Password Manager (2 Questions) **Standard: SoSBC: Test for Non-Adoption (7 Questions)** **Standard: SoSBC: Test for Maintenance (8 Questions)** **Standard: SoSBC: Test for Threat Awareness (11 Questions)** **Standard: Security Moore-Benbasat PCI (13 Questions)** **Standard: Security Rogers 1961 Adoption Leaders + Troubleshooting + extra Trialability (16 Questions)** **Standard: Security URICA (14 Questions)** **Standard: Internet Know-How (1 Question)** **Standard: General questions (5 Questions)**

Start of Block: Introduction - Consent

Q1.1 This survey is part of a research study conducted by Cori Faklaris at Carnegie Mellon University and is funded by the U.S. National Science Foundation.

We invite you to participate in this research by filling out this survey. The purpose of this study is to identify the extent to which U.S. residents are aware of cybersecurity measures, and which factors influence them to adopt, or to not adopt, these measures.

Procedures

If you agree to participate, you will be directed to an online survey. In the first part, you will be asked to mark the extent to which you are familiar with computing

measures and your level of agreement or disagreement with a set of statements regarding computing. In the second part, you will be asked about your level of knowledge and your experiences with computing, along with several demographic questions.

The survey is estimated to take 15-18 minutes to complete. Any personally identifiable information that is captured in the course of the survey will be removed before publication.

Participant Requirements

Participation in this study is limited to U.S. residents age 18 and older.

Risks

The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during other online activities, such as fatigue at the length of the survey, or boredom or mild frustration with the questions being asked.

Benefits

There may be no personal benefit from your participation in the study, but the knowledge received may help shape better experiences for end users and for IT and security professionals who support computer systems.

Compensation & Costs

You will be compensated for taking this survey per the agreement reached with the panel provider.

There will be no cost to you if you participate in this survey.

Future Use of Information

In the future, once we have removed all identifiable information from your data, we may use the data for our future research studies, or we may distribute the data to other investigators for their research studies. We would do this without getting additional informed consent from you (or your legally authorized representative). Sharing of data with other researchers will only be done in such a manner that you will not be identified.

Confidentiality

Any information about you that is obtained as a result of this research will be kept as confidential as legally possible.

By participating in this research, you understand and agree that Carnegie Mellon may be required to disclose your consent form, data and other personally identifiable information as required by law, regulation, subpoena or court

order. Otherwise, your confidentiality will be maintained in the following manner:

Your data and consent form will be kept separate. Your consent form will be stored in a secure cloud server only accessible by the Carnegie Mellon study team and will not be disclosed to third parties. By participating, you understand and agree that the data and information gathered during this study may be used by Carnegie Mellon and published and/or disclosed by Carnegie Mellon to others outside of Carnegie Mellon. However, your name, address, contact information and other direct personal identifiers will not be mentioned in any such publication or dissemination of the research data and/or results by Carnegie Mellon. Note that per regulation all research data must be kept for a minimum of 3 years.

The researchers will take the following steps to protect participants' identities during this study: (1) Each participant will be assigned an alphanumeric identifier; (2) The researchers will record any data collected during the study by this identifier, not by name; (3) Any original recordings or data files will be stored in a secured location accessed only by authorized researchers.

Right to Ask Questions & Contact Information

If you have any questions about this study, you should feel free to ask them now or by contacting the Principal Investigator, Cori Faklaris, by mail at the Human Computer Interaction Institute, 5000 Forbes Ave., Pittsburgh, PA 15213, or by email at cfaklari@andrew.cmu.edu. If you have questions later, desire additional information, or wish to withdraw your participation, please contact the Principal Investigator by mail or e-mail in accordance with the contact information listed above.

If you have questions pertaining to your rights as a research participant; or to report concerns to this study, you should contact the Office of Research integrity and Compliance at Carnegie Mellon University. Email: irb-review@andrew.cmu.edu . Phone: 412-268-1901 or 412-268-5460.

Voluntary Participation

Your participation in this research is voluntary. You may discontinue participation at any time during the research activity. You may print a copy of this consent form for your records.

Q1.2

By selecting "Yes" in the choice box below, you affirm that you are a U.S. resident age 18 or older and that you have read, understand and agree to the above.

By selecting "No" in the choice box below, you affirm that you are not eligible and/or interested in participating in this survey, and you will not be allowed to take the survey.

- ○ Yes, I want to participate in this research and continue to the survey. (1)
- ○ No, I do not want to participate. (2)

Skip To: End of Block If Q1.2 2

End of Block: Introduction - Consent

Start of Block: Demographics

Q13.1 What is your age bracket?

- ○ Under 18 (6)
- ○ 18-29 (1)
- ○ 30-39 (2)
- ○ 40-49 (3)
- ○ 50-59 (4)
- ○ 60 or older (5)

Skip To: End of Block If Q13.1 6

Q13.2 What is your gender identity?

- ○ Male (1)

- ○ Female (2)
- ○ Non-binary or gender non-conforming (3)
- ○ Prefer to self-describe (4)

_____

- ○ Prefer not to say (0)

Q13.3 Are you Hispanic, Latino or Spanish?

- ○ Yes (3)
- ○ No (2)
- ○ Prefer not to say (0)

Q13.4 What is your racial/ethnic identity?

- ○ White or Caucasian (1)
- ○ Black or African American (2)
- ○ Native American or Alaska Native (3)
- ○ Asian - East or Central Asian (4)
- ○ Asian - South, Southeast, or Southwest Asian (5)
- ○ Native Hawaiian or Pacific Islander (6)
- ○ Middle Eastern or North African (7)
- ○ Prefer to self-describe (8)

_____

- ○ Prefer not to say (0)

Q13.5 What is your estimated yearly household income?

- ○ Up to $25,000 (1)
- ○ $25,000 to $49,999 (2)
- ○ $50,000 to $74,999 (3)
- ○ $75,000 to $99,999 (4)
- ○ $100,000 or more (5)

Q13.6 Including yourself, how many people are in your household currently?

_____

Q13.7 What is the highest level of education that you have completed?

- ○ Some high school (1)
- ○ High school degree or equivalent (2)
- ○ Some college, associate's degree or technical degree (3)
- ○ Bachelor's degree (4)
- ○ Graduate or professional degree (5)

Q13.8 How much experience have you had working with sensitive data (such as government data for which a security clearance is required, health data protected by HIPAA, or education data protected by FERPA)?

- None at all (1)
- Only a little (2)
- A moderate amount (3)
- A lot (4)
- A great deal (5)

Q13.9 Have you earned a degree in and/or worked in the fields of computer science, computer engineering, information science, or information technology?

- I both earned a degree in such a field and have worked or am currently working in one. (4)
- I earned a degree in such a field, but never worked in it. (3)
- I did not earn a degree in such a field, but I have worked or am currently working in one. (2)
- I did not earn a degree in such a field, nor did I ever work in one. (1)

Q95 Click to write the question text
Browser (1)
Version (2)
Operating System (3)
Screen Resolution (4)
Flash Version (5)
Java Support (6)
User Agent (7)

End of Block: Demographics

Start of Block: Group A: Using a Built-In Password Manager

Q3.1 For the following questions, we want you to think about **Using a Built-in Password Manager**.

What do you know about this practice?

- ○ Nothing (4)
- ○ What I know: (7) _____

Page Break

Q3.2 What you should know about **password managers:**

A password manager is a piece of software that helps you generate strong passwords, stores your login information for all websites and apps you use, and helps you log into them automatically. It encrypts your password database with a master password. The master password is the only one you have to remember.

The type of password manager that the following questions focus on is the **built-in password manager**. Examples of built-in password managers are the Apple iCloud memorized passwords list, the Google Chrome memorized passwords list, and password managers that come bundled with firewalls or antivirus software. In other words, this is the type of password manager that you **do not** have to separately install.

Click to the next page for questions about **using a built-in password manager**.

End of Block: Group A: Using a Built-In Password Manager

Start of Block: Group B: Using a Separately Installed Password Manager

Q4.1 For the following questions, we want you to think about **Using a Separately Installed Password Manager**.

What do you know about this practice?

- ○ Strongly disagree (7)
- ○ Somewhat disagree (8)
- ○ Neither agree nor disagree (9)
- ○ Somewhat agree (10)
- ○ Strongly agree (11)

Page Break

Q4.2 What you should know about **password managers:**

A password manager is a piece of software that helps you generate strong passwords, stores your login information for all websites and apps you use, and helps you log into them automatically. It encrypts your password database with a master password. The master password is the only one you have to remember.

The type of password manager that the following questions focus on is the **separately installed password manager**. Examples of separately installed password managers are LastPass, 1Password, Keeper, NordPass, and Zoho Vault. These are the type of password manager that **do not** come built-in with your device, your operating system, your browser, or other software.

Click to the next page for questions about using a **separately installed password manager**.

End of Block: Group B: Using a Separately Installed Password Manager

Start of Block: SoSBC: Test for Non-Adoption

Q5.1 Currently, are you using ${e://Field/PM_type}?

- ○ Yes (1)
- ○ No (2)

Display This Question:

If Q5.1 2

Q5.2 Have you **ever** used ${e://Field/PM_type}?

- Yes (1)
- No (2)

Display This Question:

If Q5.2 2

Q5.3 Which statement **best** fits your situation?

- I never heard of ${e://Field/PM_type} before this survey (1)
- I have heard of ${e://Field/PM_type} and am willing to use it, but so far have not put it into practice (2)
- I have heard of ${e://Field/PM_type}, but I am hesitant to use it (3)
- I have heard of ${e://Field/PM_type}, but I decided not to use it (4)
- I have heard of ${e://Field/PM_type}, but I forgot it existed until now (5)

Display This Question:

If Q5.1 2

Q5.4 Why do you not currently use it? Check all that apply.

- [ ] I don't understand how to use it (1)
- [ ] I don't understand how it works (4)
- [ ] I don't think it is important (5)
- [ ] It's inconvenient (7)
- [ ] It's difficult to use (8)
- [ ] It doesn't seem currently useful (9)
- [ ] I'm already using something that I like better (10)
- [ ] I tried it and didn't like it (11)
- [ ] I tried something else I like better (12)
- [ ] I couldn't find someone to help me with it (14)
- [ ] New computing device doesn't support it (15)
- [ ] I'm not required to use it (16)
- [ ] Someone I trust told me not to use it (17)
- [ ] I heard or saw advice not to use it (18)
- [ ] I forgot about it (19)

☐ Other reason: (20)

_____

Display This Question:

If Q5.1 2

Carry Forward Selected Choices from "Q5.4"

X→

Q5.5 Which is the **most** important reason you do not currently use it?

- ○ I don't understand how to use it (1)
- ○ I don't understand how it works (2)
- ○ I don't think it is important (3)
- ○ It's inconvenient (4)
- ○ It's difficult to use (5)
- ○ It doesn't seem currently useful (6)
- ○ I'm already using something that I like better (7)
- ○ I tried it and didn't like it (8)
- ○ I tried something else I like better (9)
- ○ I couldn't find someone to help me with it (10)
- ○ New computing device doesn't support it (11)
- ○ I'm not required to use it (12)
- ○ Someone I trust told me not to use it (13)
- ○ I heard or saw advice not to use it (14)
- ○ I forgot about it (15)

○ Other reason: (16)
_____

Display This Question:
If Q5.1 2

Q5.6 How do you currently manage your passwords? Check all that apply.

☐ Memorize them (1)

☐ Keep a paper list in my wallet (4)

☐ Keep a paper list locked up at home (5)

☐ Save a list in a file in a secured cloud account online (7)

☐ Save a secured text document on my computer (8)

☐ Save an encrypted spreadsheet on my computer (9)

☐ Write them on a note taped to my computer (12)

☐ Place them in a spot other than my computer where I or others can see them (13)

☐ Save them in plaintext in an email or text-messages draft folder (14)

☐ Pin a list inside a shared online workspace (15)

☐ Use another type of password manager (16)

☐ Other: (17) _____

Display This Question:

If Q5.1 2

Carry Forward Selected Choices from "Q5.6"

Q5.7 Which is the **most** important method you currently use to manage your passwords?

- ○ Memorize them (1)
- ○ Keep a paper list in my wallet (2)
- ○ Keep a paper list locked up at home (3)
- ○ Save a list in a file in a secured cloud account online (4)
- ○ Save a secured text document on my computer (5)
- ○ Save an encrypted spreadsheet on my computer (6)
- ○ Write them on a note taped to my computer (7)
- ○ Place them in a spot other than my computer where I or others can see them (8)
- ○ Save them in plaintext in an email or text-messages draft folder (9)
- ○ Pin a list inside a shared online workspace (10)
- ○ Use another type of password manager (11)
- ○ Other: (12) _____

End of Block: SoSBC: Test for Non-Adoption

Start of Block: SoSBC: Test for Maintenance

Display This Question:

If Q5.1 1

Q6.1 How long have you been using ${e://Field/PM_type}?

- Less than six (6) months (1)
- Six (6) months or longer (2)

Display This Question:

If Q6.1 2

Q6.2 Why do you **keep** using ${e://Field/PM_type}? Check all that apply.

- [ ] I understand how to use it (1)
- [ ] I understand how it works (2)
- [ ] Because it is important (4)
- [ ] It's convenient (6)
- [ ] It's easy to use (7)
- [ ] It seems useful (8)
- [ ] I tried it and liked it (9)
- [ ] Better than something else I used to use regularly (11)
- [ ] Was able to try it out first (12)
- [ ] Was able to set it up (13)
- [ ] Found someone to help me with it (15)
- [ ] Computing device supports it (16)
- [ ] I get notifications about it (17)
- [ ] I'm required to keep using it (18)
- [ ] Someone I trust told me to keep using it (19)
- [ ] I heard or saw advice to keep using it (20)

☐ Other: (21) _____

Display This Question:

If Q6.1 2

Carry Forward Selected Choices from "Q6.2"

Q6.3 Which is the **most** important reason you keep using it?

- ○ I understand how to use it (1)
- ○ I understand how it works (2)
- ○ Because it is important (3)
- ○ It's convenient (4)
- ○ It's easy to use (5)
- ○ It seems useful (6)
- ○ I tried it and liked it (7)
- ○ Better than something else I used to use regularly (8)
- ○ Was able to try it out first (9)
- ○ Was able to set it up (10)
- ○ Found someone to help me with it (11)
- ○ Computing device supports it (12)
- ○ I get notifications about it (13)
- ○ I'm required to keep using it (14)
- ○ Someone I trust told me to keep using it (15)

- ○ I heard or saw advice to keep using it (16)
- ○ Other: (17) _____

Display This Question:
If Q6.1 2

Q6.4 Think back to the first time you started using ${e://Field/PM_type}. How long ago was that?

- ○ Less than 1 year ago (22)
- ○ 1-2 years ago (23)
- ○ 3-5 years ago (24)
- ○ 6+ years ago (25)
- ○ I can't remember (26)

Display This Question:
If Q5.1 1

Q6.5 Why did you **start** using ${e://Field/PM_type}? Check all that apply.

- ☐ I understood how to use it (1)
- ☐ I understood how it works (2)
- ☐ Because it is important (4)
- ☐ It was convenient (6)
- ☐ It was easy to use (7)

- ☐ It seemed useful (8)
- ☐ I tried it and liked it (9)
- ☐ Was better than something else I used to use regularly (11)
- ☐ Was able to try it out first (12)
- ☐ Was able to set it up (13)
- ☐ Found someone to help me with it (15)
- ☐ Computing device supported it (16)
- ☐ I get notifications about it (17)
- ☐ I was required to start using it (18)
- ☐ Someone I trust told me to start using it (19)
- ☐ I heard or saw advice to start using it (20)
- ☐ Other: (21) _____

Display This Question:

If Q5.1 1

Carry Forward Selected Choices from "Q6.5"

Q6.6 Which was the **most** important reason you started using it?

- ○ I understood how to use it (1)
- ○ I understood how it works (2)
- ○ Because it is important (3)
- ○ It was convenient (4)
- ○ It was easy to use (5)
- ○ It seemed useful (6)
- ○ I tried it and liked it (7)
- ○ Was better than something else I used to use regularly (8)
- ○ Was able to try it out first (9)
- ○ Was able to set it up (10)
- ○ Found someone to help me with it (11)
- ○ Computing device supported it (12)
- ○ I get notifications about it (13)
- ○ I was required to start using it (14)
- ○ Someone I trust told me to start using it (15)
- ○ I heard or saw advice to start using it (16)
- ○ Other: (17) _____

Display This Question:

If Q5.1 1

Q6.7 What other methods do you currently use to manage your passwords? Check all that apply.

- ☐ Memorize them (1)
- ☐ Keep a paper list in my wallet (4)
- ☐ Keep a paper list locked up at home (5)
- ☐ Save a list in a file in a secured cloud account online (7)
- ☐ Save a secured text document on my computer (8)
- ☐ Save an encrypted spreadsheet on my computer (9)
- ☐ Write them on a note taped to my computer (12)
- ☐ Place them in a spot other than my computer where I or others can see them (13)
- ☐ Save them in plaintext in an email or text-messages draft folder (14)
- ☐ Pin a list inside a shared online workspace (15)
- ☐ Use another type of password manager (16)
- ☐ Other: (17) _____

Display This Question:

If Q5.1 1

Carry Forward Selected Choices from "Q6.7"

Q6.8 Which is the **most** important other method that you currently use to manage your passwords?

- ○ Memorize them (1)
- ○ Keep a paper list in my wallet (2)
- ○ Keep a paper list locked up at home (3)
- ○ Save a list in a file in a secured cloud account online (4)
- ○ Save a secured text document on my computer (5)
- ○ Save an encrypted spreadsheet on my computer (6)
- ○ Write them on a note taped to my computer (7)
- ○ Place them in a spot other than my computer where I or others can see them (8)
- ○ Save them in plaintext in an email or text-messages draft folder (9)
- ○ Pin a list inside a shared online workspace (10)
- ○ Use another type of password manager (11)
- ○ Other: (12) _____

End of Block: SoSBC: Test for Maintenance

Start of Block: SoSBC: Test for Threat Awareness

Q7.1 Are you aware of any risks **solely from using** ${e://Field/PM_type}?

- ○ Yes (tell us which risks): (1) _____
- ○ No (2)
- ○ I'm not sure (4)

Display This Question:

If Q7.1 = 1

Q7.2 How did you learn about such risks? Check all that apply.

- ☐ Personal experience (1)
- ☐ My own reasoning (2)
- ☐ Alerts from a web browser (5)
- ☐ Alerts from an operating system (6)
- ☐ Security awareness training (7)
- ☐ Movies (8)
- ☐ TV shows (9)
- ☐ Friends (12)
- ☐ Family members (13)
- ☐ Coworkers (14)
- ☐ Supervisors (15)
- ☐ Information Technology (IT) professional (17)
- ☐ Information Technology (IT) messages (18)
- ☐ Social media posts (20)

- [ ] Blogs (22)
- [ ] Online forums (24)
- [ ] Email newsletters (25)
- [ ] News reports (28)
- [ ] Other: (30) _____

Display This Question:

If Q7.1 1

Carry Forward Selected Choices from "Q7.2"

Q7.3 Of the ways you learned about these risks of using ${e://Field/PM_type}, which made the most impact on you?

- ○ Personal experience (1)
- ○ My own reasoning (2)
- ○ Alerts from a web browser (3)
- ○ Alerts from an operating system (4)
- ○ Security awareness training (5)
- ○ Movies (6)
- ○ TV shows (7)
- ○ Friends (8)
- ○ Family members (9)

- ○ Coworkers (10)
- ○ Supervisors (11)
- ○ Information Technology (IT) professional (12)
- ○ Information Technology (IT) messages (13)
- ○ Social media posts (14)
- ○ Blogs (15)
- ○ Online forums (16)
- ○ Email newsletters (17)
- ○ News reports (18)
- ○ Other: (19) _____

Display This Question:

If Q7.1 1

Q7.4 How concerned are you that these risks would affect the security of your online data and accounts?

- ○ Not at all (1)
- ○ Only slightly (2)
- ○ Somewhat (3)
- ○ Very (4)
- ○ Extremely (5)

Display This Question:

If Q7.1 1

Q7.5 If you suffer a breach of your online data or accounts from such risks, how much would this breach impact your life?

- ○ Not at all (1)
- ○ Only slightly (2)
- ○ Somewhat (3)
- ○ Very (4)
- ○ Extremely (5)

Page Break

Q7.6 Are you aware of any threats to your online data or accounts **that can be dealt with by using** ${e://Field/PM_type}?

- ○ Yes (tell us which threats): (1) _____
- ○ No (2)
- ○ I'm not sure (4)

Display This Question:

If Q7.6 1

Q7.7 How did you learn about such threats? Check all that apply.

- [ ] Personal experience of threats (1)
- [ ] My own reasoning (2)
- [ ] Alerts from a web browser (5)
- [ ] Alerts from an operating system (6)
- [ ] Security awareness training (7)
- [ ] Movies (8)
- [ ] TV shows (9)
- [ ] Friends (12)
- [ ] Family members (13)
- [ ] Coworkers (14)
- [ ] Supervisors (15)
- [ ] Information Technology (IT) professional (17)
- [ ] Information Technology (IT) messages (18)
- [ ] Social media posts (20)
- [ ] Blogs (22)
- [ ] Online forums (24)

- [ ] Email newsletters (25)
- [ ] News reports (28)
- [ ] Other: (30) _____

Display This Question:

If Q7.6 1

Carry Forward Selected Choices from "Q7.7"

Q7.8 Of the ways you learned about threats that can be dealt with by using ${e://Field/PM_type}, which made the most impact on you?

- ○ Personal experience of threats (1)
- ○ My own reasoning (2)
- ○ Alerts from a web browser (3)
- ○ Alerts from an operating system (4)
- ○ Security awareness training (5)
- ○ Movies (6)
- ○ TV shows (7)
- ○ Friends (8)
- ○ Family members (9)
- ○ Coworkers (10)
- ○ Supervisors (11)
- ○ Information Technology (IT) professional (12)

- ○ Information Technology (IT) messages (13)
- ○ Social media posts (14)
- ○ Blogs (15)
- ○ Online forums (16)
- ○ Email newsletters (17)
- ○ News reports (18)
- ○ Other: (19) _____

Display This Question:
If Q7.6 1

Q7.9 How concerned are you that such threats will affect the security of your online data and accounts?

- ○ Not at all (1)
- ○ Only slightly (2)
- ○ Somewhat (3)
- ○ Very (4)
- ○ Extremely (5)

Display This Question:
If Q7.6 1

Q7.10 If you suffer a breach of your online data or accounts from such threats, how much will this breach impact your life?

- ○ Not at all (1)

- ○ Only slightly (2)
- ○ Somewhat (3)
- ○ Very (4)
- ○ Extremely (5)

Q7.11 What, if anything, do you think we should know about this topic that we haven't asked? If nothing applies, please type "Nothing" to preserve your answers.

_____

_____

_____

_____

_____

Skip To: End of Block If Condition: What, if anything, do you t... Is Empty. Skip To: End of Block.

End of Block: SoSBC: Test for Threat Awareness

Start of Block: Security Moore-Benbasat PCI

Q8.1 Please indicate the degree to which you agree or disagree with each statement about ${e://Field/PM_type}. In each case, make your choice in terms of how you feel **right now**, not what you have felt in the past or would like to feel. There are no wrong answers.

Q8.2 My boss does not require me to use ${e://Field/PM_type}.

- ○ Strongly disagree (1)
- ○ Somewhat disagree (2)

- ○ Neither disagree nor agree (3)
- ○ Somewhat agree (4)
- ○ Strongly agree (5)

Q8.3 Although it might be helpful, using ${e://Field/PM_type} is certainly not compulsory for **any** of my work activities.

- ○ Strongly disagree (1)
- ○ Somewhat disagree (2)
- ○ Neither disagree nor agree (3)
- ○ Somewhat agree (4)
- ○ Strongly agree (5)

Q8.4 I believe that using ${e://Field/PM_type} is cumbersome.

- ○ Strongly disagree (1)
- ○ Somewhat disagree (2)
- ○ Neither disagree nor agree (3)
- ○ Somewhat agree (4)
- ○ Strongly agree (5)

Q8.5 Learning to use ${e://Field/PM_type} is easy for me.

- ○ Strongly disagree (1)

- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.6 Using ${e://Field/PM_type} requires a lot of mental effort from me.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.7 Using ${e://Field/PM_type} is often frustrating.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.8 At my job, one sees many people using ${e://Field/PM_type}.

- Strongly disagree (1)

- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.9 It is easy for me to observe others using ${e://Field/PM_type} to protect their online data and accounts.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.10 I've had a great deal of opportunity to try various ways of using ${e://Field/PM_type}.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.11 There are enough people around me to help me try out the various ways of using ${e://Field/PM_type}.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.12 People in my profession who use ${e://Field/PM_type} have more prestige than those who do not.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q8.13 People at my job who use ${e://Field/PM_type} have a higher status than those who do not.

- Strongly disagree (1)
- Somewhat disagree (2)
- Neither disagree nor agree (3)
- Somewhat agree (4)
- Strongly agree (5)

Q12.1

We use this question to make sure that survey participants are paying attention. Please mark "51% to 75% of the time" to preserve your answers.

- ○ I have never falsified information. (1)
- ○ Under 25% of the time. (2)
- ○ 26% to 50% of the time. (3)
- ○ 51% to 75% of the time. (4)
- ○ Over 75% of the time. (5)

Skip To: End of Block If Q12.1 ! 4

End of Block: Security Moore-Benbasat PCI

Start of Block: Security Rogers 1961 Adoption Leaders + Troubleshooting + extra Trialability

Q9.1 Below is a series of statements about the use of security practices. Examples of security practices include using a password manager, using spam email reporting tools, installing software updates, using secure web browsers, activating biometric ID, and updating anti-virus software.

For each, please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel **right now**, not what you have felt in the past or would like to feel.

There are no wrong answers.

Q9.2 In the past six months, I have told at least one other person about a security practice.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.3 I am much more likely than anyone I know to be asked for advice about a security practice.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.4 Thinking back to my last discussion about a security practice, I spent much more time listening to someone else than trying to convince them of my ideas.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.5 Thinking back to my last discussion about a security practice, I spent much more time asking someone else for their opinion than giving an opinion of my own.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.6 I am much more likely to tell another person about a security practice than for someone else to tell me about one.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.7 Generally, I am regarded as a good source of advice about security practices.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.8 I help people around me to employ security practices, if I think they'll benefit from the knowledge I have.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.9 I advise other people about security practices that I have started using for myself.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.10 I reach out to experts I know personally for help with security practices.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.11 I look on the internet for help with security practices.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.12 I trust experts on the internet to help me with security practices.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.13 I contact customer support when I need help with a security product that I am trying to use.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.14 I try using free versions of security software before switching to paid versions.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.15 I usually try out security practices a little at a time before I commit to using them regularly.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q9.16 I like to try different types of security solutions for my needs, before choosing a particular solution.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

End of Block: Security Rogers 1961 Adoption Leaders + Troubleshooting + extra Trialability

Start of Block: Security URICA

Q10.1 Below is a series of statements about the use of security practices. Examples of security practices include using a password manager, using spam email reporting tools, installing software updates, using secure web browsers, activating biometric ID, and updating anti-virus software.

For each, please indicate the degree to which you agree or disagree with each statement. In each case, make your choice in terms of how you feel **right now**, not what you have felt in the past or would like to feel.

There are no wrong answers.

Q10.2 Trying to improve my use of security practices (such as using a password manager, creating unique passwords and installing software updates) is a waste of time for me because I'm not likely to be the target of cyber attackers.

- Strongly disagree (6)
- Somewhat disagree (7)
- Neither agree nor disagree (8)
- Somewhat agree (9)
- Strongly agree (10)

Q10.3 I'm not as vulnerable as others to security threats (such as phishing, computer viruses, identity theft, and account hacking), so it doesn't make sense to me to do more to protect myself.

- Strongly disagree (6)
- Somewhat disagree (7)
- Neither agree nor disagree (8)
- Somewhat agree (9)
- Strongly agree (10)

Q10.4 I would rather cope with the results of my lax security practices (such as reusing passwords or putting off software updates) than try to change these practices.

- Strongly disagree (6)

- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.5 I wish I knew more about how I can protect my online data and accounts against security threats (such as phishing, computer viruses, identity theft, account hacking)

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.6 I hope that someone will have some good advice for me about how I can better protect my online data and accounts against security threats (such as phishing, computer viruses, identity theft, account hacking).

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.7 I'm hoping that I will be able to better understand how to protect myself against security threats (such as phishing, computer viruses, malware, account hacking) that are a danger to my online data and accounts.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.8 I am vulnerable to security threats (such as phishing, computer viruses, identity theft, and account hacking), and I really think I should better protect my online data and accounts against them.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.9 I have started using security practices (such as using a password manager, creating unique passwords and installing software updates), but I would like help in better protecting my online data and accounts.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.10 Anyone can talk about keeping their online data and accounts safer; I'm actually doing something about it.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.11 I am doing something to protect myself against security threats (such as phishing, computer viruses, identity theft, and account hacking) that are a danger to my online data and accounts.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)

- ○ Strongly agree (10)

Q10.12 I have been using security practices (such as using a password manager, creating unique passwords and installing software updates) for a long time.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.13 Once I started using security practices (such as using a password manager, creating unique passwords and installing software updates), I never stopped.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)
- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

Q10.14 I have been successful in changing how I use security practices (such as using a password manager, creating unique passwords and installing software updates) to better protect my online data and accounts.

- ○ Strongly disagree (6)
- ○ Somewhat disagree (7)

- ○ Neither agree nor disagree (8)
- ○ Somewhat agree (9)
- ○ Strongly agree (10)

End of Block: Security URICA

Start of Block: Internet Know-How

Q11.1
How would you rate your familiarity with the following concepts or tools?

	I've never heard of this. (1)	I've heard of this, but I don't know what it is. (2)	I know what this is, but I don't know how it works. (3)	I know generally how this works. (4)	I know very well how this works. (5)
IP address (1)	○	○	○	○	○
Cookie (2)	○	○	○	○	○
Incognito mode / private browsing mode in browsers (3)	○	○	○	○	○
Encryption (4)	○	○	○	○	○
Proxy server (5)	○	○	○	○	○
Secure Sockets Layer (SSL) (6)	○	○	○	○	○

Tor (7)	○	○	○	○	○
Virtual Private Network (VPN) (8)	○	○	○	○	○
Privacy settings (9)	○	○	○	○	○

End of Block: Internet Know-How

Start of Block: General questions

Q12.2 How frequently or infrequently have you personally been the victim of a breach of security (e.g., account hacking, viruses, malware or theft of your personal data)?

- ○ Very infrequently (1)
- ○ Infrequently (2)
- ○ Neither infrequently or frequently (3)
- ○ Frequently (4)
- ○ Very frequently (5)

Q12.3 To the best of your knowledge, how frequently or infrequently has someone close to you (e.g., spouse, family member or close friend) been the victim of a breach of security (e.g., account hacking, viruses, malware or theft of your personal data)?

- ○ Very infrequently (1)
- ○ Infrequently (2)
- ○ Neither infrequently or frequently (3)

- ○ Frequently (4)
- ○ Very frequently (5)

Q12.4 How much have you heard or read about during the last year about online security breaches?

- ○ None at all (1)
- ○ A little (2)
- ○ A moderate amount (3)
- ○ A lot (4)
- ○ A great deal (5)

Q12.5 What other factors or strategies influence your online security behaviors? If none come to mind, please write "None."
(In your answer, please do not reveal any private or personally-identifiable information about yourself OR others.)

_____

_____

_____

_____

_____

End of Block: General questions

Appendix D: Phase 1 Interview Codebook

Code	Description(s)	Source	Associated Step
Security practice	The first mention of any method of either dealing with ("treating" or addressing) or preventing a security concern, whether cyber/virtual or physical	[222]; authors	Securing Learning (Step 2)
/Mandatory	Required, compulsory. The lack of control a participant perceives or actually experiences over adopting a security practice.	Adapted from [238]	(Cross-cutting)
/Voluntary	Not required, not compulsory. The degree of control a participant perceives or actually experiences over adopting a security practice.	Adapted from [238]	(Cross-cutting)
/Cognition-based	Any mention of facts, information, or skills for either dealing with ("treating" or addressing) or preventing a security concern, whether cyber/virtual or physical	Adapted from [238]	(Cross-cutting)
/Tool-based	Any mention of a device or software program for either dealing with ("treating" or addressing) or preventing a security concern, whether cyber/virtual or physical	Adapted from [238]	(Cross-cutting)
Communication channel	"Means by which a message gets from a source to a receiver" whether or not security-related (specific or nonspecific)	[168]	(Cross-cutting)
CS/IS experience	Skills, education, career, or ability for computing and information behaviors	[164]; authors	(Cross-cutting)
Social influence	Any instance of interpersonal, media, and/or authority guidance of someone's thoughts, feelings and/or behavior through advice, through example, or through removing choices (including influences on the participants and their influence on others)	[28,168]; authors	(Cross-cutting)
/Media	Any reference to means of mass communication (broadcasting, publishing, and the internet)	Adapted from [238]	(Cross-cutting)
/Peers	one who is of approximate equal standing with another in a sphere of influence	Adapted from [238]	(Cross-cutting)
/Authorities	a person or organization having power in a particular sphere, such as the workplace or a family	Adapted from [238]	(Cross-cutting)
Practice characteristics	Perceived characteristics of the security practice (or other technology) in context (including but not limited to compatibility, relative advantage, trialability, observability, re-invention [adapting a security practice for individual situation])	[168]	(Cross-cutting)
Security attitude	Engagement (desire to learn more), attentiveness, resistance, hesitance, or other disposition toward cybersecurity and security practices, of a negative, positive or neutral valence - also "inevitability" re perceived behavioral control	[34,70,164]	(Cross-cutting)
/Resistance of others	Any resistant attitude attributed to a person other than the interviewee	authors	(Cross-cutting)
/Resistance	attitudes that do not fall under one of the subcodes that describe some resistance or negative valence toward security practice learning, trialing, adoption, or maintenance	authors	(Cross-cutting)

/Inconvenience	participant indicates that security practices are inconvenient, or incompatible with their routine/technology in some way	[34,70]	(Cross-cutting)
/Bigger problems	participant indicates that security is not a priority, that security risks are relatively small, or that other problems are relatively large in comparison to security risks	[34,70]	(Cross-cutting)
/Too busy	participant indicates that they are too busy or do not have enough time or energy to care about, learn about, trial, or adopt a security practice	[34,70]	(Cross-cutting)
Goals	Explicitly stated aspiration or want, object of effort, or aim/desired result of an action, often indicated by "want". Can be specific to a situation or nonspecific to participants' overall aims	authors	(Cross-cutting)
Security concern	"This might be a time that you were worried about the security of your data, or the security of an account. " Mention of any threat, risk, harm, or potential harm related to security	[226,227,236]; authors	Threat Awareness (Step 1)
/Feeling a threat	Stated evaluation of the degree to which an event has significant implications for their security, involving both severity and vulnerability, while unaware of coping mechanisms	[133,153]; authors	Threat Awareness (Step 1)
/Continuing to feel a threat	Stated evaluation of the degree to which an event has significant implications has significant implications for their security, involving both severity and vulnerability, but while aware of coping mechanisms and/or having adopted them to some degree	[133,153]; authors	(Cross-cutting)
/Not feeling a threat	Stated evaluation of the degree to which their security is not likely to be impacted by an event, involving both severity and vulnerability, while aware of coping mechanisms	[133,153]; authors	Security Learning (Step 2)
Unawareness	No knowledge of the existence of a given security practice or other technology.	[69]	Threat Awareness (Step 1)
Awareness	Knowledge of existence of a given security practice or other technology, but no enactment of that practice	[69]	Securing Learning (Step 2)
/Learning about practice	the acquisition of knowledge or skills about a security practice through experience, study, or by being taught	Adapted from [238]	Securing Learning (Step 2)
/Hesitating to adopt	state of uncertainty, tentativeness, or slowness to act on knowledge of practice; evidence of cognitive balance toward cons; similar to vaccine hesitancy where people have not yet decided to resist or to reject.	authors	Securing Learning (Step 2)
/Willing to adopt	state of certainty, preparation, resolve, or eagerness to act on knowledge of practice; evidence of cognitive balance toward pros	authors	Securing Learning (Step 2)
/Deciding to try adoption	evidence of specific intention to test a security practice that one is made aware of; explicit mention of "try" or "trial" or "promo"	authors	Securing Learning (Step 2)
Adoption	Either active or passive enactment of security practice or other technology, including trialing, beginning use, and maintaining use	[69]	(Cross-cutting)
/Trialing adoption	Acting to test the security practice to evaluate its usefulness in everyday life	[168]; authors	Security Practice Implementation (Step 3)

/Implementing adoption	Acting to put the decision to adopt a security practice into effect in everyday life	[158,168]; authors	Security Practice Implementation (Step 3)
/Maintaining adoption	Acting to finalize the decision to continue using the practice and/or to use it to its fullest potential; "still" or "currently" - present time will come up in the text	[158,168]; authors	Security Practice Maintenance (Step 4)
/Educating others	Acting to share one's security learnings and/or to instruct others in the use of a security practice	authors	Security Practice Maintenance (Step 4)
Non-adoption	Decision not to use a security practice or other technology, including termination of adoption context, rejection, and stopping usage	[69]	(Cross-cutting)
/Discontinuing adoption	Stopping use of a practice once it has already been used at least once; explicit mention	[158,168]; authors	Security Practice Implementation (Step 3)
/Rejecting adoption	Deciding against use of a practice before it has been used once; explicit mention	[158,168]; authors	Security Learning (Step 2)
Time	Any recognition of something occurring other than in the current moment, either past or future	[88,168]	Security Practice Maintenance (Step 4)
CS/IS technology	First mention of any instrumental infrastructure for computing and information behaviors, including security tools and computing devices	Adapted from [238]	(Cross-cutting)

Appendix E: Phase 2 Collected Scales

Scale	Cronbach's Alpha (.700 is acceptable)
URICA Precontemplation	.730
URICA Contemplation/Preparation	.732
URICA Action/Maintenance	.846
Moore-Benbasat Image	.768
Moore-Benbasat Visibility/Trialability	.737
Moore-Benbasat Voluntariness*	.543
Moore-Benbasat Ease of Use*	.293
Rogers Adoption Leader	.835
Rogers Adoption Follower*	.619
Educating Others	.743
Proactivity in Seeking Help*	.642
Trial Preference*	.636
Internet Know-How	.905

* These were not included in the analysis due to the low alpha score

Appendix F: Phase 2 Survey Codebook

F.1. New Measures

Construct	Code	Variable(s)	Type	Values	Stage	Reference
Group assignment	PM_type	"a built-in password manager" or "a separately installed password manager"	Piped text			Pearman et al. 2019
	Q3.1	Group A assignment - Using a Built-in Password Manager				
	Q3.1_TEXT	Knowledge check	Text input	manual check - "Nothing," other	other=Awareness of Security Practice	
	Q3.2	Show definition and examples for PM_type	Text/Graphic			Zou et al. 2020, internet search
	Q4.1	Group B assignment - Using a Separately Installed Password Manager				
	Q4.1_TEXT	Knowledge check	Text input	manual check - "Nothing," other	other=Awareness of Security Practice	
	Q4.2	Show definition and examples for PM_type	Text/Graphic			Zou et al. 2020, internet search
Adoption	Q5.1	Test for Current Use	Binary	Yes = 1, No = 2	1=Adoption	ADOPT flips the numbers = 1 and 0
Non-Adoption	Q5.2	Test for Non-Adoption	Binary	Yes = 1, No = 2	1=Discontinuance	
	Q5.3	Test for type of Non-Adoption	Categorical	[1,5]	1=Ignorance 2=Willingness 3=Hesitance 4=Rejection 5=Nonengagement	
Reasons for Non-Adoption	Q5.4	Non-Adoption reason - Lack of understanding, Resistance,	Categorical	[1,20]	14, 16, 17, 18 = social influences 7, 8, 11, 12, 15 =	Interview data, prior work

Construct	Code	Variable(s)	Type	Values	Stage	Reference
		Unusability, Lack of Trialability, Lack of Relative Advantage, Lack of Troubleshooting, Lack of social support, Lack of affordance, other			practice characteristics	
Other methods used	Q5.5	Most important reason	Categorical			Interview data, prior work
	Q5.6	Lack of Relative Advantage - alternate password management method	Categorical	[1,17]		
	Q5.7	Most important alternate method	Categorical			
New or Maintained Adoption	Q6.1	Test for Maintenance	Binary	1= <6 months, 2= >=6 months	1=Implementation 2=Maintenance	TTM and DOI benchmark
Reason for Maintaining Adoption	Q6.2	Maintenance reason - Understanding, Lack of Resistance, Usability, Trialability, Relative Advantage, Troubleshooting, Social support, Voluntariness, Affordance, other	Categorical	[1,21]		Interview data, prior work
	Q6.3	Most important reason	Categorical			
Duration of Adoption	Q6.4	Innovation Adopter time scale - Add in the Implementation data as the lowest data point; standardize the distribution and look at percentiles: 16%, 34%, 34%, 13.5%, and 2.5%	Categorical	[0,10]=>z[0,1]	2.5%=Innovator 13.5%=Early adopter 34%=Early majority 34%=Late majority 16%=Laggard	Rogers 1961 (DOI)

Construct	Code	Variable(s)	Type	Values	Stage	Reference
Reason for Initial Adoption	Q6.5	Initial Adoption reason - Understanding, Lack of Resistance, Usability, Trialability, Relative Advantage, Troubleshooting, Social support, Voluntariness, Affordance, other	Categorical	[1,21]		Interview data, prior work
	Q6.6	Most important reason	Categorical			
Other methods used	Q6.7	Relative Advantage - alternate password management method	Categorical	[1,17]		Interview data, prior work
	Q6.8	Most important alternate method	Categorical			
Awareness of Risks of Using Password Managers	Q7.1	Test for PM Risk Awareness	Binary	Yes = 1, No = 2 or I'm not sure=4	1=Risk Awareness	
	Q7.2	Knowledge check	Text input	manual check		
	Q7.3	Learning about risks - Sources	Categorical	[1,30]	8, 9, 12, 13, 14, 15, 17, 18, 20, 22, 24, 25, 28 = social influences	Interview data, prior work
	Q7.4	Most impactful source	Categorical			
	Q7.5	Perceived vulnerability to risks	Interval	[1,5]	1=None to 5=High	Rogers 1983 (PMT)
Awareness of Threats that Password Managers Guard Against	Q7.6	Test for Threat Awareness	Binary	Yes = 1, No = 2 or I'm not sure=4	1=Threat Awareness	
	Q7.7	Knowledge check	Text input	manual check		
	Q7.8	Learning about threats - Sources	Categorical	[1,30]	8, 9, 12, 13, 14, 15, 17, 18, 20, 22, 24, 25, 28 = social influences	Interview data, prior work

Construct	Code	Variable(s)	Type	Values	Stage	Reference
	Q7.9	Most impactful source	Categorical			
	Q7.10	Perceived vulnerability to threats	Interval	[1,5]	1=None to 5=High	Rogers 1983 (PMT)
	Q7.11	Perceived severity of threats	Interval	[1,5]	1=None to 5=High	Rogers 1983 (PMT)
	Q7.12	Check for anything else we should know	Text input	manual check		
Calculated variables	SPA1	1 = ((Q7.6=1) OR (Q7.6=4)) AND ((Q5.3=1) OR (Q5.3=5)), else 0	Binary	1 or 0	1=Threat Awareness not Learning	cat 1
	SPA2	1 = ((Q7.6=1) OR (Q7.6=4)) AND ((Q5.3=2) OR (Q5.3=3)), else 0	Binary	1 or 0	1=Learning and Threat Awareness	cat 3
	SPA3	1 = (Q5.1=1) AND ((Q6.1=1) OR (Q6.4=22)), else 0	Binary	1 or 0	1=Practice Implementation	cat 5
	SPA4	1 = (Q5.1=1) AND (Q6.4>=23), else 0	Binary	1 or 0	1=Practice Maintenance	cat 7
	OBS1	1= (Q7.6=2) AND ((Q5.3=1) OR (Q5.3=5)), else 0	Binary	1 or 0	1=No Learning or Threat Awareness	cat 0
	OBS2	1 = (Q7.6=2) AND ((Q5.3=2) OR (Q5.3=3)), else 0	Binary	1 or 0	1=Learning not Threat Awareness	cat 2
	OBS3	1 = (Q5.1=2) AND (Q5.3=4), else 0	Binary	1 or 0	1=Practice Rejection	cat 4
	OBS4	1 = (Q5.1=2) AND (Q5.2=1), else 0	Binary	1 or 0	1=Practice Discontinuance	cat 6
	SPA_cat	Level of Security Practice Adoption	Ordinal	[0,7]	0=No Learning or Threat Awareness 1=Threat Awareness not Learning 2=Learning not Threat Awareness 3=Learning and Threat Awareness 4=Practice Rejection 5=Practice	should this also weight any of the why answers?

Construct	Code	Variable(s)	Type	Values	Stage	Reference
					Implementation 6=Practice Discontinuance 7=Practice Maintenance	
	MAND	1=(Q6.2_18 + Q6.5_18 + (Q8.2>=4) + (Q8.3>=4))	Binary	[0,1]	0=Not checked, 1=Required	
	TRUST	1= (Q6.2_19 + Q6.5_19), 0=SYSMIS	Binary	[0,1]	0=Not checked, 1=Someone I trust told me to use it	
	ADVICE	1=(Q6.2_20 + Q6.5_20), 0=SYSMIS	Binary	[0,1]	0=Not checked, 1=I heard or saw advice to use it	
	TRIAL	1=(Q6.2_7 + Q6.5_7 + Q6.2_9 + Q6.5_9), 0=SYSMIS	Binary	[0,1]	0=Not checked, 1=Tried it first	
	HELP	1=(Q6.2_11 + Q6.5_11), 0=SYSMIS	Binary	[0,1]	0=Not checked, 1=Got help with it	
	SPA	Level of Security Practice Adoption - collapses two levels into Learning and two into Rejection	Ordinal	[0,5]	0=No Learning or Threat Awareness 1=Threat Awareness not Learning 2=(Learning not Threat Awareness) OR (Learning and Threat Awareness) 3=Practice Implementation 4=Practice Maintenance 5=(Practice Rejection) OR (Practice Discontinuance)	"Step X" for Step 5 should this also weight any of the why answers?
	PM_RISK	Test for PM Risk Awareness	Binary	Yes = 1, No or I'm not sure=0	1=Risk Awareness	
	PM_PROTECT	Test for Threat Awareness	Binary	Yes = 1, No or I'm not sure=1	1=Threat Awareness	
	SOC_EXP	Averages the two items about breach experiences that are social				

F.2. Existing Measures

Construct	Code	Calculated variable	Calculation formula for SPSS	Type	Notes
TTM stage identifier	U_PR	URICA Precontemplation	MEAN(Q10.2, Q10.3, Q10.4)	Interval	URICA = U_AM + U_CP - U_PR
TTM stage identifier	U_CP	URICA Contemplation/Preparation	MEAN(Q10.5, Q10.6, Q10.7, <Q10.8>)	Interval	Performs much better without Q10.8
TTM stage identifier	U_AM	URICA Action/Maintenance	MEAN(<Q10.9>, Q10.10, Q10.11)	Interval	Not as reliable
TTM stage identifier	U_AM	_NEW Action/Maintenance	MEAN(Q10.10, Q10.11, Q10.12, Q10.13, Q10.14)	Interval	
TTM stage identifier	U_ALL11	_NEW composite TTM measure	MEAN(6-Q10.2, 6-Q10.3, 6-Q10.4, Q10.5, Q10.6, Q10.7, Q10.10, Q10.11, Q10.12, Q10.13, Q10.14)	Interval	calculate like SA-13 - reverse the PR items
My stage identifier	U_LTM	_NEW LT Maintenance	MEAN(Q10.13, Q10.14)	Interval	does not seem to meaningfully distinguish between Implementation and Maintenance
DOI social influence	AD_LEAD	Rogers Adoption Leader	MEAN(Q9.2, Q9.3, Q9.4, Q9.5, Q9.6, Q9.7)	Interval	two factors
DOI social influence	AD_LEAD	Rogers Adoption Leader	MEAN(Q9.2, Q9.3, Q9.6, Q9.7)	Interval	
DOI social influence	AD_FOLLOW	Rogers Adoption Follower	MEAN(Q9.4, Q9.5)	Interval	not reliable
My social influence	AD_EDUO	_NEW Educating Others	MEAN(Q9.8, Q9.9)	Interval	
Attitude	AD_PROA	_NEW Proactivity	MEAN(<Q9.4, Q9.5>, Q9.10, Q9.11, Q9.12, Q9.13)	Interval	Alpha = .698; unclear that they really should be smushed together.
Attitude	AD_TRY	_NEW Trial preference	MEAN(<Q9.14>, Q9.15, Q16)	Interval	Not reliable
DOI characteristics	MB_VOL	M-B Voluntariness	MEAN(Q8.2, Q8.3)	Interval	Not reliable
DOI characteristics	MB_EAS	M-B Ease of Use	MEAN(6-Q8.4, <Q8.5>, 6-Q8.6, 6-Q8.7)	Interval	Q8.5 speaks more to learnability
DOI characteristics	MB_VIS	M-B Visibility	MEAN(Q8.8, Q8.9)	Interval	Not reliable
DOI characteristics	MB_TRI	M-B Trialability	MEAN(Q8.10, Q8.11)	Interval	Not reliable
DOI characteristics	MB_IMG	M-B Image	MEAN(Q8.12, Q8.13)	Interval	items do not load cleanly in the

					total factor analysis
(DOI marged)	MB_VT	Visibility/Trialability	MEAN(Q8.8, Q8.9, Q8.10, Q8.11)	Interval	
Knowledge	IKH	Internet Know-How	MEAN(Q11.1_1, Q11.1_2, Q11.1_3, Q11.1_4, Q11.1_5, Q11.1_6, Q11.1_7, Q11.1_8, Q11.1_9)	Interval	
Threat exposure	BREACH_P	Frequency of personally suffering a security breach in the past year	Q13.2	Ordinal/Interval	
Threat exposure	BREACH_C	Frequency of a close tie suffering a security breach in the past year	Q13.3	Ordinal/Interval	
Threat exposure	BREACH_N	Frequency of hearing or reading about a security breach in the past year	Q13.4	Ordinal/Interval	
Demographics	AGE	Age bracket	Q14.1	Categorical	
Demographics	GEN	Gender identity	Q14.2	Categorical	
Demographics	HLS	Hispanic/Latinx/Spanish	Q14.3	Categorical	
Demographics	RETH	Race/ethnic identity	Q14.4	Categorical	
Demographics	INC	Yearly household income	Q14.5	Ordinal/Interval	
Demographics	HOU	Size of household	Q14.6	Numeric	
Demographics	EDU	Level of educational attainment	Q14.7	Ordinal/Interval	
Demographics	SEN	Experience working with sensitive data	Q14.8	Ordinal/Interval	
Demographics	EXP	Experience in IS/CS fields	Q14.9	Categorical	

VITA

Cori N. Faklaris
cori@corifaklaris.com
(317) 289-6460
6005 5th Ave., Apt 10A, Pittsburgh, PA 15232
CoriFaklaris.com, Linked In, Facebook, Twitter & elsewhere

Education

2022 Ph.D. Human-Computer Interaction, Human-Computer Interaction Institute, School
2021 M.S. of Computer Science, Carnegie Mellon University.
Thesis: "Toward a Socio-Cognitive Stage Model of Cybersecurity Behavior Adoption."
Advisors: Laura Dabbish and Jason I. Hong.
2017 M.S. Human-Computer Interaction, Department of Human-Centered Computing,
Indiana University School of Informatics and Computing at IUPUI.
1996 B.S. Journalism (News-editorial), University of Illinois at Urbana-Champaign.

Research Interests

- Usable security and privacy.
- Social computing.
- Interaction design.
- Mixed methods.
- Psychometrics.

Selected Work Experiences

- Graduate Research Assistant, Carnegie Mellon HCII, August 2017-July 2022.
- Graduate Research Assistant, IU School of Informatics and Computing, January 2015-2017.
- UX Researcher, Meta, June 2020-August 2020.
- Social Media Consultant and Editor/Writer, January 2015 – August 2017.
- Engagement Producer/Local Network Editor, IndyStar.com, 2013 – 2015.
- Page Designer and CCI Superuser, IndyStar Media Group/Gannett, previous to 2013.

Links to Other Materials

- Research statement: https://corifaklaris.com/files/research.pdf
  - Google Scholar: https://scholar.google.com/citations?user=QyK75JQAAAAJ&hl=en.
- Teaching statement: https://corifaklaris.com/files/teaching.pdf
  - Sample lecture: https://www.slideshare.net/CoriFaklaris/designing-for-usable-security-and-privacy
- Diversity statement: https://corifaklaris.com/files/dei.pdf