A Framework for Reasoning about Social Influences on Security and Privacy Adoption

Cori Faklaris
University of North Carolina at Charlotte
cfaklari@charlotte.edu

Laura Dabbish
Carnegie Mellon University
dabbish@cmu.edu

Jason I. Hong
Carnegie Mellon University
jasonh@cs.cmu.edu

ABSTRACT

Much research has found that social influences (such as social proof, storytelling, and advice-seeking) help boost security awareness. But we have lacked a systematic approach to tracing how awareness leads to action, and to identifying which social influences can be leveraged at each step. Toward this goal, we develop a framework that synthesizes our design ideation, expertise, prior work, and new interview data into a six-step adoption process. This work contributes a prototype framework that accounts for social influences by step. It adds to what is known in the literature and the SIGCHI community about the social-psychological drivers of security adoption. Future work should establish whether this process is the same regardless of culture, demographic variation, or work vs. home context, and whether it is a reliable theoretical basis and method for designing experiments and focusing efforts where they are likely to be most productive.

CCS CONCEPTS

• **Security and privacy**; • **Human and societal aspects of security and privacy; Usability in security and privacy**; • **Human-centered computing**; • **Human computer interaction (HCI); HCI design and evaluation methods, User studies; HCI theory, concepts and models; Empirical studies in collaborative and social computing**;

KEYWORDS

social influences, attitudes, usable security, social cybersecurity, stage models

ACM Reference Format:
Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2024. A Framework for Reasoning about Social Influences on Security and Privacy Adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3613905.3651012

1 INTRODUCTION

We now have many findings of the importance of social influences, mental models, and usability in designing for cybersecurity with humans-in-the-loop [9, 10, 58, 61]. However, it is not easy to decide which studies to rely on, or the extent to which findings on awareness will also apply to adoption, or how best to direct scarce resources. Even experts and longtime practitioners might become so frustrated that they fall back to more-restrictive security designs that do not allow for human differences, nuances, or special cases. For example, years of low voluntary adoption of two-factor authentication [69] led Google to auto-enroll 150 million accounts and to require 2 million YouTube creators to turn it on [6, 68]. We see a need for a framework that helps us to reason about which influences are likely to be effective in moving users step-by-step to the goal of regular use of security practices.

Toward this goal, we have developed a prototype framework that gives structure to prior work on social influences in security awareness and adoption. We started by asking: (1) How does security behavior evolve over time? And (2): How do social influences affect the process? We brainstormed ideas, discussed and kept informal notes on our thoughts drawn from our expertise in usable security, social computing, and design-oriented research [22], and we researched theories of behavior change that could apply to end-user cybersecurity [2, 15, 26, 40, 47, 53]. We also consulted prior work and conducted new empirical work to help us discover common narratives in people's recall of security adoption (N=17 interviewees).

The result is a novel framework of the steps of security behavior adoption (Figure 1): No Learning or Threat Awareness (Step 0), Threat Awareness (Step 1), Security Learning (Step 2), Security Practice Implementation (Step 3), Security Practice Maintenance (Step 4), and Security Practice Rejection (Step X). Analysis of prior work and data from our interviews offers support for the "whats" and "whys" of the framework.

This work adds to what is known in the literature and the SIGCHI community about the social-psychological drivers of security adoption. Further work can establish whether this is a reliable theoretical basis and method for focusing efforts where research shows that they are likely to be most productive. A refined version of this framework could provide an agenda for future experiments to validate whether step-matched interventions influence the adoption process.

2 RELATED WORK

Many examples exist of how *social influences* (ways in which the social environment leads people to adjust their beliefs, attitudes, and behaviors [64]) help boost uptake of protective practices [58]. Yet, as far as we know, no cybersecurity-specific framework exists that traces how awareness leads to action and the social influences to leverage at each step.

CHI EA '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0331-7/24/05
https://doi.org/10.1145/3613905.3651012

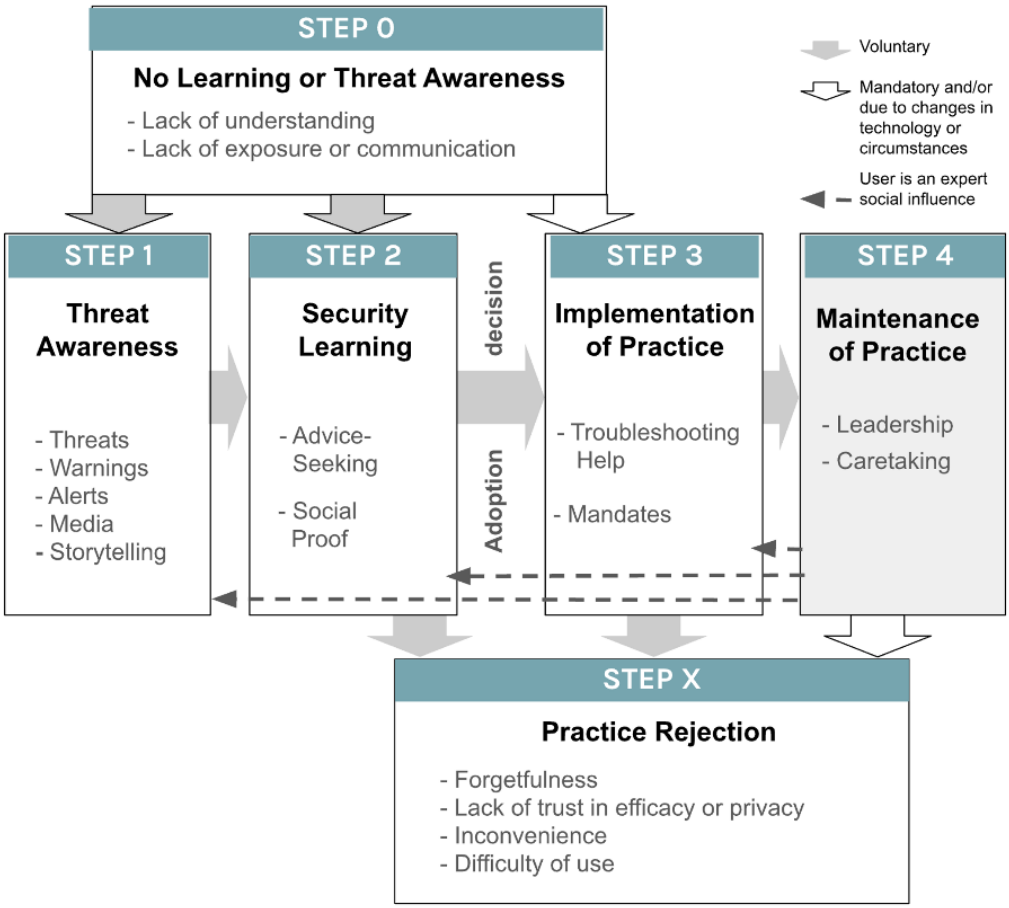

Figure 1: Our framework for reasoning about social-influence-in-the-loop shows six baseline steps, the associated social influences, obstacles, and path relationships. The outlined arrows indicate where the path could be a forced change (such as an employer requiring security awareness training, a bank mandating two-factor authentication, or a new Mac user discontinuing anti-virus).

2.1 Social Drivers of Threat Awareness and Security Learning

An extensive literature now documents how users become aware of cyberthreats and of the security practices that help them cope with these threats. Users' first-hand experiences of security breaches are significantly associated with their security attitudes and behavior intentions [19] and can be the "prompt" that drives acceptance of security and privacy practices [10]. People hear informal stories that teach them about cybersecurity [42–44, 54]. They seek advice when needed from trusted family members and authority figures [45, 46], and they passively become aware of secure practices and whether and how to enact them through observing others' behaviors [9, 11, 13].

News media make the public aware of threats through reporting on data breaches, such as the 2017 Equifax hack [65] or the 2021 and 2012 breaches of LinkedIn [50]. Beyond these reports, many lessons about security come via entertainment media such as the television show *Black Mirror*, although this can result in mental models that are incorrect [24]. Social proof, in which people look to others for signifiers of correct behaviors [4], is an influence on security awareness and adoption [9, 11] that can operate at mass scale through social computing [14, 58]. 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 [12, 13].

Our framework incorporates these findings as Step 1: *Threat Awareness* and Step 2: *Security Learning*, and the associated factors of *Threats*, *Warnings*, *Alerts*, *Media*, *Storytelling*, *Advice-Seeking*, and *Social Proof*. It notes their absence as Step 0: *No Learning or Threat Awareness*.

2.2 Social Drivers of Implementing and Maintaining Security Practices

An important form of social influence on security behaviors is authority [4, 5]. 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 [5]. For example, in a 2016 interview study on advice sources for digital security [45], 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" [34], "tech caregiver" [30] or "helper" [38] for friends, family and coworkers. These leadership or caretaking roles are embedded in social relationships and can be inconsistent with traditional power dynamics [30, 34, 38]. By contrast, authority derived from a hierarchy can nudge or force action (such as with security mandates) and can be seen as impersonal [5]. Its effectiveness can vary due to the type of practice, individual characteristics, and advice form [45].

Fear appeals are important [3, 32, 48] but not sufficient to persuade people to adopt security practices [55]. One study of those impacted by the 2017 Equifax data breach found that more than half of interview participants had failed to actively take protective measures such as freezing their credit, despite the perceived high risk [60]. Studies of more general security concerns have found that people need not just awareness, but also ability and sufficient motivation to use security practices [9, 11, 32, 48]. A 2020 CHI paper [62] reported that security, privacy, and identity theft protection practices were partially adopted or abandoned because users found them inconvenient, unusable, or unnecessary due to low perceived risk. Troubleshooting or "reactive" help [17] has long been found effective in removing barriers such as lack of ability or lack of usability. Participants in a 2016 study of the software updating process [51] mentioned troubleshooting at each step, most often when the installation failed or when the updated software showed problems.

Our framework incorporates these findings as Step 3: *Implementing Security Practices* and Step 4: *Maintaining Security Practices*, and the associated factors of *Troubleshooting Help*, *Mandates*, *Leadership*, and *Caretaking*. It notes adoption failure as Step X: *Security Practice Rejection*, associated with *Forgetfulness*, *Lack of Trust in Efficacy or Privacy*, *Inconvenience*, and *Difficulty of Use*.

2.3 Other Relevant Theories and Empirical Work

We also conducted a review of the behavior models that seemed most relevant to our research questions. For example, *Protection Motivation Theory (PMT)* [32, 48], argues that, in the presence of a threat, threat appraisal and coping appraisal will lead to protection motivation (Figure 2). PMT has been used widely in cybersecurity [57] to craft fear appeals, such as messaging about potential threats [3] and their potential severity [57]. But, Menard et al. noted that applying PMT has not always resulted in individuals performing a behavior to safeguard information [33]. We included questions in our interview study to ask about participants' recent security concerns and how they recalled responding to them.

For behavior change, *Innovation Diffusion Theory (IDT)* [47] seemed particularly relevant. IDT is best known for its adopter stages by time to adoption (innovator, early, early majority, late majority, and laggards), specified environmental factors for diffusion

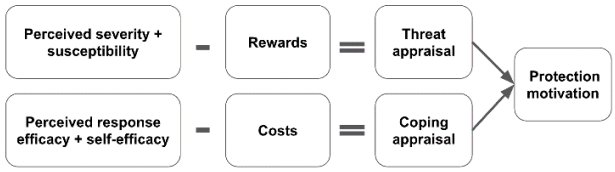

Figure 2: Illustration of Protection Motivation Theory. Threat appraisal and coping appraisal are the key antecedents of protection motivation; each is the result of a calculation of pros and cons.

(messaging channels, time, and social systems) and attractiveness of innovation characteristics that support diffusion (relative advantage, complexity, trialability, potential for re-invention, and observable effects). The innovation-decision process unfolds in five stages (Figure 3): (1) knowledge, (2) persuasion, (3) decision, (4) implementation, and (5) confirmation. In security and privacy, researchers have used IDT to examine mobile banking [1], social influences on security awareness, motivation, and knowledge [11], the diffusion of federated identity management [27], and individual differences affecting secure behaviors [28]. Inspired by IDT, we included interview questions to discover how communication channels and the perceived characteristics of security practices affected the decision process.

We found that empirical research also has been used in human-computer interaction to define an adoption process from the ground up. Vaniea and Rashidi [52] surveyed N=307 Amazon Mechanical Turk workers about memorable software updates. They used content analysis to identify six steps: (1) awareness, usually through a notification; (2) deciding to update, (3) preparation, (4) installation, (5) troubleshooting, and (6) post state. We likewise decided to conduct original empirical research to inform our framework development.

3 DEVELOPING THE FRAMEWORK

We developed our framework for reasoning about social influences on humans-in-the-loop (Figure 1) using data from three sources: (1) our team discussions and iterative drawings of potential constructs and relationships; (2) what we gleaned from the behavior-change literature and from prior work in usable security and privacy (Section 2); and (3) an original interview study with N=17 adult U.S. internet users. We received approval from our Institutional Research Board for the interview study. By examining the commonalities in the details of interviewees' security narratives and how they resonate with prior work, we inferred the existence of a baseline four-step process that resonated with our team discussions and insights from the behavior-change literature: *Threat Awareness* (Step 1), *Security Learning* (Step 2), *Security Practice Implementation* (Step 3), and *Security Practice Maintenance* (Step 4). We also inferred the "pre state" of *No Learning or Threat Awareness* (Step 0) and the "failure state" of *Security Practice Rejection* (Step X).

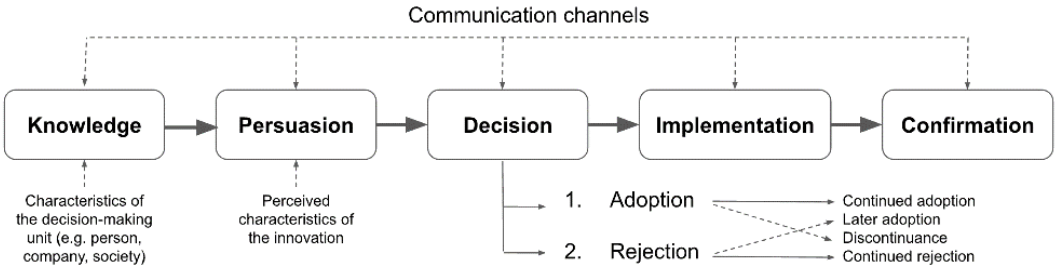

Figure 3: The innovation-decision process in Innovation Diffusion Theory. This describes how a person (or other decision-making unit) moves through, first, knowledge of an innovation; then, to forming an attitude toward the innovation; next, to a decision to adopt or reject it; and, finally, to implementing the new idea and to confirmation of the decision. Communication influences each stage.

3.1 Ideation

The idea for this framework, and the associated research questions, emerged from team discussions about how to pull together ad-hoc research into social influences in the usable security literature and enable measurable impacts. We identified a need for an easy-to-communicate theory that can help with reasoning before usable security failures instead of testing for them, and that can guide brainstorming and testing ways to intervene with end users that are proactive rather than reactive.

The first author conducted a thorough literature review that encompassed social drivers of security awareness and adoption, and of relevant theoretical models and process documentation (Section 2). Then, they created slides and sketches that listed possible constructs for such a theory and diagrammed possible relationships among the constructs. At each new phase of the development process, such as after conducting the literature review or analyzing the interview data, the team met to discuss how the new findings either confirmed these constructs and relationships or (more often) suggested changes to more closely fit the preliminary framework to the new data. Throughout, the first author drew on what they know of abductive thinking and sensemaking, triangulation, and synthesis of mixed-methods data [8, 23, 29, 59, 63]. The process is in the SIGCHI tradition of Design-oriented Research [22], in which truth or knowledge is produced through designing a tool or from the process of bringing a research artifact into being, and Social Computing [16, 35], which often mixes design ideation with social-behavioral data collection.

3.2 Interview study

Next, using findings from our literature review, we planned an interview study. The advantages of the interview method for empirical research are that we can elicit richer insights from fewer participants than with surveys and follow up on what participants say [56] and that the study can be conducted remotely and in a shorter period of time than if we observed behaviors in person [39]. To reach potential participants, we placed recruitment ads on Craigslist, Facebook, and Google targeted to 12 U.S. metro areas. People who clicked through to our pre-interview screener survey received a $3 e-gift card for responses to items about their awareness of and attitudes about security practices, as well as demographic characteristics. We computed a Security Score based on their screener responses and tried to recruit a diverse set from those with a High (150 and above), Middle (120-149), and Low (below 120) score (Table 1). The interview incentive was a $15 e-gift. In these 60-minute Zoom sessions, we used directed storytelling to elicit data about participants' memorable security concerns within the past three months; the steps that they recalled taking to respond to those security concerns; and, to what extent those steps were influenced by their social contacts, their prior experiences, or the characteristics of a given security practice. We discussed the interview data as it was collected and stopped conducting interviews once we reached data saturation, e.g., later participants repeated what we had heard earlier and contributed no new and relevant insights. See the Appendix for recruitment post, pre-screener survey and score method, and interview script.

For the interview analysis, we used qualitative coding and diagramming to identify and describe a coherent set of time-ordered details in participants' security narratives. By examining the commonalities in these details, we inferred the existence of a baseline four-step process for security awareness and adoption, along with a "pre state" and "failure state." We then examined how our interview data fit existing behavior-change models such as PMT and IDT, and prior work in usable security and privacy. The prior work included empirical studies of social influences on security awareness and adoption described in Section 2, as well as what is known from public media about how users have reacted to data breaches such as the 2017 Equifax hack [60, 65]. See the Appendix for the final version of our interview codebook.

4 FINDINGS FROM INTERVIEW DATA

Below, we highlight what we learned from our original research to develop the framework. Our findings for Step 2: Security Learning were consistent with prior work, so we omit the details below for brevity.

Table 1: Profile of *N*=17 participants whose data was used in the study analysis and the Security Score group that they were placed in. Data from one recruit, D1, was removed because of poor audio quality.

ID	Description	Score
C1	College lecturer in foreign languages	High
C2	Administrative assistant in government	High
C3	Financial and patient services	Middle
D2	Security worker for private companies	High
D3	Accountant and parent in large metro	Middle
D4	Recent college graduate in finance	Middle
D5	Householder and computer gig worker	Middle
D6	Freelance in information technology	Middle
D7	Accountant and parent in large metro	Middle
D8	Ex-teacher and computer gig worker	Low
D9	Recent college graduate and gig worker	Middle
D10	Contractor for medical scheduling	Low
D11	Teacher and parent in a small metro	Low
D12	Musician/gamer, spouse in security	High
D13	Householder and computer gig worker	Low
D14	Householder and graduate student	Middle
D15	Full-time in information technology	Low

4.1 Findings for Step 0 and Step 1 (Pre-Security Learning)

Lack of understanding was a key obstacle for those in Step 0: *No Learning or Threat Awareness* and in Step 1: *Threat Awareness.* 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. Others said they only learned of practices such as two-factor authentication when they were forced to adopt them 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.)

Echoing Ruoti et al. 2017 [49], some felt a sense of inevitability about the prospect of suffering a breach. 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."*

A few participants also reported cultural or linguistic barriers to learning about or educating others about practices. This is because interface text or directions are often written in English 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."*

4.2 Findings for Step 3, Step 4, and Step X (Post-Security Learning)

Once interview participants had resolved their uncertainties about a security practice, trialability provided a specific path for them to move forward from Step 2 (*Security Learning*) to Step 3 (*Security Practice Implementation*). 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.

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 . . . 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."* 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. 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.

Less-savvy 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. We 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 [42, 45, 46] and social proof [11, 13] with not just awareness but also adoption of security practices. *"You call them back at this number for the company. And it's busy. . . . So, I'm after a while, thinking and I called my brother and my friend to help me out of this little jam here."*

In Step 4, social influence flows outward. Interview participants in long-term adoption seemed drawn to adoption leadership and to educating others on security. This suggests a natural pairing with those in Step 2 (*Security Learning*) or in Step X (*Security Practice Rejection*). Those in Step 2 have made no decision and may act if trusted sources resolve their doubts and troubleshoot their problems with implementing security practices, as in the case of password managers. Those in Step X have decided against the security practices they were asked about, as in the case of password managers, 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.

Lastly, for Step X, interview participants who reported rejecting or discontinuing security practices cited 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 [36, 62].

5 APPLYING THIS FRAMEWORK TO RESEARCH AND DESIGN

For security practices such as using password managers, Virtual Private Networks (VPNs) and Two-Factor Authentication (2FA), our framework (Figure 1) can help them figure out how to 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 put these practices to use? What defeats their intention to use the 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. Researchers can use the framework as a basis for creating a survey to use as a pre- and post-intervention measurement in future research studies. Such a survey could 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 [31] and Faklaris et al. 2022 for messaging and a short survey to measure use of two-step authentication among Amazon Mechanical Turk workers [21].)

Product and service designers also can benefit from the framework. They can make use of the framework 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.

6 LIMITATIONS AND FUTURE WORK

We suggest one possible framework for security practice adoption. 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. Future work should explore these social influence mechanisms in more depth, such as the impact of negative social influences and the role of digital literacy. This program of work will also need to identify whether the same model holds for end-user cybersecurity in the context of the workplace as well as in the home or other personal contexts.

Our interviews 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. While we felt that we had reached data saturation with our interview sample (participants began to simply repeat the same issues and offer no unique insights), we recognize that we likely have missed important voices and perspectives. Future work should assess the validity of this framework with people of other cultures and demographic variations.

Our approach introduces a pro-practice bias, in that it assumes that adopting a given security practice is the best course of action. 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 process as it happens.

7 CONCLUSION

In this paper, we described a framework for reasoning about social-influences-in-the-loop, and how we synthesized it from ideation within our team, findings from the behavior-change literature, prior work in Usable Security and Privacy, and N=17 interviews with adult U.S. internet users. We summarized results from the literature survey and the interview study, and we provided recommendations for applying this framework to research and design. Finally, we listed the limitations and described future work that can build on this short paper.

Our work will help researchers and designers to identify new interventions in social computing that can remove obstacles at each step of security practice adoption. We hope this will be a meaningful step toward reducing the overwhelming amount of human involvement in cybersecurity breaches.

ACKNOWLEDGMENTS

The authors thank our research participants for their insights, as well as our reviewers and lab and department colleagues for their generous and useful feedback. This work was supported by a grant from the U.S. National Science Foundation, number CNS-1704087.

REFERENCES

[1] 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

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

[3] 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

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

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

[6] 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/

[7] 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

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

[9] 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), 2019. USENIX Association Berkeley, CA. . Retrieved August 28, 2019 from https://www.usenix.org/conference/soups2019/presentation/das

[10] Sauvik Das, Cori Faklaris, Jason I. Hong, and Laura A. Dabbish. 2022. The Security & Privacy Acceptance Framework (SPAF). *Found. Trends® Priv. Secur.* 5, 1–2 (December 2022), 1–143. https://doi.org/10.1561/3300000026

[11] 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*, 2014. USENIX Association Berkeley, CA. . Retrieved from https://www.usenix.org/system/files/conference/soups2014/ soups14-paper-das.pdf

[12] 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*), 2014, New York, NY, USA. ACM, New York, NY, USA, 739–749. . https://doi.org/10.1145/2660267.2660271

[13] 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*), 2015, New York, NY, USA. ACM, New York, NY, USA, 1416–1426. . https://doi.org/10.1145/2675133.2675225

[14] 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.

[15] James W. Dearing and Jeffrey G. Cox. 2018. Diffusion Of Innovations Theory, Principles, And Practice. *Health Aff. (Millwood)* 37, 2 (February 2018), 183–190. https://doi.org/10.1377/hlthaff.2017.1104

[16] Thomas Erickson. Social Computing. *The Encyclopedia of Human-Computer Interaction*. Retrieved September 12, 2023 from https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/social-computing

[17] World Leaders in Research-Based User Experience. Help and Documentation: The 10th Usability Heuristic. *Nielsen Norman Group*. Retrieved February 10, 2023 from https://www.nngroup.com/articles/help-and-documentation/

[18] Cori Faklaris, Laura Dabbish, and Jason Hong. 2018. Adapting the Transtheoretical Model for the Design of Security Interventions. Baltimore, Md., USA. Retrieved December 4, 2019 from https://doi.org/10.13140/RG.2.2.15447.57760

[19] 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)*, August 12, 2019, Santa Clara, CA. USENIX Association Berkeley, CA, Santa Clara, CA, 18. . Retrieved from https://www.usenix.org/system/files/soups2019-faklaris.pdf

[20] 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)*, August 12, 2019, Santa Clara, CA. USENIX Association Berkeley, CA, Santa Clara, CA, 18. . Retrieved from https://www.usenix.org/system/files/soups2019-faklaris.pdf

[21] 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. https://doi.org/10.48550/arXiv.2205.06937

[22] Daniel Fallman. 2003. Design-oriented Human-computer Interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (*CHI '03*), 2003, New York, NY, USA. ACM, New York, NY, USA, 225–232. . https://doi.org/10.1145/642611.642652

[23] 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. https://doi.org/10.1111/1475-6773.12117

[24] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L. Mazurek. 2019. The Effect of Entertainment Media on Mental Models of Computer Security. 2019. 79–95. . Retrieved August 21, 2022 from https://www.usenix.org/conference/soups2019/presentation/fulton

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

[26] Heather A. Hausenblas, Erin A. Dannecker, Daniel P. Connaughton, and Timm R. Lovins. 1999. Examining the validity of the stages of exercise change algorithm. *Am. J. Health Stud. Silver Spring* 15, 2 (1999), 94–99.

[27] Detlef Hühnlein, Heiko Roßnagel, and Jan Zibuschka. 2010. *Diffusion of federated identity management*. Gesellschaft für Informatik e.V. Retrieved January 15, 2022 from http://dl.gi.de/handle/20.500.12116/19795

[28] 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. https://doi.org/10.1080/0144929X.2021.1977849

[29] Jon Kolko. 2010. Abductive Thinking and Sensemaking: The Drivers of Design Synthesis. *Des. Issues* 26, 1 (January 2010), 15–28. https://doi.org/10.1162/desi.2010.26.1.15

[30] 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. https://doi.org/10.1145/3432954

[31] 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*), 2006, Berlin, Heidelberg. Springer-Verlag, Berlin, Heidelberg, 261–278. . https://doi.org/10.1007/11853565_16

[32] 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. https://doi.org/10.1016/0022-1031(83)90023-9

[33] 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. https://doi.org/10.1080/07421222.2017.1394083

[34] 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. https://doi.org/10.1145/3449212

[35] Manoj Parameswaran and Andrew B. Whinston. 2007. Social Computing: An Overview. *Commun. Assoc. Inf. Syst.* 19, (2007). https://doi.org/10.17705/1CAIS.01937

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

[37] 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. https://doi.org/10.1097/JES.0b013e3181d49612

[38] 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*), April 04, 2009, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 739–748. . https://doi.org/10.1145/1518701.1518816

[39] Jennifer Preece, Helen Sharp, and Yvonne Rogers. 2015. *Interaction Design: Beyond Human-Computer Interaction* (4th ed.). Wiley. Retrieved May 10, 2019 from https://www.wiley.com/en-us/Interaction+Design%3A+Beyond+Human+Computer+Interaction%2C+4th+Edition-p-9781119020752

[40] 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.

[41] 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. https://doi.org/10.1037/0022-006X.51.3.390

[42] 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. https://doi.org/10.1111/spc3.12329

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

[44] 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)*, 2012. USENIX Association Berkeley, CA, 1. . https://doi.org/10.1145/2335356.2335364

[45] 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)*, May 2016. 272–288. . https://doi.org/10.1109/SP.2016.24

[46] 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*), 2016, New York, NY, USA. ACM, New York, NY, USA, 666–677. . https://doi.org/10.1145/2976749.2978307

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

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

[49] 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. 2017. 211–228. . Retrieved February 11, 2021 from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/ruoti

[50] Michael Hill and Dan Swinhoe. 2022. The 15 biggest data breaches of the 21st century. *CSO Online*. Retrieved February 9, 2023 from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[51] 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*), 2016, New York, NY, USA. ACM, New York, NY, USA, 3215–3226. . https://doi.org/10.1145/2858036.2858303

[52] 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*), 2016, New York, NY, USA. ACM, New York, NY, USA, 3215–3226. . https://doi.org/10.1145/2858036.2858303

[53] 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.

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

[55] 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*), September 10, 2001, New York, NY, USA. Association for Computing Machinery, New York, NY, USA, 137–143. . https://doi.org/10.1145/508171.508195

[56] Robert S. Weiss. 1995. *Learning From Strangers: The Art and Method of Qualitative Interview Studies*. Simon and Schuster.

[57] Emma J. Williams, Jan Noyes, and Bogdan Warinschi. 2018. How Do We Ensure Users Engage In Secure Online Behavior? A Psychological Perspective. January 29, 2018. . https://doi.org/10.5176/2251-1865_CBP18.49

[58] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *Proceedings of the 43rd IEEE Symposium on Security & Privacy*, 2022, Oakland, CA, USA. IEEE Computer Society, Oakland, CA, USA, 17. . Retrieved from https://sauvikdas.com/uploads/paper/pdf/36/file.pdf

[59] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research Through Design As a Method for Interaction Design Research in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (*CHI '07*), 2007, New York, NY, USA. ACM, New York, NY, USA, 493–502. . https://doi.org/10.1145/1240624.1240704

[60] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. 2018. 197–216. . Retrieved October 14, 2022 from https://www.usenix.org/conference/soups2018/presentation/zou

[61] 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*, April 21, 2020, Honolulu HI USA. ACM, Honolulu HI USA, 1–15. . https://doi.org/10.1145/3313831.3376570

[62] 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*, April 21, 2020, Honolulu HI USA. ACM, Honolulu HI USA, 1–15. . https://doi.org/10.1145/3313831.3376570

[63] 2010. Triangulation. In *Encyclopedia of Research Design*. SAGE Publications, Inc., 2455 Teller Road, Thousand Oaks California 91320 United States. https://doi.org/10.4135/9781412961288.n469

[64] 2017. Social influence. *Wikipedia*. Retrieved September 13, 2017 from https://en.wikipedia.org/w/index.php?title$=$Social_influence&oldid$=$800243709

[65] 2017. Equifax data leak may affect nearly half the US population. *CNET*. Retrieved October 23, 2017 from https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/

[66] 2019. *2019 Data Breach Investigations Report*. Verizon Enterprise. Retrieved May 8, 2019 from https://enterprise.verizon.com/resources/reports/dbir/

[67] 2020. *2020 Data Breach Investigations Report*. Verizon Enterprise. Retrieved May 28, 2020 from https://enterprise.verizon.com/resources/reports/dbir/

[68] 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/

[69] 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

[70] Home: Oxford English Dictionary. Retrieved January 15, 2022 from https://www.oed.com/

[71] 2021 Data Breach Investigations Report. *Verizon Business*. Retrieved September 19, 2021 from https://www.verizon.com/business/resources/reports/dbir/

APPENDIX

A EXAMPLE RECRUITMENT POST

Hello, my name is [anonymous], and I am part of a research project at [anonymous]. My colleagues and I need your help.

For our research into how people use information technology, we want to know more about how you deal with concerns about your devices and your accounts. If you are a U.S. resident age 18 or older, you are eligible to take our initial survey. The survey should take about 10-12 minutes to complete, for which you will be emailed a $3 Amazon gift card. You may also be invited to take part in a paid research interview at a later date.

Are you interested? If so, please email us at [anonymous], and we will send you more details. Thanks in advance for your consideration! Please forward this to anyone you think would be a good fit for our project, as well."

Table 2: Matrix table for the awareness questions in the screener.

	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)					

B A.2. PRE-INTERVIEW SCREENER

B.1 Survey Items

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

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: Never (1) Rarely (2) About half the time (3) Most of the time (4) 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

Q6.1 On the next page, we will present a series of statements about the use of security measures [19, 21]. 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: Strongly disagree (1) Disagree (2) Neither agree nor disagree (3) Agree (4) 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.

B.2 Method To Compute Security Score from Screener

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) [reverse-score Q7.7-Q7.10]

C INTERVIEW PROTOCOL

[After introductions, consent to recording and answering any questions:] 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?
- What caused your concern?
- How did you deal with it?
- Did you get advice about this from anyone? Tell me more about that. Why did you trust this person? Did you find their advice useful? Why? Why did you trust this source? Did you find their advice useful? Why?
- Did this make you aware of any tools or practices that you could use to deal with this concern? What was that?
- Did this make you consider using any new tools or practices to safeguard your security or privacy? Why do you think that is?
- Did you get any advice about this? Did you trust it? Did you find it useful?
- Did you, in fact, start using any new tools or practices? *[if yes]* Are you still using this? Why did you keep using it? *[if no]* Why do you think that is?
- Did this make you consider stopping anything you do online or with a computing device or account? Why is that?
- Did you get any advice about this? What was it? Did you trust it? Did you find it useful?
- Did you stop? Why?
- To what extent do you think that this concern is now resolved?
- 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?
- 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.

- 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 / If using, ask how long and why]*
- Did you get any advice about this? Did you trust it? Did you find it useful?
- [If not using, ask whether have considered using] If not, why? Did you once use it and then stop?
- Are there other benefits or drawbacks that we haven't covered?
- Did you get any advice about this? Did you trust it? Did you find it useful? If so, why?
- Do you think you are likely to start using this? When?

Are there other measures that you use for safeguarding your security and privacy online, that we haven't talked about?

- *[for each]* How long have you used this measure? What made you start using this measure? How did you find out about it?
- Do any family members use this measure? Did they give you advice about it? Did you trust it? Did you find it useful?
- o any friends use this measure? Did they give you advice about it? Did you trust it? Did you find it useful?
- Did you have any interactions with someone in IT about this? Did you trust it? Did you find it useful?
- 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? Did you trust their advice? Did you find it useful?
- Are there any other sources that you consulted?
- Have you given anyone advice about using this measure?
- Is there anything else that you think I should know about this?

Are there other measures that you are aware of but do not use?

- *[if no]* Why not?
- *[if yes]* Did you get any advice about this? Did you trust it? Did you find it useful?
- Have you tried to use any other measures and stopped using them? Why? 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?

[Thank them for their time and answer any questions that they have]

D INTERVIEW CODEBOOK

We iteratively developed the following codebook based on initial data collection, then discussion among the team, followed by successively applying the codes to new transcripts and discussing the definitions and associated steps.

Table 3: Code, Description, Source, and Associated Step.

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	[62]; 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 [70]	(Cross-cutting)
/Voluntary	Not required, not compulsory. The degree of control a participant perceives or actually experiences over adopting a security practice.	Adapted from [70]	(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 [70]	(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 [70]	(Cross-cutting)
Communication channel	"Means by which a message gets from a source to a receiver" whether or not security-related (specific or nonspecific)	[47]	(Cross-cutting)
CS/IS experience	Skills, education, career, or ability for computing and information behaviors	[45]; 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)	[4, 47]; authors	(Cross-cutting)
/Media	Any reference to means of mass communication (broadcasting, publishing, and the internet)	Adapted from [70]	(Cross-cutting)
/Peers	one who is of approximate equal standing with another in a sphere of influence	Adapted from [70]	(Cross-cutting)
/Authorities	a person or organization having power in a particular sphere, such as the workplace or a family	Adapted from [70]	(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])	[47]	(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	[7, 20, 45]	(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	[7, 20]	(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	[7, 20]	(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	[7, 20]	(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	[66, 67, 71]; 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	[32, 37]; 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	[32, 37]; 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	[32, 37]; authors	Security Learning (Step 2)
Unawareness	No knowledge of the existence of a given security practice or other technology.	[18]	Threat Awareness (Step 1)
Awareness	Knowledge of existence of a given security practice or other technology, but no enactment of that practice	[18]	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 [70]	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	[18]	(Cross-cutting)
/Trialing adoption	Acting to test the security practice to evaluate its usefulness in everyday life	[47]; authors	Security Practice Implementation (Step 3)
/Implementing adoption	Acting to put the decision to adopt a security practice into effect in everyday life	[41, 47]; 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	[41, 47]; 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	[18]	(Cross-cutting)
/Discontinuing adoption	Stopping use of a practice once it has already been used at least once; explicit mention	[41, 47]; authors	Security Practice Implementation (Step 3)
/Rejecting adoption	Deciding against use of a practice before it has been used once; explicit mention	[41, 47]; authors	Security Learning (Step 2)
Time	Any recognition of something occurring other than in the current moment, either past or future	[25, 47]	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 [70]	(Cross-cutting)