

# I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security

Elissa M. Redmiles  
Department of Computer Science  
University of Maryland  
College Park, Maryland 20742  
eredmiles@cs.umd.edu

Amelia Malone  
Department of Computer Science  
University of Maryland  
College Park, Maryland 20742  
amalone2@terpmail.umd.edu

Michelle L. Mazurek  
Department of Computer Science  
University of Maryland  
College Park, Maryland 20742  
mmazurek@cs.umd.edu

**Abstract**—Users receive a multitude of digital- and physical-security advice every day. Indeed, if we implemented all the security advice we received, we would never leave our houses or use the Internet. Instead, users selectively choose some advice to accept and some (most) to reject; however, it is unclear whether they are effectively prioritizing what is most important or most useful. If we can understand from where users take security advice and how they subsequently develop security behaviors, we can develop more effective security interventions.

As a first step, we conducted 25 semi-structured interviews of security-sensitive (those users who deal with sensitive data or hold security clearances) and general users. These interviews resulted in several key findings: (1) users' main sources of digital-security advice include IT professionals, workplaces, and negative events, whether experienced personally or retold through TV; (2) users determine whether to accept digital-security advice based on the trustworthiness of the advice-source, as they feel inadequately able to evaluate the advice content; (3) users reject advice for many reasons, from believing that someone else is responsible for their security to finding that the advice contains too much marketing material or threatens their privacy; and (4) security-sensitive users differ from general users in a number of ways, including feeling that digital-security advice is more useful in their day-to-day lives and relying heavily on their workplace as a source of security information. These and our other findings inform a set of design recommendations for enhancing the efficacy of digital-security advice.

## I. INTRODUCTION

In the United States Computer Emergency Readiness Team (US-CERT) list of advice for home computer users there are 61 topics, with at least three paragraphs and approximately 500 words of advice per topic. This single US-CERT page contains more than 30,000 words of digital-security advice. If users listened to all of the security advice that must be contained in all of the digital- and physical-security advice sources available today, they would never leave their houses or use the Internet again. Since users are still leaving their houses, and most certainly still using the Internet, how are they determining which security advice to implement and which to discard? It is important to understand how users learn security behaviors in order to ensure that the best or most important security tactics can break through the noise and attract adoption from users.

Previous research related to users' security behaviors has primarily focused on identifying those behaviors and experi-

menting with how to change them [1], [2]. Other work has shown the important influence of social factors on security behavior [3], [4]. Additional work has proposed that users choose which behaviors to practice based on an analysis of the costs and benefits [5], [6]. Yet other work has examined which pieces of digital-security advice are most important [7].

Despite this past work, there has been no comprehensive analysis of why users choose to accept and reject digital security advice and from what sources they take this advice. Therefore, as a first step toward establishing best practices for designing and disseminating security advice, we sought to answer the following research questions:

- Q1) Where do users learn digital and physical security behaviors?
- Q2) Why do users accept or reject different advice?
- Q3) How do users' advice sources, reasons for accepting or rejecting advice, and valuation of advice differ for digital and physical security?
- Q4) Do users from different demographic groups consult different advice sources or have different reasons for accepting or rejecting advice?
- Q5) Do different advice sources lead to more secure users?

To address these questions, we conducted a semi-structured interview study with 25 participants of varied demographics. During a 60-minute interview, we asked questions designed to help participants articulate their digital-security habits, as well as where they learned these strategies and why they chose to implement them. We also addressed where they learned and why they reject security strategies that they have heard about but choose not employ. We explicitly compared this information to the ways that participants learn and process physical-security advice, to see whether mechanisms that inform physical-security advice-taking can be imported to the digital domain. Further, we recruited participants in two groups: security-sensitive users who handle data governed by a security clearance or by HIPAA or FERPA regulations, and general users who do not. This allowed us to consider the effect that regular exposure to a data-security mindset has on the ways that users process security advice in their personal (non-work) lives. Finally, we explored as a case study participants' reactions to two-factor authentication, which has

been identified as a highly effective but underutilized security tool [7].

We rigorously analyzed this interview data using an iterative open-coding process. We identified several key findings, including:

- Participants evaluate digital-security advice based primarily on the trustworthiness of the advice source. This contrasts sharply with physical security, where the trustworthiness of the source is less important because users feel comfortable evaluating the content of the advice themselves and determining its value. Security-sensitive participants are even more likely than other participants to rely on the trustworthiness of the source of digital-security advice.
- Participants have many more reasons for rejecting both digital- and physical-security advice than for accepting it. For digital security in particular, these reasons include not just the obvious—that advice is too complicated or that the participant is oversaturated—but also more subtle rationales, such as the presence of too much marketing, concerns about privacy, and the expectation that someone or something else (often a digital service provider) is responsible for keeping them safe.
- Prior work has identified negative personal experience as a learning tool [2]; we extend this by finding that TV shows and movies that present negative security events with clearly defined causes can be equally strong motivators for adopting new security behaviors.
- Security-sensitive participants are more likely than other participants to believe that digital-security advice is more useful in their day-to-day lives than is physical-security advice; they are also more likely to cite their workplace as a source of digital-security advice they adopt. This suggests that exposure to a data-security mindset does affect the way users process security information, even in a non-work context.

Based on these and other trends extracted from our interviews, we distill recommendations for designing and disseminating more effective security advice. We believe these guidelines can help security experts to magnify the impact of truly important security advice.

## II. RELATED WORK

In this section, we discuss prior research in three related areas: examining the factors that influence users’ security behaviors, determining which security behaviors or recommendations are valuable, and developing or evaluating security behavior interventions.

### A. Factors Influencing Security Behaviors

Several researchers have examined how specific factors influence security behaviors. Das et al. demonstrated the importance of social influence; for example, showing users information about their Facebook friends’ security behaviors made them more likely to adopt the same behaviors [1], [8].

Relatedly, Rader et al. found that security stories from non-expert peers affect how users think about computer security and how they make security decisions like whether to click on a link [2]. Wash identified “folk models” of security, such as viewing hackers like digital graffiti artists, that influence users’ perceptions of what is and is not dangerous [9]. Our work broadens these findings by explicitly considering a variety of ways, social and otherwise, in which users may learn about different security behaviors.

Security decisions are often framed as economic tradeoffs, in which users ignore security best practices due to rational cost-benefit optimization. Herley, for example, suggests that if users were to spend one minute of each day checking URLs to avoid phishing, the time cost would be much larger than the cost of the phishing itself [5]. To investigate whether users are in fact making rational cost-benefit calculations, we examine users’ reported thought processes when accepting and rejecting security advice. Further, researchers have considered a *compliance budget*: the limited time and resources users can spend on security behavior [6], [10]. This highlights the importance of understanding how users decide which advice they spend their compliance budget on, so that the most valuable advice can be designed to rise to the top. Although this prior work also focuses on why users implement or reject security behaviors, our work differs in a few key ways: our study is about home security behaviors, whereas Beaument et al. addressed only the organizational environment; relatedly, our study draws from a larger and more diverse participant pool; finally, we investigate not only why users reject security behaviors but also why they accept or reject advice and from what sources, including but not limited to their workplace, they get this advice.

Other researchers have considered how demographics affect security and privacy decision-making. Howe et al. note that socioeconomic status, and the corresponding belief that one’s information may not be “important enough to hack,” can affect security behaviors [4]. The paper also notes large differences in advice sources between undergraduate and adult populations. Wash and Rader investigated security beliefs and behaviors among a large, representative U.S. sample and found that more educated users tended to have more sophisticated beliefs but take fewer precautions [11]. Others have investigated how demographic and personality factors influence susceptibility to phishing [12], [13]. Rainie et al. found that younger people, social media users, and those who had a prior bad experience were more likely to try to hide their online behavior. Based on this prior work, we recruited specifically for diversity of age, income, education, and race. Further, we recruited for and analyzed the impact of an additional type of diversity: security sensitivity, meaning professional training to handle confidential or sensitive data. In addition, during our data analysis, we coded for participants who discussed whether their information was important to protect and whether they had prior negative experiences.

Although prior work touches on similar themes, to our knowledge we are the first to comprehensively examine users’

primary sources of digital security advice in general and why they choose to accept or reject it. Further, our work directly compares digital security to physical security, which has a much longer history of providing and adopting behavioral advice. By drawing lessons from each domain, we develop design guidelines for effectively transmitting security information.

**Assessing Security Behaviors.** In order to assess the factors that influence participants' security behaviors, it is important to know what behaviors participants are using. One tool to assess participant behaviors is SEBIS, a 16-item measure of self-reported security behaviors [14]. In this paper, we apply SEBIS as an objective measure of participants' relative security levels.

### *B. Expert Advice and Best Practices*

Any attempt to improve the dissemination and adoption of security advice will of course require decisions about which advice is relevant and important. In recent work, Ion et al. surveyed more than 200 security experts to determine what behaviors they most often practice and/or strongly recommend [7]. Top suggestions included installing software updates, using two-factor authentication, and using a password manager. Corporate and government help pages from organizations such as Microsoft, the United States Computer Emergency Readiness Team, and McAfee also provide users with pieces of top advice, including tips for improving the strength of passwords and encouragement to update software regularly [15]–[17]. These best practices provide insight into what advice is most valuable to give users; in this paper, we address the related but orthogonal problem of how users receive and respond to advice, and therefore how important advice can be disseminated when it is identified.

### *C. User Education and Security Interventions*

There is a large body of work devoted to analyzing and improving delivery of security information to users, particularly in the context of user education and designing security warnings. For example, significant research has examined how to educate users about phishing prevention [18]–[20]. There has also been considerable work addressing the effectiveness of phishing and SSL warnings for browsers [21]–[24], banking security warnings [25], and security-warning habituation generally [26]. Other researchers have considered how best to nudge users to create stronger passwords [27], [28] and how to inform them about potentially invasive mobile app permissions [29], [30]. Our work takes an alternate view: rather than focus on how to promote adoption of one specific security behavior, we consider why users make the security decisions they do, where they get their educational materials, and how they evaluate credibility.

## III. METHODOLOGY

To answer our research questions, we conducted semi-structured interviews in our laboratory between March and October 2015. To support generalizable and rigorous qualitative results, we conducted interviews until new themes

stopped emerging (25 participants) [31]. Our subject pool is larger than the 12-20 interviews suggested by qualitative best-practices literature; as such, it can provide a strong basis for both future quantitative work and generalizable design recommendations [32].

The study was approved by our institution's human-subjects ethics review board. Below, we discuss our recruitment process, interview procedure, details of our qualitative analysis, and limitations of our work.

### *A. Recruitment*

We recruited participants from a large metro area in the U.S. via Craigslist postings and by sending emails to neighborhood listservs. We also distributed emails in public- and private-sector organizations with the help of known contacts in those organizations. In addition, we posted flyers in university buildings and emailed university staff members. We collected demographic information including age, gender, income, job role, zip code, and education level from respondents in order to ensure a broad diversity of participants. Participants were compensated \$25 for an approximately one-hour interview session.

### *B. Procedure*

We asked participants to bring a device they use to connect to the Internet for personal use with them to their interview. Two researchers conducted all of the interviews, which took between 40 and 70 minutes. We used a semi-structured interview protocol, in which the interviewer primarily uses a standard list of questions but has discretion to ask follow-ups or skip questions that have already been covered [33]. Semi-structured interviews allow researchers to gather information about participants' practices, habits, and experiences as well as their opinions and attitudes [33].

During the interview, we asked questions about participants' digital- and physical-security habits as well as where they learned those habits (Q1). We also asked participants to "act out" their use of technology in a series of scenarios. We asked questions about participants' behaviors and advice sources for digital-security topics such as device security, including password protection and antivirus use; web browsing and emailing, including two-factor authentication and phishing questions; and online banking and shopping, including questions about the participant's banking login process and payment methods (Q1, Q3). We asked similar questions regarding physical-security topics such as dwelling security, including questions about locking methods and alarm systems; transit (e.g. car and bike) security, with questions similar to those asked for dwelling security; and personal safety when walking alone, including questions about carrying weapons (Q1, Q3). We validated that our list of digital security topics broadly covered the same topics as those mentioned as high priority in Ion, Reeder and Consolvo's recent paper [7].

On each of these topics, participants were first asked a general open-ended question regarding their security behaviors: for example, "How do you protect your devices?" and

then asked sequentially more specific questions, for example: “Can you show me how you access the home screen on your smartphone?”, “Have you always had/not had a password on your smartphone?”, and “Are there other strategies you use for protecting your devices which you have not mentioned?” Participants were subsequently asked a series of follow-up questions on each topic, such as “Why do you use this strategy?” (Q2); “Have you ever had a negative experience with...?” (Q1); and “Where or from whom did you learn this strategy?” (Q1). In addition to questions regarding specific security topics, participants were asked more generally about where, from whom, and why they accepted security advice, as well as about strategies they had considered but not adopted (Q2). Participants were also asked to compare digital- and physical-security advice in terms of usefulness and trustworthiness (Q3). Finally, participants were asked to briefly describe their current or most recent job. They were specifically asked if they handled sensitive data as part of their job, and if so, what kind (Q3).

To more objectively assess participants’ security behavior, we also administered the Security Behavior Intentions Scale (SEBIS) at the end of the interview session (Q5) [14]. The SEBIS measure was given to 16 of our 25 participants, as we added it once it became available. Finally, demographic information was collected during recruitment (Q4).

### C. Analysis

The interview data was analyzed using an iterative open-coding process [34]. Once the two researchers completed the interviews, they transcribed 17 of the interviews. The remaining eight interviews were transcribed by an external transcription service. The researchers then met in person to develop and iteratively update an initial set of codes for the data. Subsequently, they independently coded each interview, incrementally updating the codebook as necessary and re-coding previously coded interviews. This process was repeated until all interviews were coded. We then compared the codes of the two interviewers by computing the inter-coder percent agreement using the ReCal2 software package [35]. The inter-coder percent agreement for this study is 75%. This is a reasonable score for an exploratory semi-structured study, with a large number of codes, such as ours [36]. Further, after calculating this percent agreement score, the interviewers met to iterate on the codes until they reached 100% agreement on the final codes for each interview.

### D. Signifying Prevalence

For each finding, we state the number of participants who expressed this sentiment, as an indication of prevalence. However, our results are not quantitative, and a participant failing to mention a particular item for which we coded does not imply they disagree with that code; rather the participant may have simply failed to mention it. We plan to conduct a follow-up quantitative analysis to investigate the prevalence of our findings on a statistically representative sample.

### E. Limitations

Our study has several limitations common to qualitative research. While we asked participants to search their memory for answers to our questions, they may not have fully done so, or they may have forgotten some information. To mitigate satisficing [37], interviewers repeatedly prompted participants to give full answers to all questions. Participants may also have tired and provided less thorough answers toward the end of the interview, and those who were particularly concerned about the interviewer’s perception of them may have altered their answers in order to not portray themselves as overly secure or insecure [37], [38]. Additionally, the age, gender and race of the interviewers may have introduced some bias into participants’ responses. We recruited a diverse pool of participants to increase the odds that relevant ideas would be mentioned by at least one participant, despite these limitations.

## IV. RESULTS

In this section we detail the results of our study. First, we will discuss our participants’ demographics and security-sensitivity. An overview of these demographics is shown in Table I. Second, we will address the sources from which participants accept security advice and how these sources differ across genders and for physical and digital security. A summary of these sources is shown in Figure 1. Third, we will address the different reasons our participants gave for accepting and rejecting digital- and physical-security advice; some of the differences in these reasons were unanticipated. Fourth, we address differences between security-sensitive and general users, which imply that security-sensitive users’ advice taking behavior differs based on the digital-security information they are exposed to in their workplaces. Finally, we present a case study on two-factor authentication, a behavior found by Ion et al. to have high security importance, but low adoption [7].

### A. Participants

We recruited 158 potential participants and selected 47 to interview. We selected a balance of men and women, as well as a diversity of age, ethnicity and education. Of the 47 participants selected for interviews, 25 attended their interview appointments.

Demographics for our 25 participants are shown in Table I. Fifty-six percent of our participants are female, slightly more female than the general U.S. population in 2014 (51%) [39]. Our sample is somewhat less Hispanic (8% vs. 17%) and less White (40% vs. 62%), but more Black (44% vs. 13%) than the U.S. population [39]. We had a proportional number of Asian participants (8%). However, the racial makeup of our sample more closely matched the racial proportions of our metro area. Our metro area is 43% White (our sample: 40% White), 46% Black (our sample: 44%), 10% Hispanic (our sample: 8%) and 4% Asian (our sample: 8%) [40]. Our participant sample is wealthier than the US population and our demographic area: 28% of our participants earn less than \$50,000, whereas 47% of the general US population earns less than \$50,000 per year [41]; and 40.1% of people in

ID	Gender	Age	Race	Educ.	Income	Sec. Type
P1	M	31-40	W	M.S.	\$90-\$125k	F
P2	F	22-30	A	B.S.	\$50-\$70k	-
P3	M	18-22	W	SC	\$90-\$125k	F
P4	F	51-60	W	PhD	\$150k+	S
P5	F	22-30	B	M.S.	\$90-\$125k	F
P6	F	41-50	W	M.S.	\$30-\$50k	-
P7	F	31-40	H	M.S.	\$70-\$90k	F
P8	F	31-40	B	M.S.	\$90-\$125k	-
P9	M	22-30	W	B.S.	\$50-\$70k	S
P10	M	22-30	B	B.S.	\$50-\$70k	S
P11	M	60+	W	P	\$90-\$125k	C
P12	M	41-50	B	SC	\$0-\$30k	S
P13	F	31-40	A	M.S.	\$0-\$30k	-
P14	F	31-40	B	SC	\$90-\$125k	-
P15	F	41-50	B	Assoc.	\$50-\$70k	C
P16	F	31-40	H	H.S.	\$0-\$30k	-
P17	F	18-22	B	H.S.	\$0-\$30k	-
P18	M	18-22	B	H.S.	\$0-\$30k	-
P19	F	22-30	B	M.S.	\$50-\$70k	F
P20	F	60+	W	PhD	\$150k+	-
P21	M	41-50	W	PhD	\$150k+	C
P22	M	60+	W	SC	\$90-\$125k	-
P23	F	22-30	B	Assoc.	\$70-\$90k	H
P24	M	41-50	W	B.S.	\$30-\$50k	S
P25	M	18-22	B	Assoc.	\$70-\$90k	H

TABLE I

PARTICIPANT DEMOGRAPHICS. THE COLUMNS SHOW: PARTICIPANT IDENTIFIERS (CODED BY INTERVIEW DATE ORDER), GENDER, AGE, RACE, EDUCATION, INCOME, TYPE OF WORK SECURITY, AND SECURITY SENSITIVITY. THE ABBREVIATIONS W/B/A/H IN THE RACE COLUMN STAND FOR WHITE, BLACK, ASIAN, AND HISPANIC, RESPECTIVELY. THE ABBREVIATIONS NO H.S./H.S./SC/B.S./ASSOC./M.S./PH.D./P IN THE EDUCATION COLUMN STAND FOR NO HIGH SCHOOL, HIGH SCHOOL GRADUATE, SOME COLLEGE, BACHELORS DEGREE, ASSOCIATES DEGREE, MASTERS DEGREE, DOCTORAL DEGREE, AND PROFESSIONAL DEGREE (E.G. MBA, J.D.), RESPECTIVELY. THE SECURITY TYPE DATA COLUMN INDICATES WHICH TYPES OF SENSITIVE DATA THE PARTICIPANTS HANDLE, IF ANY. THE ABBREVIATIONS F/H/S/C/- IN THE SECURITY TYPE COLUMN STAND FOR FERPA, HIPPA, AND SSN DATA HANDLING, THE HOLDING OF A SECURITY CLEARANCE, AND NO WORK WITH SENSITIVE DATA, RESPECTIVELY.

our metro area earn less than \$50,000 [40]. Our sample is, however, representative of the educational attainment in our demographic area: 88% of our participants hold a high school degree or higher, compared with 90.1% per our metro area census; and 60% of our participants hold a Bachelor’s degree or higher, compared to 55% in our metro area [40].

### B. How Security Behaviors Are Learned

Participants reported implementing digital- and physical-security advice from a number of sources. In this section, we address our findings on users’ most common sources for both digital and physical security: media, family members, and peers. Additionally, we discuss negative experiences as a security behavior learning tool; our findings emphasize and expand prior findings on the importance of security stories for teaching digital security behaviors [2]. Next, we address advice sources unique to digital security, including IT professionals,

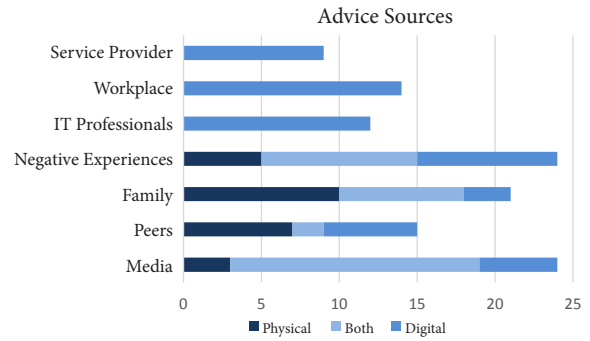


Fig. 1. Prevalence of advice sources for digital and physical security.

the workplace, and providers of participants’ digital services (e.g. Comcast). Finally, we include two interpretive sections discussing differences in advice sources between men and women, as well as whether different advice sources have an impact on users’ security behaviors, as measured with the SEBIS scale [14].

**Common Source: Media.** Almost all participants (N=24) reported receiving both digital- and physical-security information from media. Media included online articles, forums, television shows, news shows, the radio, magazines, and advertisements. Five participants reported using media as an information source only for digital security, three reported using media only for physical security, and the remaining 16 participants used media for both digital- and physical-security information. Of those who cited media as an advice source for digital security, six participants cited a specific technology-oriented resource: “Some of the blog[s] I read [are] by computer people. For example, I read Wired,” says P20. In general, the technical sources cited by these participants were: CNet, Wired, Bruce Schneier’s blog, Mashable, and an interview on the topic of Snowden conducted by John Oliver [42]–[46].

**Common Source: Peers.** Fifteen participants cited their peers as a source of digital- or physical-security advice. Peers included friends and colleagues who were not family members. Interestingly, only two participants cited peers as a source of advice for *both* digital and physical security. The remaining participants only cited peers as a source for digital (N=6) *or* physical security (N=7). It seems that if participants trust their friends on the topic of physical security, they do not consider them authoritative on digital security, and vice versa. Further, while a few participants consider some of these peers to be experts (N=5), expert status in all cases was determined not by education or job role (e.g. IT professional, alarm technician) but rather by participant’s perceptions of the “tech-savviness” or physical-security expertise of their peer.

**Common Source: Family.** Family members are another frequent source of physical and digital-security advice (N=21). Unlike their use of peers for only digital- or physical-security advice but not both, eight participants took advice from a fam-

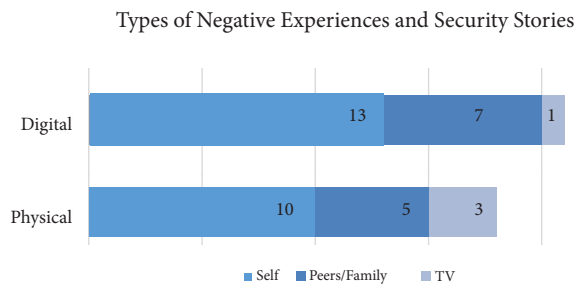


Fig. 2. Distribution of types of negative experiences from which participants learned new security behaviors: personal events, stories told by peers, and stories in TV shows or movies.

ily member for both physical and digital security. That said, 10 participants consulted family members *only* for physical-security advice while three consulted family strictly for digital-security advice. This may be because the family members most often consulted were parents, and younger participants whose parents are still living may not consult their older, and perhaps less tech-experienced, parents for digital security advice.

**Common Source: Negative Experiences.** As reported in Rader and Wash’s work on security stories, negative events described by peers or directly experienced by participants can be strong learning tools [2]. In our study, we found that 24 participants either had negative experiences themselves or knew peers who described negative events, which led to behavior changes. Our participant sample was smaller, yet broader, than that used in Rader and Wash’s work, and our results thus confirm the generalizability of their findings beyond the college student population [2]. Even more interestingly, we found that vignettes from TV shows may be equally salient as stories told by a friend or negative events experienced in real life.

Although only four participants cited TV shows specifically, each strongly recalled stories of negative physical or digital security-related events happening to characters in those shows. They directly credited these shows with leading to a specific change in their behavior. For example, P12 put a password on his WiFi network after watching a tech show that showed “people going by houses and WiFi snooping and knocking on people’s doors saying, ‘Oh your WiFi is open, you need to protect it’ ...shows like that, [they] make you think.” P14 had a similar experience: Watching a movie motivated her to always check the back seats in her car for a lurking person before getting into the car. “People had mentioned that you should check your back seats before but I never paid attention to it until [this] movie,” she says. Thus, it seems that TV shows or movies may serve as strong proxies for a negative experience that happens directly to the user or someone she knows. We hypothesize two reasons for this: (1) while participants often blamed themselves or their friends for personality or behavioral flaws that led to security problems, they were more likely to give relatable fictional characters or the unknown real victims shown on TV the benefit of the

doubt; and (2) TV shows and movies are typically designed to be vivid, realistic, and believable, thus making participants feel that what is happening on the screen could happen to them, too.

That said, we found that negative experiences that occur directly to the user were the most prevalent learning tools (N=13 for digital, N=10 for physical), as compared to security stories told by others (N=7 for digital, N=5 for physical) or conveyed via visual media (N=1 for digital, N=3 for physical). The distribution of the types of security stories on which participants relied is shown in Figure 2. Additionally, as might be expected, when participants feel that the person who experienced the negative event did all they could to prevent it and there are no additional measures that could be taken, the story of the negative event does not lead to any behavior change. For example, P2 had a friend who was robbed, but did not change her own behavior “because I think she took all the precautions she reasonably could. She parked in a brightly lit area and a reasonably safe neighborhood, pretty close to where she was going to be. I don’t think that there was much [that she could have done.] She could have had somebody walk with her maybe, but the guy had a gun, so I don’t think anything would have changed.” Further, if the participant believes the victim bears some responsibility for the negative event—for example, they are “not as tech-savvy” than the participant, or live in a “less safe area”, the negative event likely will not serve as a learning tool. P24 and P9 have had friends who got viruses, but they did not do anything differently afterwards, because they felt that the friends were victimized due to their lack of technical expertise. Finally, negative experiences may not be effective information sources when the user cannot identify why the negative event happened, or what they could have done to prevent it. For example P18 comments, “I actually think recently someone tried to log into my email from China and Google sent me an email and Google blocked it and said it looked strange and I said it was very strange,” but he did not alter his behavior after this incident.

In summary, our participants shared with us a total of 45 negative experiences or stories. As a result of 20 of these stories the participants’ changed a digital-security behavior. Additionally, 14 stories and experiences led to a physical behavior change, and eleven led to no change in behavior.

**Digital Only: IT Professionals.** IT professionals are an information source strictly for digital-security methods (N=12). These professionals can be colleagues in the participant’s work environment or friends of the participant. As we will discuss in Section IV-C, a participant’s belief that a digital-security advice source is trustworthy is a primary factor in whether participants choose to accept the advice; it seems that participants view IT professionals as especially trustworthy. “For personal, I might talk to one of the IT guys about that. I just talk to ...the one I’m most friends with, I always try to get information: what’s the best intervention, what do you think?” comments P15. Further, participants may use IT professionals to evaluate the trustworthiness of advice they

have seen elsewhere. For example, P19 says that when she is looking for new digital-security advice, she will “talk to the IT guy at my office. I’ve talked to him a couple of times about my phone and whatever I hear or read.” Although participants may receive useful advice from colleagues and friends who are IT professionals, this advice may not be sufficient. For example, as P13 notes: “My friends who work in IT, they just tell you to change your password as often as possible.”

**Digital Only: Workplace.** In addition to information users solicit from IT professionals, users also receive unsolicited security advice from their workplaces in the form of newsletters, IT emails, or required trainings. Fourteen participants cited receiving this type of advice. P4 says, for example, that she learned from work not to click links in emails that claim she needs to update her password. “We got an email from IT telling us that, never will there’ll be an email from them that would require you to do that.” Similarly, P8 pays attention to her security trainings at work: “They’ll do yearly IT security training, which is not even necessarily for work, but just for life ...they talk about things like not sending people money over Facebook ...they also email out updates when things change. I do actually pay attention to those emails when they send them, like about privacy notice updating.” Further, P2 says she “always reads the IT newsletter” put out by her workplace.

**Digital Only: Service Provider.** Another source of digital security information cited by nine participants is the corporations that provide a service to the participant (e.g. SunTrust Bank, Apple, Verizon). For example, P23 comments: “I usually call my carrier (Comcast) and they have security stuff for your internet and they’ll tell me what I can do.”

**Comparison: Gender and Advice.** Eighteen participants, evenly split between men and women, cited a man as a source of digital-security advice, while only three cited a woman. This may be because historically men have been overrepresented in technology and computing fields and thus are considered to be more authoritative on that topic [47]. Alternatively, the overabundance of digital-security advice provided by men may occur because men offer more unsolicited advice in the domain of digital security, or because women are still underrepresented in IT and computing fields and thus there are fewer women who chose to offer digital-security advice [48].

On the other hand, 12 participants cited a woman as a source of physical-security advice, compared to three participants who cited men. Eight of these 12 participants were women themselves. Historically, women have had higher rates of crime victimization, perceive themselves to be at higher risk of victimization, and express greater fear of crime than do men [49]. It is probable that women are aware of this gendered difference in threat levels and perceptions, and thus find each other more relatable sources of advice.

**The Impact Of Different Advice Sources On Users’ Security Behaviors.** We used the SEBIS scale to measure participants’ security behavior intentions; the scale results in

a score from 1 to 5 [14]. A score of 5 indicates that the user intends to behave more securely than a user with a score of 1. The average SEBIS score for participants who used each of the information sources mentioned above were all between 2.7 and 3.3; therefore, we find no evidence that any particular advice source impacts behavioral intentions more than another.

### C. Why Advice is Accepted

What leads users to accept advice from the sources mentioned above? In this section, we discuss participants’ reasons for accepting digital-security advice: we find the trustworthiness of the advice source is the key metric for the domain of digital security. This finding may be explained by another of our findings: participants struggle to assess the plausibility and value of digital-security advice. In contrast, participants’ relative confidence in their assessment of the plausibility of and necessity for physical-security advice leads them to cite their own evaluation of the advice’s content as the primary assessment metric in the physical domain. We also in this section compare which advice, physical or digital, participants feel is more useful and/or more trustworthy.

**Digital-Security Advice.** Eleven participants used the trustworthiness of the advice source to determine whether to take digital-security advice.

In the case of media advice, participants must determine whether advice offered by an unknown author is trustworthy. Participants mentioned five heuristics that they use to measure the trustworthiness of a media advice source, including: their knowledge and trust of the advice author, other user’s reviews of the advice, how widespread the advice was on various media outlets, whether the content of the advice differed strongly from their current behavior, and the simplicity of the advice. All of these heuristics were equally prevalent in our data.

The first technique mentioned for evaluating media advice source trustworthiness was to evaluate the author or media outlet providing the advice: P20 notes that her acceptance of advice, “depends on the author and how the article is written.” P22 says he finds advice useful “If I would quote that source to someone else, like the Washington Post, [or another] reputable media outlet. If it’s just some Matt Drudge on the Internet advising about computer security, I would just ignore that more quickly than I saw it.”

A second evaluation metric was other users’ reviews of the advice. Two security sensitive users, one who holds a M.S. in digital security (P24) and another who handled FERPA data as an HR file clerk (P10), crowd-sourced their advice and software evaluation. P24 comments, “I evaluate YouTube howto videos and other advice channels via user comments.” Similarly, P10 says, “I look at reviews and the software and the website to decide whether to use the advice or download [software]. I look at whether it has a good reputation—whether it is popular with online reviewing.”

A third heuristic for advice evaluation was how widespread across different media outlets the advice became, with the implicit assumption that distribution outlets who reprinted a given

piece of advice had evaluated the sources and information and found it to be valid. P25 comments that he trusts “news that’s backed up by facts and is across multiple channels, because if it’s not good, multiple places won’t pick it up.”

A fourth metric for evaluating a media advice-source trustworthiness was how much the content of the advice differed from the participant’s current behavior: P5 says she took the advice because “it was the opposite of what I was doing, so it automatically made it seem as though it was more credible.” P2 comments that she took the advice since “it made sense; I guess if [my password is] a bit longer, it’s harder for [a malicious] computer to figure it out.”

Finally, a fifth heuristic for media advice-source evaluation is the simplicity of the advice. P2 adds, “If it’s just tips that you can implement in your everyday life, then the advice feels more trustworthy” and P16 wishes that advice “would have a better setup to say ‘Here, this is what you have to do for step one, step two, step three.’ ...like from Google when they’re saying that you can [add] privacy.”

Participants may rely on the trustworthiness of the advice source because they are not confident in their own ability to evaluate the content of the advice. Indeed, P7 says, “physical security is related more to me and my body ... it makes sense to me whereas with computer security, I’m securing myself from threats that I don’t even know anything about...I know when somebody walks up with a gun that I should be worried.” P12 also notes that the tangibility of physical security can make personal safety strategies more trustworthy and easier to implement, commenting, “you know, cyber security is great, but the people who are doing it are so smart that they can put back doors in it that you don’t even know about, so sometimes, I don’t even trust the advice...with physical security, I can touch that, or I know someone that I can relate to.”

That said, participants’ ability to judge the trustworthiness of the advice source may vary. For example, in the case of peer advice, users may not be able to accurately judge the trustworthiness of their peers as an advice source. As an example of good advice, P9 learned to use incognito browsing from a friend, “incognito came out in college and a friend came over and needed to use gmail and just said look at this and logged himself into gmail and didn’t need to log me out and it’s useful.” Similarly, P15 learned about security alarm systems “years ago, from a friend of mine who had a security alarm business.” However, P17 mentioned being told less credible information such as the following: “A lot of my friends don’t have iPhones because, this is the term they use, iPhones are hot. Like they attract all the attention to your phone, like anything you’re doing illegal it can get caught on your phone, ‘cause its like a hot box iPhone. It can be tracked in any type of way, stuff like that. I didn’t even know that, I was like whoaaaaa it can be tracked? If I had known that, I wouldn’t have gotten an iPhone, yeah.”

**physical-security advice.** Consequently, since participants are more confident in their ability to evaluate the plausibility of physical-security advice content, for physical security, the ad-

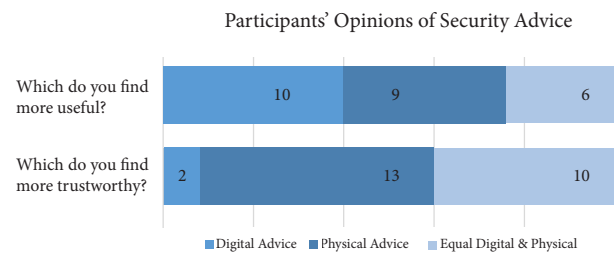


Fig. 3. Participants’ opinions regarding which security advice, digital or physical, is most useful.

vice source is of lesser importance. Only three participants cite the trustworthiness of a physical-advice source as an important metric, and those participants also cited this metric for digital security. Instead, participants rely on their own assessments of the plausibility of and necessity for the physical-security advice to determine whether to implement new physical-security behaviors (N=7). On the subject of plausibility, P22 says about physical-security advice, “if it doesn’t pass the smell test, in other words if it just doesn’t seem plausible, then I dismiss it. If it’s something that I recognize as making sense,” then he will consider implementing it.

#### Digital vs. Physical Advice: Usefulness and Trust.

Figure 3 shows participants’ assessments of the trustworthiness and usefulness of digital- and physical-security advice.

Half of our participants (N=13) felt that physical-security advice was more trustworthy overall than digital-security advice. Only two participants felt that digital-security advice was more trustworthy than physical-security advice. The remaining 10 participants felt that digital- and physical-security advice was equally trustworthy. We suspect that this was largely because, as mentioned above, participants find physical-security advice easier to mentally evaluate (N=7). P9 comments that he would probably trust physical-security advice more than digital-security advice because: “there are a lot fewer variables. I trust it more because it’s easier to evaluate if it’s legitimate.” Similarly, P23 says that she trusts physical-security advice more because it is “more hands on and visual, it’s in your face a little bit more.”

Relatedly, five participants trust physical-security advice more because they feel it is simpler and easier to implement than digital-security advice. “Physical-security advice is more trustworthy because it’s more common sense and they don’t typically require you to download and install something that would be trouble in itself,” comments P20.

Participants are more split on which advice, digital or physical, is more useful. Nine participants feel that physical advice is more useful, primarily for the same reasons they found physical advice more trustworthy: “I can see the relevance in the personal security whereas the computer security, again I am trusting that because I have a little icon on the right that it is doing its job. Do I know what it it’s doing? No.” says P7. Similarly, P3 comments that he finds physical-security advice more useful because: “Again, it’s my understanding. It just



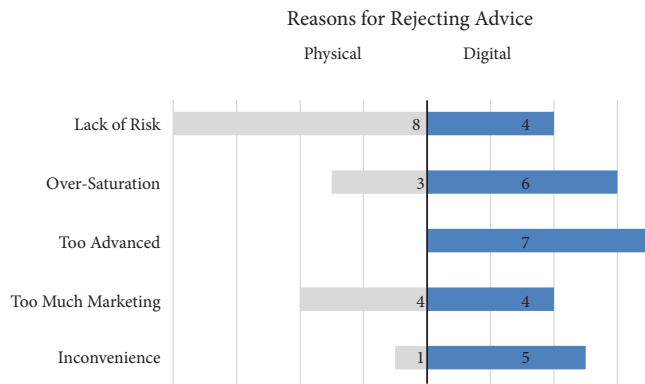


Fig. 4. Distribution of reasons participants rejected digital- and physical-security advice.

comes so much more naturally.”

On the other hand, the 10 participants who feel that digital advice is more useful noted that there are more techniques available for digital than physical security and that they feel a higher risk of digital threats. To the first point, P15 says: “digital-security advice is more useful—because with digital I can probably do more research, and there’s more to do there than the physical. Physical you can only do so much, I don’t care what I have on me, someone can overpower me.” With regard to feeling that there is more digital than physical security risk, P11 comments, “[I] find digital security more useful and more trustworthy because there is so much more research on it and it’s so much more pervasive.”

#### D. Why Advice is Rejected

While trustworthiness and plausibility are the two main reasons users choose to *accept* advice, there are a multitude of reasons for which they reject it. Reliance on others to take care of security needs; digital-security advice that is too marketing-oriented, too inconvenient, or too advanced; over-saturation; and the belief that the user either is not at risk or will be victimized no matter what they do are all common reasons for rejecting advice or stopping security behaviors. Figure 4 summarizes the prevalence of these reasons for rejecting digital- and physical-security advice. Below, we provide further detail on these reasons, and compare and contrast participant’s motivations for rejecting advice in each domain.

**It’s Not My Job.** Eighteen participants rely on the companies whose software, hardware, or services they use to keep them safe. These users do not seem to be making rational cost-benefit calculations about particular personal behaviors being redundant to the services provided by these companies; rather, they simply assume that they are not responsible for the security of a given system because a corporation they trust is taking care of it. For example, P8 comments, “I had been banking with a bank that I wasn’t happy with. Then I went to Bank of America, which was this big bank. I’m like, ‘Oh, they’re awesome so I don’t have to worry about anything. I will be safe.’”

In addition to trusting corporations to take care of security for them, participants also rely on browser and device prompts (N=20), software defaults (N=20) and security requirements imposed by their services (e.g., your password must be 16 characters long) (N=14) to keep them safe. For example, many participants use a password or passcode to lock their phone because the phone prompted them to do so at set-up. P2 says, “When you boot up these phones now, they just give you the option.” Relatedly, P4 says she only has passwords or passcodes on her Mac products because, “the Mac products prompt you to set up the security things...I never thought about it [for the Kindle]. I guess it wasn’t prompted...I would have to look up, how to do it on the Kindle.” In addition to prompts, users rely on software defaults, such as those in anti-virus software, to provide security tactics: P17 comments, that she has a script and popup blocker because it “was through McAfee and it was automatic. ...I’m not really technical savvy where I can block stuff and...go into my settings and know what I’m messing with.”

**This Is Too Inconvenient.** Inconvenience is often cited as a possible explanation for users rejecting digital-security advice [5], [6], [50], but it was not the most prevalent reason we discovered. The inconvenience of implementing advice was cited by six participants, five of whom mentioned it in the context of digital security. P20 says she does not change the passwords on her accounts, because “from a convenience standpoint, it’s just easier to keep them as they are and not risk being locked out.” Relatedly, P23 says she “took the password off the wireless because we [her family] were forgetting it.” In another example, P9 comments that a security strategy he has considered, and thinks would be useful, is encryption. However, “I haven’t *really* thought about it...maybe I should...it seems like it would make everything infinitely harder to break into and only 10% harder for me to deal with, but it just hasn’t been worth the trouble.” Thus, even minor inconvenience may deter users from implementing a new security behavior.

**Too Much Marketing.** Eight participants rejected digital- and physical-security advice because it appears to be more about selling a product than about providing advice: “I don’t do anything with a price tag attached. I could be persuaded to do it if I had a serious problem. I did have my identity stolen one time but I was able to fix it, but I’m not one of these people who signs up for LifeLock or something like that,” says P22. Similarly, P16 wishes that physical-security advice could be more substantive, “instead of just on an ad, because they change ads every day.”

**This Advice is Too Advanced.** Some participants find the digital-security advice they see too advanced (N=7). Four of the participants who reported this were highly educated (they held an M.S. or above). P9 holds a computer engineering degree, but says, “I know just enough to not be useful about various levels of security on website and HTTPS and SSL and I don’t even know what the acronyms mean, but I know that some websites are more secure and others aren’t,

and I don't pay attention to it." P8, who holds a masters degree, also struggles to understand too-complex advice: she sometimes rejects advice, "Depending on the number of steps and the complexity of it because I'm not a IT person ... it can be complex what they're asking me to do." Similarly, P13 comments, "I've heard when you transfer files, you can encrypt, but I don't know how, but one of my colleagues did do that when he sent out files, but I don't because of lack of knowledge and skill." An additional three participants chose not to practice a particular digital-security behavior because they did not understand how to do so: "I'm still trying to figure out how in the world do I use that [antivirus software] because they never explained it to me," says P16.

**I'm Over-saturated.** Participants may also reject advice not because the behavior proposed is inconvenient in itself, but because they cannot bear the thought of needing to use one more security behavior. Nine participants stated that they felt over-saturated and lacked the time to implement the advice they see, even if they think it is good advice. P7 says: "Part of it is just saturation. You get so much information from so many sources. I don't even know sometimes what's worth looking at." P23 intends to implement the advice but has not gotten around to it yet: "[I've] heard about things that will protect your information, I don't remember the names of them. Haven't gotten around to it yet, but I will in the near future." P6 thinks that two-factor authentication is a good idea but hasn't yet implemented it on all of his services. "I just don't think about it day to day. Every time I run across it, I'm like, 'Yeah, that's a good idea,' but then it just falls right out of my head," he says. Additionally, P6 notes that in general that he often does not take security advice because he has "kind of reached a level of don't care. It's so obvious to me that I don't know what I don't know, that it's frustrating to try to tease apart what would be helpful and what wouldn't."

**I'm Not At Risk.** Eight participants rejected physical-security advice as unnecessary due to their low risk profile. For example, P24 says: "[I've] heard about 24-7 monitoring and crap like that, I think it's overkill. If everyone [in my neighborhood] was driving fancy cars, maybe."

Four participants rejected digital-security advice for the same reason. P5 says he does not put a password on his phone because, "I just don't feel I have that much interesting stuff on there." P10 comments that she does not use or look for security tactics for her tablet, because "there's nothing personal on the tablet." Similarly, P3 does not take security advice for browsing because she is "not so concerned about browsing as opposed to personal financial information." Surprisingly, the participants who cited these feelings for digital security were of varied incomes, and the overall incidence of feelings of "unimportance" around digital security was quite low. This is in contrast to prior work, which had proposed that many users, particularly those with lower incomes, might not execute security behaviors due to low valuation of their data [4]. One possible cause for this change is that as technology becomes more ubiquitous, users are becoming more aware of the value

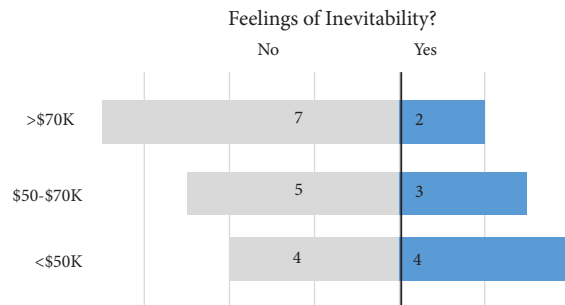


Fig. 5. Lower income participants are more likely to feel that it is inevitable they will become the victim of a digital security threat.

of their data.

**No Matter What, I Will Get Hacked.**

Participants may also reject digital-security advice because they feel that no matter what they do, they will still become victims. Interestingly, seven out of nine participants with incomes above \$70,000 do not feel this sense of inevitability, while only four out of eight participants with incomes below \$50,000 do not cite these feelings. "I feel like there is a level of inevitability. I feel like you're lucky if nothing ever happens. You can take all of the steps and people will find ways. We can clearly see around pretty much anything. If you don't fall into that by chance then you're lucky. I feel like if you do everything you're supposed to do, like in life, something can still happen," says P6, who lives in a household that earned between \$30,000 and \$50,000 in 2014. Figure 5 shows these results. This difference in feelings may also be related to a difference in these participants' levels of security sensitivity, which we discuss below in Section IV-E. Only three participants cited similar feelings of inevitability in the domain of physical security. These three participants were all women, and it is probable that their feelings of inevitability may stem from gender-based crime rate differences and socialization to be more fearful due to their gender [49].

**Other reasons for rejecting advice.** A few participants described reasoning that was less common but still interesting, with possible implications for design. One participant (P3) noted that he rejects advice because he see it in the wrong venue: "I see the information while on [public transit] to work and then by the end of the day, looking at a computer is the last thing I want to do." We hypothesize that this factor may be important for many users, even though no other participants explicitly mentioned it; we discuss it further in the context of design recommendations in Section V.

Additionally, some participants reported rejecting what they perceived as good advice for others because they were already confident in their own behaviors (N=3). P25 notes that having others tell him how to be digitally secure is pointless, because: "I do what I do based on my own personal feelings and intellect, so I don't find it useful, but for someone who didn't know it would be useful. Never found any of the advice useful. I just have my own way of protecting what I do, so it's like

if someone’s telling you how to make a PB&J sandwich, and I’m like I know how to do it. But if they’re saying something drastic—don’t do this, this, and this—then I’ll look at it, but usually, no.”

**Reasons for Rejecting Digital vs. Physical Security.** Many reasons for rejecting advice were common to the digital and physical domains. However, a few reasons were unique to digital security: advice that is too advanced, over-saturation, and the assumption that a corporation who provides services to the user will protect them. Feelings of inevitability were more prevalent for digital security (N=8 digital, N=3 physical) than for physical security. Inversely, feelings that risk was low and therefore implementing a new behavior was unnecessary were more common for physical than digital security. These differences imply that the digital-security community has much to learn from the physical security domain about effective security education.

*E. Security-Sensitive vs. General Users*

In addition to differences between users’ behavior in the physical- and digital-security domains, there are also differences between *users* who are or are not security-sensitive. We recruited security-sensitive users to investigate whether extra training in handling confidential or sensitive data at work would affect how participants process security advice in their personal lives. Below, we address security-sensitive users’ differences from general users in the domain of digital security: they are more likely to evaluate advice based on the trustworthiness of the advice source; they are *less* likely to use two-factor authentication than general users; they feel that digital-security advice is more useful than physical; the majority take security advice from their workplace; and they may express fewer feelings of inevitability than do general users. The prevalence of these differences is summarized in Figure 6. Additionally, we examine whether security-sensitive users have better security behavior intentions than do general users.

**Security-Sensitive Participants are Even More Likely to Evaluate Advice Based on Their Trust of the Source.**

Nine of 15 security-sensitive participants cited the trustworthiness of the advice source as their key metric for choosing to take digital-security advice, compared to only two of 10 general users. We suspect that security-sensitive users may be more discerning about advice because they have been trained to look critically at the digital information they come across. A primary component of workplace digital-security training is reminders not to trust unknown individuals [51], [52]. This emphasis on judging sources of information critically may translate over to security-sensitive users’ home environments from these trainings, making them more skeptical of advice provided by sources they do not trust.

**Security-Sensitive Users are Less Likely to Use Two-Factor Authentication.**

Seven of 15 security-sensitive users had adopted 2FA, compared to eight of 10 general users. We hypothesize that security-sensitive users are less trusting that the

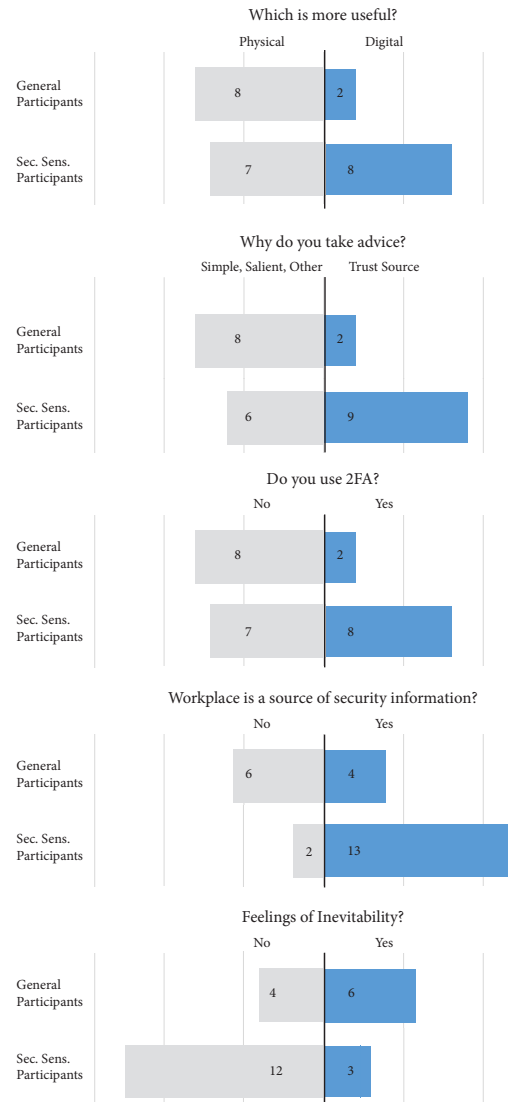


Fig. 6. Security sensitive users differ from general users in their valuation of digital-security advice, their reasons for taking advice, their use of two-factor authentication, and some of their advice sources.

service requesting 2FA can protect the personal information they are providing, as four of the security-sensitive users cite privacy concerns as a reason for not using 2FA. User’s motivations for accepting and rejecting two-factor authentication are discussed in more detail in Section IV-F.

**Security-Sensitive Users Feel Digital Advice is More Useful than Physical Advice.**

Eight of 15 security-sensitive users believe digital-security advice is more useful, compared to two of 10 general users. We speculate this may be related to these users being more frequently reminded to pay attention to digital security and data sensitivity.

**Most Security-Sensitive Participants Took Digital-Security Advice from Their Workplace.**

Thirteen out of 15 security sensitive users took advice from their workplace, contrasted with four of 10 regular users. This is unsurprising given the

workplace emphasis on digital-security and regular trainings that occur for security-sensitive users. Additionally, security-sensitive users may be more likely to take advice from IT professionals. Eight of 15 security sensitive users took digital-security advice from IT professionals, compared to four out of 10 general users. This trend is not as differentiable as the other trends detailed in this section, and thus will require more investigation in future research.

We suspected this reliance on workplace and IT professionals for security information would correspond to a relative decrease in reliance on other advice sources. Surprisingly, however, security-sensitive and general users cited family, peers, media, and negative experiences at similar rates.

**Security Sensitivity and Feelings of Inevitability.** As mentioned in Section IV-D, we found that participants with lower incomes expressed more feelings of inevitable victimization in digital security than did higher-income participants. We also found that general users expressed more feelings of inevitability than did security-sensitive users. Six out of 10 general users expressed these feelings, contrasted with three out of 15 security sensitive users. However, in our sample security-sensitive users also tended to have higher incomes than general users. Thus, it is unclear whether the correlate in the case of inevitability feelings is income, security-sensitivity, or a combination of both.

**Security-Sensitive Users and Security Behavior.** We used the SEBIS scale, as described in Section IV-B, to compare behavioral intentions of security-sensitive participants to those of general participants. Security-sensitive users scored an average of 3.3 (S.D.=0.6), while general users scored a slightly lower average of 2.8 (S.D.=0.4). Given our small sample size, it is difficult to assess whether this difference is meaningful; further exploration is needed in this area.

#### *F. Case Study: Two-factor Authentication*

As mentioned in Section II-B, Ion et al. report that use of two-factor authentication (2FA) is one of the top three security behaviors recommended by or used by security experts. However, only 40% of the non-expert users in that study reported using 2FA. Our results shed some light on the reasoning behind users' acceptance or rejection of this behavior.

**How and Why I Use Two-Factor Authentication.** Of the participants we interviewed, more than half reported using 2FA (N=14). In our interview questions about 2FA, we started by defining 2FA as "a service where you might put in your phone number and then be sent a verification code." Given this definition, all participants recognized 2FA and were able to substantively answer our interview questions on this topic. We hypothesize that providing this more detailed definition may account for the difference in the proportion of our respondents (50%) and the proportion of respondents in the work of Ion et al. (40%) who reported using 2FA. Of our 14 participants who had used 2FA, five used 2FA for some, but not all services. These participants use 2FA for those services they feel are particularly important: P6 says, "I've got 2FA on one thing,

and that is my insurance company. I did that because [of a negative experience at my workplace.] I figured that [my insurance] was one of the most important things, because...it covers every aspect in my life. I didn't want anyone to mess with that."

Alternately, users may only use 2FA on services that strongly encourage or force them to do so: "I do that with Xbox Live, they force me to do that. I think Google, they want me to do that but I always say later," comments P12.<sup>1</sup> Similarly, P14 says: "Yes, at one time Verizon, because I have a Verizon email account, it asked me to do [2FA], it takes a while but I've done it...it forced me to do it." Of the remaining nine participants who used 2FA, two did not understand what they were doing: P16 comments, "You mean when it asks to use by text or phone call? I do that, even though I hate doing it, because I'm trying to figure out what is the purpose, but it says the purpose is your safety and security."

**Why I Don't Use Two-Factor Authentication.** Eleven participants knew about but chose not to use 2FA. Five of these participants declined 2FA due to privacy concerns: specifically, they worried about giving out their personal phone number, about GPS tracking based on that phone number, and about the service providing 2FA's ability to keep their information secure. For example, P13 says: "No, [I want] nothing connected to the phone. So, the phone is directly connected to the email. I don't feel comfortable to let people in if it's connected to the email account." With regard to Google's ability to protect the information used for verification, P3 says: "I think I do have that [2FA] capacity. I think I've always declined Gmail enabling that access...Based on what I know about Gmail, it just seemed like giving up too much information to Google." Similarly, P23 says: "Google has prompted but I've always ignored it because I think that someone will get ahold of it, I'm not saying they would, but I'm just always like, you know, yeah."

In addition to privacy concerns, two participants declined to use 2FA due to convenience concerns: "Two years ago, at the beginning of the summer, Google introduced 2FA, and this was an issue because I tried to log in and I didn't get cell service and I couldn't get the text message to log in, and that was the last time I tried to change anything," says P9. And two participants declined the service due to lack of understanding.

## V. DESIGN GUIDELINES

It is important to minimize digital-security advice so that users do not feel overwhelmed. As mentioned in results, several users felt over-saturated with advice and further, felt that they lacked the time to implement all the advice they were given. This is consistent with the compliance-budget model [6]. Given that we found that many users struggle to evaluate the plausibility and usefulness of digital-security advice, reducing the amount of advice they need to process will significantly reduce their cognitive load. This of course

<sup>1</sup>Note that XBox Live does not require two-factor authentication, but this participant may have misinterpreted the prompt screen as a requirement.

requires identifying a small set of recommendations that provide high value to users; Ion et al. have made progress in this direction [7]. While the amount of advice provided should be strictly limited, our findings suggest that critical advice can be made more effective in several ways. Design recommendations for achieving this efficacy and distributing advice to users are detailed below.

**Signal Credibility.** Our participants reported relying on the credibility of sources to evaluate digital-security advice, but sometimes struggling to assess this credibility. Drawing on the heuristics our participants report using, we recommend designing digital-security advice that clearly states the author’s qualifications in digital security. Because some participants used user reviews to evaluate advice, a system to request and promote high-quality user rankings might also provide evidence of credibility.

Further, we found that users reject security advice that contains marketing material; therefore, advice that suggests or encourages purchasing a particular product or service (especially if associated with the advice source) reduces credibility and should therefore be avoided.

**Address Privacy.** Our case study of two-factor authentication suggests that users may reject security advice if they feel it threatens their privacy. Both 2FA and password managers appear in the top six expert-recommended digital security behaviors [7]; our results suggest that privacy concerns and mis-understandings are at least partially driving low adoption of each technique. For example, with regard to password managers, P7 notes that she does not like “the notion of a machine memorizing my password, I don’t know where it’s going, I don’t know who has it and I don’t know what is happening with it.” We hypothesize that users may be prioritizing the immediate risk of sharing private information (e.g. phone number) over the long-term risk of compromising the service (e.g. email) for which they are considering 2FA. This is an example of present bias, our tendency to prioritize immediate rewards or concerns over long-term gains [53].

Thus, our second recommendation for designing advice is to clearly explain to users (and not just in a privacy policy that no users will read) how their personal data, such as a phone number for 2FA or passwords for a password manager, will be protected. Mitigating these privacy concerns could provide high-impact benefits for users.

**Simplify and Explain.** More than half of our participants felt that physical-security advice was more trustworthy, or more useful, than digital-security advice, in part due to the simplicity and actionability of physical-security advice. Consequently, we suggest that it is key to ensure digital-security advice is straightforward, contains step-by-step instructions, and avoids technical jargon while clearly explaining why the technique recommended is necessary to keep users secure.

**Distribute Advice Via Pre-existing Channels.** Somewhat surprisingly, we found that many participants trust hardware and software companies to keep them secure without ad-

ditional intervention; other participants valued direct advice from those companies. It seems, therefore, that corporations such as Google, Apple, and Comcast are well positioned to make a large impact on users’ digital security, as already-trusted sources of perceived credible advice. As mentioned above, however, it is crucial for these corporations to be easily recognizable as the source of advice and to avoid the perception of marketing.

We also found that participants rely on IT professionals, particularly those from their workplaces, as a source of credible digital-security advice even for personal technology. We believe these individuals, too, could make a significant positive impact on users’ security behavior, if they can be trained to distribute a small set of valuable advice.

Additionally, as shown both in our results and in Rader et al.’s work, negative events experienced by users or their friends can be key motivators for security behavior change [2]. We find that mimicking these negative events via visual media can also be very effective. As a result, we suggest developing movies or TV shows that demonstrate negative digital-security events via realistic, relatable characters. Since we found that users did *not* learn from negative experiences in which they could not clearly see the cause of the event and how to prevent it, it is also important to make clear in this visual-media advice what users could do to prevent the negative event shown.

## VI. SUMMARY

Users must sift through a multitude of security advice to determine which security behaviors to implement and which to reject. This process of deciding to implement security tactics based on the advice of others is multi-faceted and complex. In an effort to understand users’ choices, we conducted a semi-structured interview study of 25 participants with varied demographics and security sensitivities. We asked questions about users’ security behaviors, how they learned these behaviors, and why they accepted or rejected different behaviors and pieces of advice. Our analysis of these interviews resulted in three key findings.

First, our findings suggest a few notable differences between security-sensitive and general users: they consider digital-security advice more useful than physical advice in their day-to-day lives and they rely heavily on their workplace as a source of digital-security advice.

Second, we found that users reject security advice for a number of somewhat surprising reasons, including containing too much marketing information and threatening users’ sense of privacy. Further, a majority of participants believed that someone or something else was responsible for their security in at least one digital domain (e.g., online banking).

Third, and perhaps most importantly, our findings indicate that users believe they lack the skills to evaluate the content of digital-security advice and must instead rely on their evaluation of the trustworthiness of the advice *source* when determining whether to accept the advice. Sources they trust include their workplace, providers of their digital services, IT professionals, family members, and friends. Our participants

also relied upon media as a source of advice, but only if it passed an heuristic credibility test. Finally, the majority of participants reported changing their security behavior based on negative events. These events took the form of personal experiences, stories told by family and friends, or vignettes in TV shows or movies. Thus, by signaling credibility and relying on pre-existing trusted channels, security experts may be able to amplify the most important advice, helping users to spend their security-compliance budget wisely.

#### ACKNOWLEDGMENT

Our thanks to Yla Tausczik, Bethany Tiernan, and Bruce Webster, Jr. for their input and assistance. This material is based upon work supported by the Maryland Procurement Office under contract no. H98230-14-C-0137.

#### REFERENCES

- [1] S. Das, T. H. Kim, L. Dabbish, and J. Hong, "The effect of social influence on security sensitivity," in *Tenth Symposium on Usable Privacy and Security*. USENIX Association, 2014. [Online]. Available: <https://www.usenix.org/conference/soups2014/proceedings/presentation/das>
- [2] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," in *Eighth Symposium on Usable Privacy and Security*. ACM, 2012. [Online]. Available: <http://doi.acm.org/10.1145/2335356.2335364>
- [3] L. Rainie, S. Kiesler, R. Kang, and M. Madden, "Anonymity, privacy and security online," *Pew Research Center*, 2013. [Online]. Available: <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
- [4] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The psychology of security for the home computer user," in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2012. [Online]. Available: <http://dblp.uni-trier.de/db/conf/sp/sp2012.html#HoweRRUB12>
- [5] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in *New Security Paradigms Workshop*. ACM, 2009. [Online]. Available: <http://doi.acm.org/10.1145/1719030.1719050>
- [6] A. Beauteament, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *2008 workshop on New security paradigms*. ACM, 2009. [Online]. Available: <http://portal.acm.org/citation.cfm?id=1595676.1595684&coll=DL&dl=ACM&CFID=595658384&CFTOKEN=19488999>
- [7] I. Ion, R. Reeder, and S. Consolvo, "'...no one can hack my mind': Comparing expert and non-expert security practices," in *Eleventh Symposium On Usable Privacy and Security*. USENIX Association, 2015. [Online]. Available: <https://www.usenix.org/conference/soups2015/proceedings/presentation/ion>
- [8] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong, "Increasing security sensitivity with social proof: A large-scale experimental confirmation," in *SIGSAC Conference on Computer and Communications Security*. ACM, 2014. [Online]. Available: <http://doi.acm.org/10.1145/2660267.2660271>
- [9] R. Wash, "Folk models of home computer security," in *Sixth Symposium on Usable Privacy and Security*. ACM, 2010. [Online]. Available: [http://cups.cs.cmu.edu/soups/2010/proceedings/a11\\_Walsh.pdf](http://cups.cs.cmu.edu/soups/2010/proceedings/a11_Walsh.pdf)
- [10] C. Herley, "More is not the answer," *IEEE Security and Privacy magazine*, 2014. [Online]. Available: <http://research.microsoft.com/apps/pubs/default.aspx?id=208503>
- [11] R. Wash and E. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users," in *Eleventh Symposium On Usable Privacy and Security*. USENIX Association, 2015. [Online]. Available: <https://www.usenix.org/conference/soups2015/proceedings/presentation/wash>
- [12] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in *22nd International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2013. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2487788.2488034>
- [13] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," in *SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010. [Online]. Available: <http://doi.acm.org/10.1145/1753326.1753383>
- [14] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behavior intentions scale (sebis)," in *33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015. [Online]. Available: <http://doi.acm.org/10.1145/2702123.2702249>
- [15] "Microsoft safety and security center." [Online]. Available: <http://www.microsoft.com/security/default.aspx>
- [16] "Us-cert:tips." [Online]. Available: <https://www.us-cert.gov/ncas/tips>
- [17] "Mcafee security advice center." [Online]. Available: <http://home.mcafee.com/advicecenter/>
- [18] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish," in *Third Symposium on Usable Privacy and Security*. ACM, 2007. [Online]. Available: <http://doi.acm.org/10.1145/1280680.1280692>
- [19] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," *Comput. Hum. Behav.*, vol. 29, pp. 706–714, 2013. [Online]. Available: <http://dx.doi.org/10.1016/j.chb.2012.12.018>
- [20] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, pp. 7:1–7:31, June 2010. [Online]. Available: <http://doi.acm.org/10.1145/1754393.1754396>
- [21] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: An empirical study of the effectiveness of web browser phishing warnings," in *SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008. [Online]. Available: <http://doi.acm.org/10.1145/1357054.1357219>
- [22] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *22nd USENIX Conference on Security*. Berkeley, CA, USA: USENIX Association, 2013. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2534766.2534789>
- [23] J. Sunshine, S. Egelman, H. Almuhammedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of ssl warning effectiveness," in *18th Conference on USENIX Security Symposium*. USENIX Association, 2009. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1855768.1855793>
- [24] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2006. [Online]. Available: <http://doi.acm.org/10.1145/1124772.1124863>
- [25] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The Emperor's New Security Indicators," *IEEE Symposium on Security and Privacy*, pp. 51–65, 2007. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1264196>
- [26] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your attention please: Designing security-decision uis to make genuine risks harder to ignore," in *Ninth Symposium on Usable Privacy and Security*. ACM, 2013. [Online]. Available: <http://doi.acm.org/10.1145/2501604.2501610>
- [27] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "How does your password measure up? the effect of strength meters on password creation," in *21st USENIX conference on Security symposium*. USENIX Association, 2012. [Online]. Available: <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final209.pdf>
- [28] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven?: the impact of password meters on password selection," in *SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2470654.2481329&coll=DL&dl=ACM&CFID=543110690&CFTOKEN=49806099>
- [29] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Eighth Symposium on Usable Privacy and Security*. ACM, 2012. [Online]. Available: [http://cups.cs.cmu.edu/soups/2012/proceedings/a3\\_Felt.pdf](http://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf)
- [30] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *SIGCHI Conference on Human*

- Factors in Computing Systems*. ACM, 2013. [Online]. Available: <http://patrickgagekelley.com/papers/android-decision.pdf>
- [31] K. Charmaz, *Constructing grounded theory : a practical guide through qualitative analysis*. London; Thousand Oaks, Calif.: Sage Publications, 2006. [Online]. Available: <http://www.amazon.com/Constructing-Grounded-Theory-Qualitative-Introducing/dp/0761973532>
- [32] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough?: An experiment with data saturation and variability," *Field Methods*, vol. 18, pp. 59–82, 2006.
- [33] M. C. Harrell and M. A. Bradley, "Data collection methods. Semi-structured interviews and focus groups," DTIC Document, Tech. Rep., 2009. [Online]. Available: [http://www.rand.org/content/dam/rand/pubs/technical\\_reports/2009/RAND\\_TR718.pdf](http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf)
- [34] A. Strauss and J. Corbin, *Basics of qualitative research: Procedures and techniques for developing grounded theory*, 1998.
- [35] D. G. Freelon, "Recal: Intercoder reliability calculation as a web service," *International Journal of Internet Science*, vol. 5, no. 1, pp. 20–33, 2010.
- [36] M. Lombard, J. Snyder-Duch, and C. C. Bracken, "Content Analysis in Mass Communication: Assessment and Reporting of Intercoder Reliability," *Human Communication Research*, vol. 28, pp. 587–604, 2002. [Online]. Available: <http://dx.doi.org/10.1111/j.1468-2958.2002.tb00826.x>
- [37] A. L. Holbrook, M. C. Green, and J. A. Krosnick, "Telephone versus Face-to-Face Interviewing of National Probability Samples with Long Questionnaires: Comparisons of Respondent Satisficing and Social Desirability Response Bias," *Public Opinion Quarterly*, vol. 67, pp. 79–125, 2003. [Online]. Available: <http://poq.oxfordjournals.org/cgi/citmgr?gca=pubopq;67/1/79>
- [38] R. Tourangeau and T. Yan, "Sensitive Questions in Surveys." *Psychological Bulletin*, vol. 133, no. 5, p. 25, 2007.
- [39] "State and county quickfacts," 2015. [Online]. Available: <http://quickfacts.census.gov/qfd/states/00000.html>
- [40] "American community survey 1-year 2013 census," 2013. [Online]. Available: <https://www.census.gov/acs/www/data/data-tables-and-tools/index.php>
- [41] "Household income in the past 12 months: 2009-2013 american community survey 5-year estimates," 2013.
- [42] "Cnet." [Online]. Available: <http://www.cnet.com>
- [43] "Wired." [Online]. Available: <http://www.wired.com>
- [44] "Schneider on security." [Online]. Available: <https://www.schneider.com>
- [45] "Mashable." [Online]. Available: <http://mashable.com>
- [46] "Last week tonight with john oliver: Edward snowden on passwords." [Online]. Available: <https://www.youtube.com/watch?v=yzGzB-yYKcc>
- [47] A. Fisher and J. Margolis, "Unlocking the clubhouse: The carnegie mellon experience," *SIGCSE Bull.*, vol. 34, pp. 79–83, Jun. 2002. [Online]. Available: <http://doi.acm.org/10.1145/543812.543836>
- [48] L. O. Campbell, M. Kepple, and C. Herlihy, "Women in technology: an underrepresented population," in *Global Learn 2015*. AACE, 2015. [Online]. Available: <http://www.edlib.org/p/150902>
- [49] D. C. May, N. E. Rader, and S. Goodrum, "A gendered assessment of the 'threat of victimization': Examining gender differences in fear of crime, perceived risk, avoidance, and defensive behaviors," *Criminal Justice Review*, vol. 35, no. 2, pp. 159–182, 2010. [Online]. Available: <http://cjr.sagepub.com/content/35/2/159.abstract>
- [50] J. B. Hardee, R. West, and C. B. Mayhorn, "To download or not to download: An examination of computer security decision making," *interactions*, vol. 13, pp. 32–37, May 2006. [Online]. Available: <http://doi.acm.org/10.1145/1125864.1125887>
- [51] "The department of health and human services information systems security awareness training." [Online]. Available: <http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/issa.pdf>
- [52] "Federal communications commission cyber security planning guide." [Online]. Available: <https://transition.fcc.gov/cyber/cyberplanner.pdf>
- [53] D. Laibson, "Golden eggs and hyperbolic discounting," *Quarterly Journal of Economics*, vol. 112, pp. 443–477, 1997.

## VII. APPENDIX

### A. Questions

#### Employment

- Could you tell me a little bit about what you do?

- Do you handle sensitive or private data as part of your job?

- Could you tell me a little bit more about that data?

#### Digital Security

##### Device Protection

- How many devices do you use to access the internet for personal use?
  - Do you have a smartphone? Tablet? Multiple computers?
  - What type or brand of smartphone or computer (e.g. Windows/Mac/Linux) do you use?
- Can you show me how you access your devices?
  - When was the last time you changed this password?
- Are there any other tactics you use to protect your devices?
- Do you use antivirus software?
  - How often do you run the software?
  - Did you install it or did it come with your computer?
  - Why do you use it?
- Why do you use these strategies for protecting your [phone/computer/devices]? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?
  - Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- Is there a password on your wireless internet at home?
  - Did you set up this password?
  - When was the last time you changed this password?
  - Were you prompted to do so?
- Is there a password on your router?
- Are there any other tactics you use to protect your wireless internet?
- Why do you use these strategies for protecting your wireless internet? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?

- Are there ever times when you do not choose to use this strategy?
- Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- How secure do you feel your devices and your wireless internet are?

### Internet Activities

#### Browsing and Emailing

- Do you browse the internet?
- Do you access your email via a web browser (e.g. Safari/Firefox/Chrome/Internet Explorer)?
- Do you shop online or bank online?
- Do you do all of these activities on all of your devices?
- Scenario: Let's imagine that you have a family member (parent/spouse/sibling/child) with whom you share a computer. You are searching for a surprise birthday gift, lets say a necklace, for this person, and you are using the internet to research potential gifts. Can you show me what you would do to start this project?
- In general, how do you stay secure when browsing the internet or checking your email?
  - When was the last time you changed your email password?
    - \* Were you prompted to do so?
  - Do you use two-factor authentication?
    - \* Two-factor authentication is a service where you might put in your phone number and then be sent a verification code.
  - Do you use the privacy settings when browsing?
  - Do you ever use incognito browsing or private browsing?
  - Do you use a script, popup, or cookie blocker?
  - How do you treat emails from unknown individuals?
  - Are there any particular precautions you take when downloading from the internet?
- Are there any other tactics you use when browsing the internet/accessing your email via the internet?
- Why do you use these strategies for staying secure while browsing the internet or accessing your email? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?
  - Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?

- How secure do you feel you are when browsing the internet and accessing your email?

#### Online Shopping/Banking

- Narration: Can you please walk me through what you would do to login to your banking website? Now please pretend you are exiting the website as if you had just completed your banking business.
- How often do you change your password for online banking or shopping accounts?
- Are there any other tactics you use when shopping online or doing online banking?
  - Do you always use the same credit card?
  - Do you use paypal?
  - Do you use a single use credit card number?
- Why do you use these strategies for staying secure while online shopping or online banking? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?
  - Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- How secure do you feel you are when online shopping and online banking?

#### General Advice

- Do you store your passwords anywhere?
  - Where do you store them?
  - In what format do you store them?
  - Is it password protected or locked?
  - Why did you start doing this?
  - When did you start doing this?
- Do you ever look for new information or talk to someone about tactics such as [what they mention above for security]?
  - Where do you look for this information and with whom do you talk?
- Do you often see news pieces, ads, or articles on TV, in the newspaper, or online with tips or advice about how to protect yourself online?
  - How do you feel about the information provided?
  - Are there strategies you have learned from these sources?
- What other sources do you consult when seeking security advice?
- Do you see any security advice that you do not take?



- Why do you not take it?
- Do you feel that you have the ability to make yourself more digitally secure?
- Whom or what would you say has most influenced your overall approach to computer security, and in what way?

## Physical Security

### *Dwelling Security*

- Do you live in a house or an apartment?
  - Do you own your dwelling?
  - Do you live alone, with a partner, family, or with roommates?
- Can you walk me through what you do as you leave your dwelling?
  - Are there one or two locks?
  - Is it a hard lock or an electronic lock?
  - Is that something that came with the building or something you installed?
    - \* Why did you install the locks?
- Can you walk me through what you do when you prepare to go to bed in the evening and when you return from your day of work?
- Are there any other strategies, which you have not mentioned, that you use to secure your dwelling?
  - Light timers?
  - Security system?
  - Security system or guard dog signs?
- Is there anything that led you to buy or rent in the location you did?
- Why do you use these strategies for securing your dwelling? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?
  - Is this strategy something that is important to you, or something you feel is more important to other members of your household who share the dwelling?
  - Why would you say that it is more important to [you/other]?
  - Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- How secure do you feel that you are when you are at home?
- How secure do you feel that your belongings are when you are not home?

### *Transit Security*

#### Car (if applicable)

- What is your primary method of transportation?
- Do you own or lease your car?
- Where is it typically parked?
- Can you walk me through what you do when you get out of your car, once it is parked?
  - What do you do if you have to store items in the car?
- Are there any other strategies, which you have not mentioned, that you use to protect your vehicle?
- Why do you use these strategies for protecting your vehicle? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?
  - Is this strategy something that is important to you, or something you feel is more important to people with whom you share the car (if applicable)?
  - Why would you say that it is more important to [you/other]?
  - Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- How secure do you feel that your car is when it is parked?
- How secure do you feel the belongings you have in your car are, when the car is parked?

#### Bicycle (if applicable)

- Do you own or rent or bikeshare your bicycle?
- Where is it typically stored?
- Can you walk me through what you do when you get off your bicycle once it is parked somewhere?
  - What type of lock do you use?
  - To what object do you lock the bike?
  - Where do you affix the lock?
- Are there any other strategies, which you have not mentioned, that you use to protect your bike?
- Why do you use these strategies for securing your bike? *For each strategy, ask:*
  - When did you start using this strategy?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?

- Is this strategy something that is important to you, or something you feel is more important to people with whom you share the bike?
  - \* Why would you say that it is more important to [you/other]?
- Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- How secure do you feel that your bike is when it is unattended?

#### Personal Security (walking)

- Where do you tend to walk?
  - Do you walk more than 10 minutes a day?
- Are there any particular approaches you take, or items you carry, when walking alone?
- Have you had any martial arts/self defense training?
  - Why did you undergo this training? Who administered the training?
- Why do you use these strategies? *For each strategy, ask:*
  - When did you start using this strategy?
  - How do you feel that this strategy works to protect you?
  - Why did you choose to use this strategy over using a different one?
  - What are you most worried about?
  - Have you ever had a negative experience?
  - Do you know anyone who has had a negative experience?
  - Are there ever times when you do not choose to use this strategy?
  - Where or from whom did you learn this strategy?
- Are there strategies you have considered or heard about but do not use?
- How secure do you feel you are when walking?

#### General Advice

- Do you ever look for new information or talk to someone about tactics such as for protection your [dwelling, vehicle/bike, self, other members of your family]?
  - Where do you look for this information and with whom do you talk?
- Do you often see news pieces, ads, or articles on TV, in the newspaper, or online with tips/advice, social media posts, chain emails on how to protect your [dwelling, vehicle/bike, self, other members of your family]?
  - How do you feel about the information provided?
  - Are there strategies you have considered or heard about but do not use?
- What other sources do you consult when seeking physical security advice?
- Do you feel that you have the ability to make yourself more physically secure?
- Whom or what would you say has most influenced your overall approach to physical security, and in what way?