How I Learned To Be Secure: Advice Sources and Personality Factors in Cybersecurity

Elissa Redmiles
University of Maryland
eredmiles@cs.umd.edu

Amelia Malone
University of Maryland
amalone2@terpmail.umd.edu

Michelle L. Mazurek
University of Maryland
mmazurek@cs.umd.edu

1. INTRODUCTION

As of 2013, 21% of online adults have had an email or social media account hijacked, 11% have had vital information stolen, and between 2013 and 2014, there was a 48% increase in the number of cybersecurity incidents [1,2]. Given the high, and increasing, potential that users will encounter cybersecurity threats, it is important to understand how users learn security behaviors in order to promote good security tactics and discourage ineffective ones. However, if the average American listened to all of the security advice they encountered, they would never leave their house, or use the Internet again. Thus, to better construct instructional material (advice) on security, we must first understand what advice users are seeing, as well as which of this advice they choose to utilize and why.

In this paper, we investigate advice sources for those security behaviors that users repeatedly and consistently practice, what or whom users consult when seeking new security information, and what or who most strongly influences users' overall approach to cybersecurity. We consider how demographics, personality, and prior experiences affect users' security behaviors and the sources from which they seek out security advice. We also consider whether users who have additional security-sensitivity – those who handle confidential records, or hold security clearances – process advice differently than less-sensitive users.

Previous research related to users' security behaviors has primarily focused on identifying these behaviors and experimenting with how to change them [3,4,5]. Other work has focused on the important influence of social factors on security behavior [3,5].

We wish to ask a broader set of questions examining how many factors impact security behaviors: What security advice do users see, where or from whom does this advice originate, what advice do they take, and why do they take it? (Q1); How does the security domain (cybersecurity vs. physical security) affect which security-advice sources they utilize and what advice they adopt? (Q2); How do personality factors such as self-monitoring, conscientiousness and sensation-seeking play into users' security practices and the advice that led them to those practices? (Q3); How do users' knowledge and awareness of security threats, motivations, and belief that they can change their levels of security and security outcomes affect the advice they take? (Q4).

To answer these questions, we designed a semi-structured interview study. During a 60-minute interview, we ask questions designed to help participants articulate their cyber- and physical-security habits, as well as when, where, and from whom they learned these strategies. Along with qualitative coding and statistical analysis, we will apply the Theory of Planned Behavior to better understand why users take certain security behaviors and why, or why not, users seek out and implement particular security advice [6]. The Theory of Planned Behavior provides a framework for understanding how users' knowledge about security tactics and agency, or perceived ability to be secure, affect their outcomes.

Thus far we have conducted the study with ten pilot participants, and we anticipate approximately 50 participants total. Although it is too early to identify definitive results, our interviews thus far suggest that cybersecurity advice is more diffuse and less authoritative than physical-security advice, sensation-seeking (risk-taking) is correlated with using fewer total security behaviors, and women undertake more physical-security behaviors, but not more cybersecurity behaviors, than men. We believe that our eventual results can inform the design of security interventions targeting the points where behaviors are learned and focused on helping users identify and prioritize the most important suggestions.

2. RELATED WORK

In this section, we discuss what prior research has already discovered about users' security behaviors.

Das et al. have shown that social influence can affect users' choice to adapt or change security behaviors [3,4]. Rader et al. found that security stories from non-expert peers impacted how users thought about computer security and what security decisions they made [6]. Additionally, a review by Howe et al. of previous research on factors influencing users' in-the-moment security decisions highlights how socioeconomic status, and the corresponding belief that one's information may not be "important enough to hack," can play into users' security behaviors [7]. This review also notes large differences in advice sources between the undergraduate and adult population. In this work, we take a broader view and ask participants about all the sources from which they learned certain security behaviors, including social sources such as those investigated by Das et al. and Rader et al.

3. METHODS

To answer our research questions, we designed a semi-structured interview protocol. We ask participants when, where, and from whom they learned these security strategies (Q1). We investigate what security tactics users are aware of, which tactics they choose not to use, and why they choose to use or not use each tactic of which they are aware (Q1). We explore what sources of advice users encounter and which sources they use for different domains of their online safety (safety while online banking, emailing, etc.), as well as which sources of advice they use for physical safety

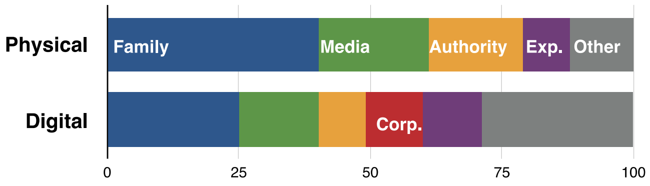

Figure 1. Sources of cybersecurity advice are more diffuse.

(protecting their dwelling, their vehicle, themselves) (Q2). We also investigate how secure users feel and whether they feel they have the ability to make themselves more secure if they so choose (Q4). Finally, we collect demographic information as part of our screening process and administer three personality measures at the end of the interview session (Q3). The measures are the Snyder 18-item Self-Monitoring Scale, which measures participants' need to control their presentation to the outside world [8]; the Ten-Item Personality Inventory (TIPI), which measures participants' Big 5 personality traits (openness, conscientiousness, extraversion, agreeableness, and emotional stability) [9]; and an eight item measure of sensation-seeking measure, which provides insight into participants' propensity to take risks [10]. We will recruit approximately 50 participants for these interviews.

Participants are selected based on demographic factor blocking (elicited via a screening survey). As discussed in Section 2, demographic factors like socioeconomic status and age may play an important role in cyber-security behaviors; as a result, we focus on recruiting participants with a broad range of ages, income levels, ethnicities, and education levels.

The data collected during these interviews is coded and analyzed using open coding and the Theory of Planned Behavior. Security behaviors (such as password protecting devices, using two-factor authentication, locking car doors, and carrying mace when walking alone) are identified and counted. Security advice sources are identified and classified as: **active media** (e.g., online articles or social media content explicitly sought for its security content), **passive media** (e.g., a TV show or other media not explicitly sought for its security content), **authority** (e.g., police), **corporate** (e.g., recommendation from a bank or advertisement from Apple), **employer IT** (e.g. IT staff or an IT newsletter), **expert peers**, **peers**, **family**, **intuition/personal experience**, and **prior negative experience**.

4. PRELIMINARY RESULTS

In this section, we discuss preliminary trends identified from interviewing our 10 pilot participants.

Thus far, six of our participants are security-sensitive. Seven are women. Ages ranged from 18 to 60, with seven participants older than 30; annual incomes ranged from $30,000 to over $150,000; and ethnicities included White, Black, Hispanic, and Asian.

We have seen a wider variety of cyber-security than physical-security advice sources cited (Figure 4). While family and media are important sources for both, they are less important for cyber-security; authority sources like police are replaced with corporate sources like tips from the user's bank or Apple. (Negative experiences play a small but significant role in both cases.) Participants are also less confident about whether cyber-security advice is trustworthy. According to one participant, "plausibility is hard to measure with cyber-security [advice], so it can be harder to believe." We were surprised that multiple participants cited employer IT as a significant cyber-security advice source. For example, participants noted, "I always read the IT newsletter" and "I often ask my colleague in IT about [security tactics]."

Within our small sample size, thus far we have observed a negative correlation (*r=-0.68)* between sensation seeking (a proxy for risk-taking) and the total number of cybersecurity behaviors practiced by a given user. There is a positive correlation between being female and practicing more physical-security behaviors (*r*=, but no such correlation between being female and practicing more cyber-security behaviors (*r=0.29)*. Finally, being older is positively correlated with practicing more physical-security behaviors (*r=0.69)*; no correlation is observed between age and cybersecurity behaviors (*r=0.34)*.

We expect further interesting insights to emerge as we conduct more interviews.

5. ACKNOWLEDGEMENTS

We thank Yla Tausczik, Bethany Tiernan, and Claire Tills for their input. This material is based on work supported by Maryland Procurement Office contract no. H98230-14-C-0137.

6. REFERENCES

[1] Lee, R., Kiesler, S., Kang, R., and Madden, M. 2013. Anonymity, Privacy, and Security Online. Pew Research Center. http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

[2] Pricewaterhouse Coopers. 2014. The Global State of Information Security Survey 2015. http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.

[3] Das, S., Kim, T. H., Dabbish, L. A., and Hong, J. I. 2014. The Effect of Social Influence on Security Sensitivity. In *Proc. SOUPS*.

[4] Das, S., Kramer, A. D.I., Dabbish,, L. A., and Hong, J. I. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proc. ACM CCS*.

[5] Rader, E., Wash, R., and Brooks, B. Stories as Informal Lessons about Security. 2012. In *Proc. SOUPS*.

[6] I. Ajzen. 1991. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50, 2, 179-211.

[7] Howe, A. E., Ray, I., Roberts, M., Urbanska, M., and Byrne, Z. 2012. The Psychology of Security for the Home Computer User. In *Proc. IEEE S&P*.

[8] Snyder, M., and Gangestad, S. 1986. On the Nature of Self-Monitoring: Matters of Assessment, Matters of Validity. *J. Personality and Social Psychology.* 51:1, 125-139.

[9] Gosling, S. D., Rentfrow, P. J., and Swann, W. B. 2003. A very brief measure of the Big-Five personality domains. *J. Research in Personality.* 37, 504-528.

[10] Hoyla, R. H., Stephenson, M. T., Palmgreen, P., Lorch, E. P., and Donohew, R. L. 2002. Reliability and validity of a brief measure of sensation seeking. *Personality and Individual Differences*. 32, 401-414.