End-user Willingness to Follow Expert Information Privacy Recommendations From a Tip Sheet.

Nelson Jaimes
The George Washington University
njaimes@gwmail.gwu.edu

ABSTRACT

Prior research has examined segmentations of end-user populations by their information-security-related mental models, perceptions, and security-related intentions. Different categories of individuals have notable differences in technical background and privacy preferences. Rule lists and tip sheets are often deployed by organizations to enlist the help of the end-user to improve computer security. In this study, a group of 25 Amazon Mechanical Turk workers responded questions about their information-security-related intentions, then read a tip sheet about information privacy from the Cybersecurity and Infrastructure Security Agency, (CISA) then answered questions about their willingness to spend resources on following the recommendations from the tip sheet. This study finds that not all subjects are willing to spend money, time, or effort to follow the rules in the tip sheet. This study also finds that subjects that had higher scores on a security intentions scale were willing to spend a significantly different amount of effort following the recommendations on the tip sheet in some, but not all scenarios. The study concludes with recommendations based on these findings.

1. INTRODUCTION

Efforts to improve information security and privacy in an end-user population have often included attempts to inform end-users to improve their mental models about information security and to persuade them to adopt information-security-protecting behavior.

Prior research appears to show that end-users have notable differences in their information privacy perceptions and mental models.

Many studies have attempted to reduce the complexity of variation in end-user perceptions and mental models by aggregating user perceptions into categories.

One of the benefits of segmentation of end-user populations by their beliefs and perceptions is that it might permit better prediction of end-user information-security-related behavior.

Unfortunately, population segmentation is not directly translated into population behavior. The well-known privacy paradox is an observed gap between information security goals and information-security-seeking behavior in individuals.

Some research has attempted to close the gap between perceptions and behavior by measuring individuals' willingness to spend resources in support of information-security-related goals.

Another benefit of optimal segmentation of end-user populations is that it might allow information security experts to optimally persuade end-users to adopt information-security behaviors by tailoring advice for each of the knowledge and perception categories.

However, data about information security end-user perceptions is not always available, and tailored information delivery is not always possible, so it is not surprising that recommendations that target all end-user types (such as tip sheets) are still widely used.

This study will evaluate the intentions of spending time, money, and effort resources of end-users after reading an information security recommendations tip sheet provided by the Cybersecurity and Infrastructure Security Agency (CISA).

This study also attempts to determine whether segmentation of an end-user population by their information security behavior intentions results in significantly different willingness to spend resources to follow the recommendations on the tip sheet.

1.1 Research Questions

- RQ1: How willing are individuals to spend time, money and/or effort resources to follow the cybersecurity recommendations from CISA about online privacy and passwords?
- RQ2: When categorized by their responses to the Security Intentions Behavior Scale, (SeBIS) do individuals that belong to different groups intend to spend significantly different time, money, and/or effort resources to follow the online privacy and password recommen-

dations from CISA?

2. RELATED WORK

2.1 Privacy Perceptions

The privacy paradox is a well-known [1, 6] computer-security associated behavior, and it can describe the inconsistencies between computer security and privacy abstract goals and specific behavior in each individual.

2.2 Advice Delivery

Delivering advice with the intent of persuasion has been previously studied in several settings, [8, 10, 16, 20, 23, 28] including advice by peers, experts, and computers. In the context of computer security and privacy, even small changes in advice delivery can have an effect [2, 4].

Several studies[2–4, 17, 25, 26, 29] have examined the effectiveness of information privacy advice that attempts to help users make better privacy protecting choices online.

A 2020 study by Redmiles, et al. [22] studied the usability of different types along axes of comprehensibility, perceived usefulness, and perceived actionability of the advice. It found that end-users quality ratings of information privacy advice were wide-ranging. Computer security experts participating did not agree on the prioritization of the advice, and the study found "significant room for improvement."

A study by Johnston et al. [17] evaluated the influence of fea appeal in end-user computer security compliance. It found that the impact of fear appeals are determined by perceptions of self-efficacy, response efficacy, threat severity, and social influence.

A field study by Liu et al. [19] recruited subjects online using social media related to mobile devices that use the Android operating system. A personal mobile phone information privacy assistant was developed and evaluated in the study. Subjects in the study were convinced to follow most of the app's recommendations. Although some of those results might have happened due to social desirability, the findings are still promising for the field of information security and privacy usability.

2.3 Relating End-User Information to Protective Actions

Several papers have attempted to find categories of end-user information privacy behavior. Initial segmentations like the often-cited Westin categories have not always matched with intended user behavior [27].

In a 2015 study by Kang et al, [18] end-user mental models of the internet were evaluated. The study found that the amount of technical training (n.b. technical training did not necessarily mean computer security training) did not have a relationship to the amount of protective actions individuals took to protect their information. The same paper stated that knowledge about privacy threats and risks might predict privacy protecting behavior, and found many misunderstandings and use of suboptimal safety heuristics in the subjects the study interviewed.

A 2016 study by Dupree et al [11] attempted to cluster 32 end-users by their attitudes and behaviors toward security practices. It found five different clusters, including "Lazy Experts," who helped others with security concerns, and "Fundamentalists," who did not usually help others with computer security.

A 2008 study by Beautement et al. [5] studied the cost-benefit perceptions of employer-required computer security policies. The study found that framing effort-related user costs as financial costs.

A 2015 study by Egelman et al. [12] developed the Security behavior Intentions Scale, (SeBIS) which can be used for measuring computer security and information privacy goals.

2.4 Need for Streamlined Presentation of Information to End-Users

A 2016 study by Rao et al. [21] evaluated mismatches between data privacy policies and user expectations about them, given a lack of end-user motivation or ability to read data policies of different websites. It found that end-users found website data policies were perceived as hard to read, and found that around half of subjects were uninterested in knowing how their data was used. The paper argued that simplification of privacy notices could be achieved by emphasizing common mismatches between end-user expectations and existing policies.

2.5 Willingness to Spend Resources on Information Privacy

A 2007 study by Grossklags et al. [14] found that individuals were not willing to spend much on protecting their information. Of course, the study's findings might be different after information privacy issues that have happened in the public sphere since then, such as the Cambridge Analytica scandal. The effects of that scandal have been evaluated by several studies [9, 13, 15, 24].

Another study [7] evaluated willingness to pay for secure Internet of Things (IoT) devices by potential end-users. It found that willingness to spend financial resources on IoT devices increasees when indiviudals are primed advice related to information security.

2.6 Tailored surveys for specific goals

The paper by Dupree et al [11] recommends clustering of end-users for specific end-goals, rather than establishing a more permanent classification of end-user behavior.

3. METHODS

3.1 Subjects

In this study, 31 subjects completed onine surveys. Subjects were recruited using Amazon Mechanical Turk. They completed surveys hosted on Qualtrics. Six subjects failed attention checks, and 25 subjects were included in the data for analysis. Attention checks failure was manually determined by the author for each of the subjects if the subjects did not attempt to summarize the CISA tip sheet, or when they failed a multiple-choice attention check question.

Subjects were categorized by high vs. low SeBIS scores, which resulted in placement into high or low groups based on whether each individual score was higher or lower than the average SeBIS score of the subjects in this study.

3.2 Tasks

Subjects answered questions based on the SeBIS survey. Questions were taken from the Gelman et al. 2015 paper, [12] and were adapted as true/false binary questions in an effort to reduce subject survey fatigue.

After the SeBIS questions, subjects read an information privacy tip sheet provided by the Cybersecurity and Infrastructure Security Agency (CISA) as part of National Cybersecurity Awareness Month (NCSAM). After reading, subjects were asked to summarize the recommendations in the tip sheet. Finally, subjects answered questions about their willingness to spend time, money, and/or effort on following the advice in the tip sheet.

3.3 Data Analysis

All plots and data analysis were conducted using R. To support the repeatability, reusability, and reliability of this research, all statistical tests are included in the R markdown code that generates the pdf for this document.

To answer the first research question, descriptive plots were used to show the willingness of subjects to spend time, money and/or effort on following the tips from the tip sheets.

To answer the second research question, subjects were divided into groups as described earlier and results were computed with each group. Groups were compared by Chi Square tests where numbers were sufficient, and by the Fisher Exact Test when Chi Square would not have provided a reliable answer. For continuous data, the Student's t-test was used to determine significance.

Importantly, the plots and data analysis for this paper can be automatically re-run with any new group of interest.

3.4 Limitations

This study was limited by possible sampling error. There were no requirements placed on the mTurk workers recruited other than a high acceptance score, so the sample is likely not representative of any specific population. Of course, this could impact the ecological validity of the findings of this study. However, this is a natural avenue for future research. A greater number of subjects would allow stratification between age groups and/or other groups of people that might increase external validity. This study used questions adapted from the SeBIS, but did not use the SeBIS. Any reductions in correlation between SeBIS scores and responses in this study might have been due to this change. Similar to the previous difficulty, this could be addressed in future research by determining the correlation between the adapted SeBIS used in this study and the original SeBIS. However, even though the SeBIS is adapted, the validity of the results in this study can be effectively considered using the adapted SeBIS used in this study. Finally, no baseline responses were obtained before reading the tip sheet, so it is uncertain whether the tip sheet had any effect. However, the fact that all subjects read the tip sheet assures that regardless of their prior preferences, all subjects were aware of the recommendations in the tip sheets. Further research could establish a baseline of a representative population.

4. RESULTS

4.1 Overall Subject Responses

Answering the first research question requires the description of the overall subject responses in reference to information security.

4.1.1 Overall SeBIS Scores

Subject SeBIS scores spanned almost the entire possible range (Figure 1). The mean score was 15.12 (interquartile range = 12-18).

4.1.2 Overall Multi-Factor Authentication Preferences

Subjects were most willing to use Multi-Factor Authentication (MFA) when using banking websites, and least likely to use MFA when using learning websites. When given an option to use from zero to one hundred minutes, subjects were willing to spend a mean time of 33.17 minutes (interquartile range 10-50). Overall MFA preferences are plotted in Figure 2.

4.1.3 Overall Willingness to Use a Password Manager

Overall subject willingness to use a password manager is plotted in figure 4. When given an option to spend from 0-100 dollars on a password manager, the mean amount subjects were willing to spend was 30 dollars (interquartile range = 5-52). Overall subject willingness to spend money on a passsword manager is plotted in figure 5.

4.1.4 Overall Willingness to Update Apps

Subject responses regarding their willingness to update their apps (Figure 6) appeared to gravitate to secure options like enabling automatic updates or updating their apps after every request. The peak willingness to enable automatic updates occurred in education and job related apps. Not all subjects were willing to update their apps. A few subjects were never willing to update their apps, and several subjects were only willing to update their apps when the apps stop working. The peak of these less secure behaviors was in social media apps.

4.1.5 Overall Willingness to Verify App permissions

No subjects were willing to always check whtether their app permissions are the minimum required for their apps to function. Less than 50 percent of subjects were willing to check their app permissions often.

4.1.6 Overall Wifi-Seeking Behavior While Traveling

Overall, a non-zero amount of subject reported that they were likely to use hotspots from an unknown source or public wireless internet. However, secure responses to internet seeking behavior was higher in secure responses (i.e. seeking non-public wifi or using a hotspot) than in insecure responses (i.e. using an unknown hotspot or public wifi). Re-

sponses between non-privacy-seeking and privacy seeking responses (A vs B) were significantly different and are plotted in Figure 8 (p = 0.0476176).

4.2 Grouped Subject Responses

Answering the second research question requires the description and comparison of subject responses in reference to information security when grouped by high SeBIS scores vs. low SeBIS scores.

4.2.1 Grouped SeBIS Scores

Subjects in the high scoring group had a mean SeBIS score of 18.75, (interquartile range 17.75 - 20.25) while subjects in the low scoring group had a mean SeBIS score of 11.50 (interquartile range 10.25 - 14.25). Subject SeBIS scores are plotted in Figure 9.

4.2.2 Grouped Multi-Factor Authentication Preferences

Subject willingness to use MFA was not significantly different between high-scoring and low-scoring groups on the SeBIS. Subject responses related to MFA are plotted in Figure 10 and Figure 11.

4.2.3 Grouped Willingness to Use a Password Manager

Subject willingness to use a Password Manager was not significantly different between high-scoring and low-scoring groups on the SeBIS. Subject responses related to password managers are plotted in figure 12 and figure 13.

4.2.4 Grouped Willingness to Update Apps

Subject willingness to update apps was significantly different ($p < 0.00001$) between high-scoring and low scoring groups. Subject responses related to app-updating behavior are plotted in figure 14.

4.2.5 Grouped Willingness to Verify App permissions

Subject willingness to verify app permissions was significantly different (p = 0.0068376) between high-scoring and low scoring groups. Subject responses related to app-updating behavior are plotted in figure 15.

4.2.6 Grouped Wifi-Seeking Behavior While Traveling

Subject internet seeking behavior intentions while traveling were significantly different between secure and not secure behaviors (p = 0.010101 and p = 0.0438228) for the high-scoring group but not significant for the low scoring group both in wifi preferences and in hotspot preferences. Subject responses related to app-updating behavior are plotted in figure 16.

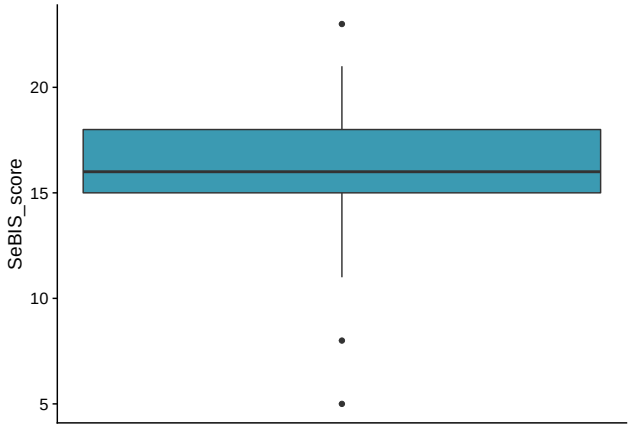

Figure 1. SeBIS scores for all subjects in the study. The questions from the SeBIS were adapted such that subjects only had a True/False option for each question. The minimum score was 5 out of 24 questions and the maximum score was 21 out of 24 questions. The mean score was 15.12, and the median score was 16.

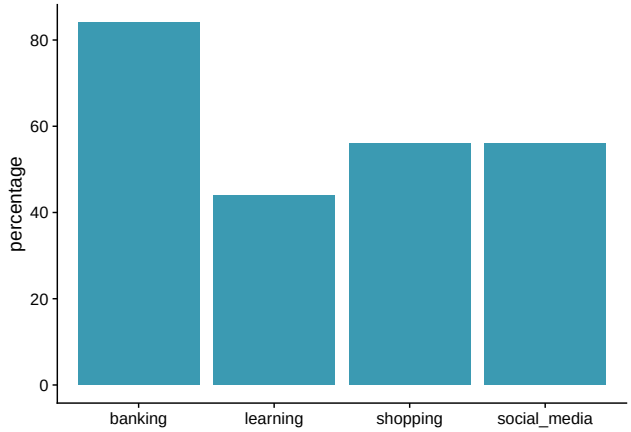

Figure 2. Multi-Factor Authentication (MFA) preferences by type of website. Banking was the most popular purpose for use of MFA. Answers to this question were significantly different (chi square p = 0.0238158).

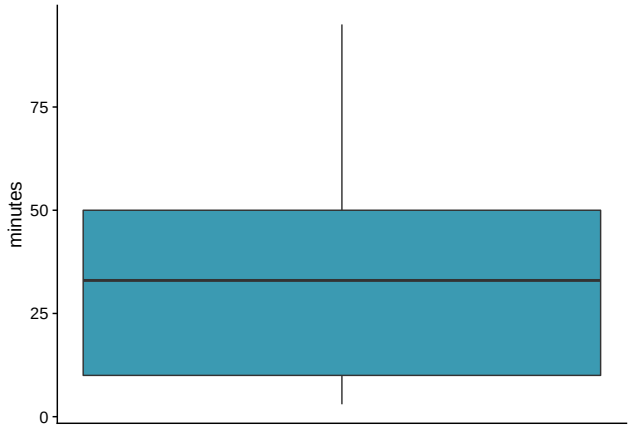

Figure 3. Willingness to spend time on setting up MFA for an online account when given a range from 0 to 100 minutes. Subject willingness to set up MFA varies widely, with a mean

of 33.17 minutes (interquartile range 10-50).

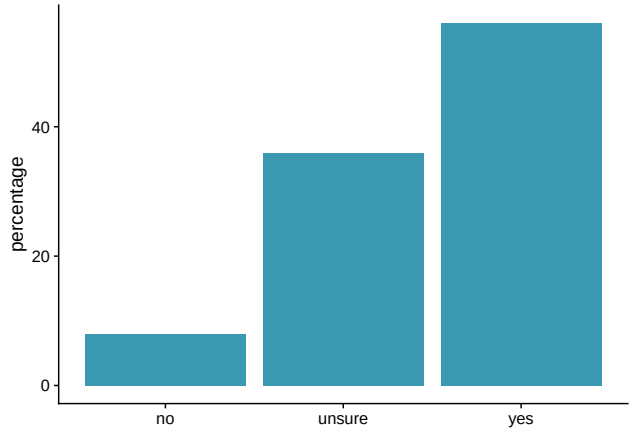

Figure 4. Willingness to use a Password Manager. Around half of subjects were willing to use a password manager, and many subjects were unsure about using a password manager.

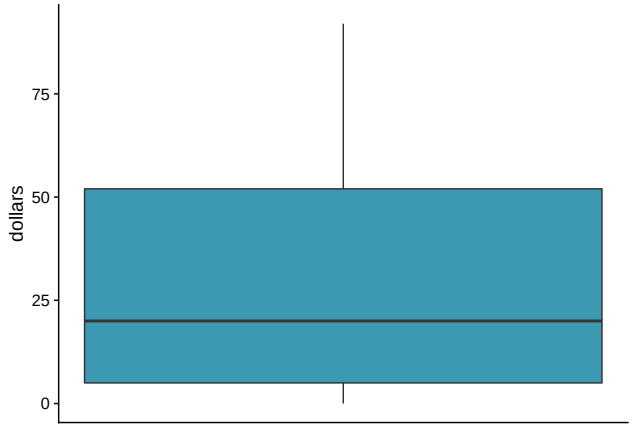

Figure 5. Willingness to spend money on a Password Manager when given a range from 0 to 100 dollars. Subject willingness to spend money on a password manager is positively skewed. The mean amount subjects were willing to spend was 30 dollars (interquartile range 5-52).

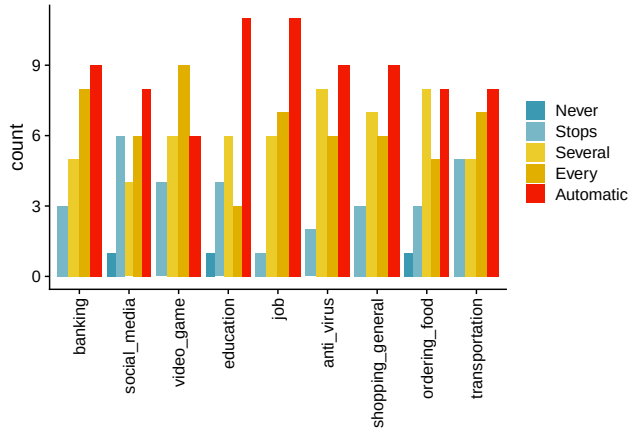

Figure 6. Willingness to update apps by the purpose of the apps. Overall, the most popular responses from subjects were updating apps automatically or after every request from the app. Updating automatically was the most popular in every application other than in video games and in food ordering apps. The applications where automatic apps were most likely were in education apps or job-related apps.

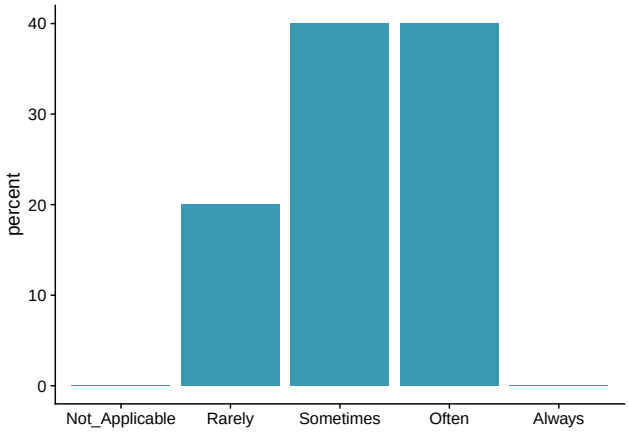

Figure 7. Willingness to verify app permissions are the minimum required for the app to function. Even though subjects had just read a tip sheet from an expert source (CISA), no subjects were willing to always check whether their app permissions are the minimum for the app to function, and less than half of subjects were willing to check their apps' permisisons often.

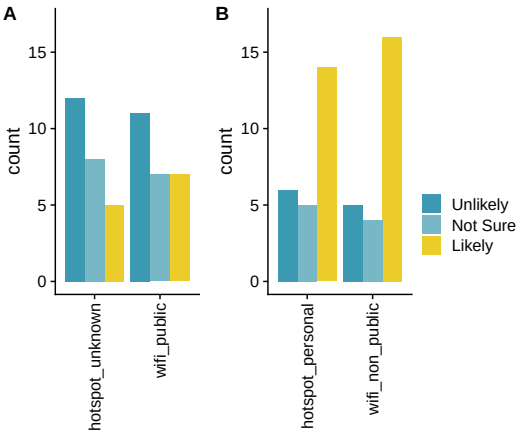

Figure 8. Behavior related to internet access while traveling. In A, risky behavior responses are shown. Overall, a non-zero amount of subjects reported they were likely to use hotspots from an unknown source or public wifi. More subjects responded they were likely to use a personal hotspot or wait until they could access a non-public wifi than any other option. Responses between non-privacy-seeking and privacy seeking responses (A vs B) were significantly different ($p = 0.0476176$).

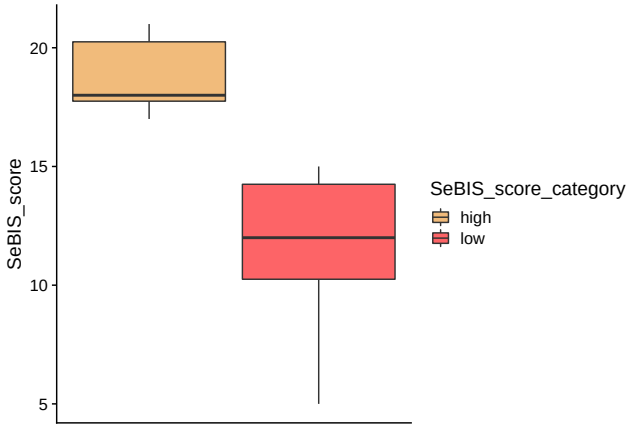

Figure 9. SeBIS score by SeBIS score group. Subjects in the high group had a mean SeBIS score of 18.75, (interquartile range 17.75 - 20.25) while subjects in the low group had a mean SeBIS score of 11.50 (interquartile range 10.25 - 14.25).

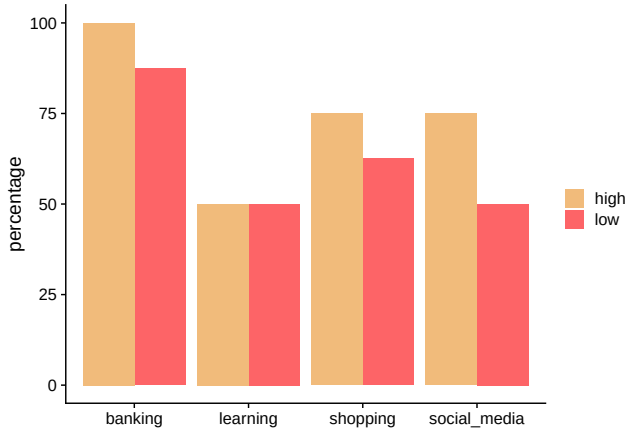

Figure 10. Multi-Factor Authentication (MFA) preferences by SeBIS score grouped by type of website. The high scoring group and the low scoring group on the SeBIS did not have significantly different Multi-Factor Authentication (MFA) responses (p=1).

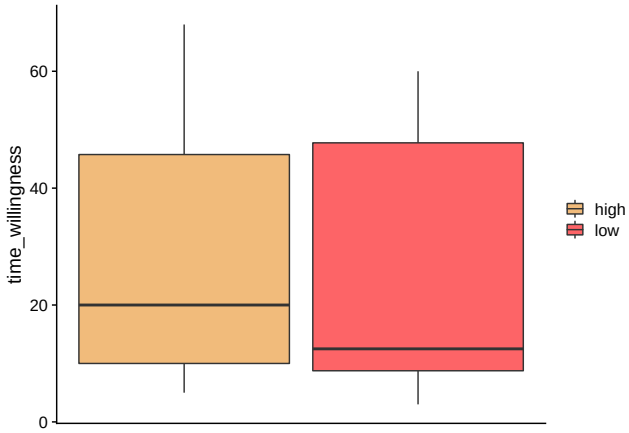

Figure 11. Willingness to spend time on setting up MFA for an online account in subjects grouped by having high scores vs. low scores on the SeBIS. There were no significant differences between the high and low scoring groups (p = 0.7159863)

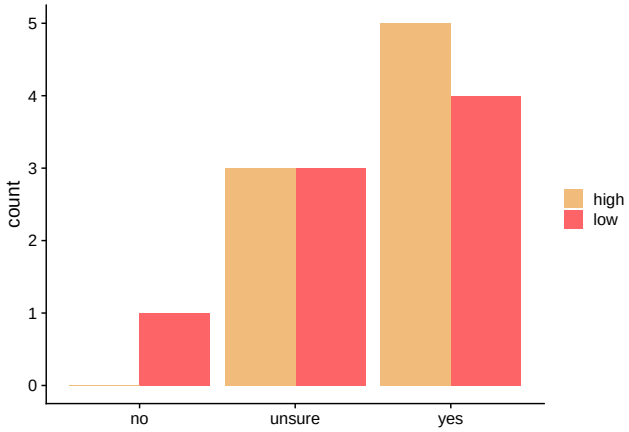

Figure 12. Willingness to use a Password Manager by SeBIS score. Groups determined by high vs. low subject scores on the SeBIS were not significantly different from each other (p = 1).

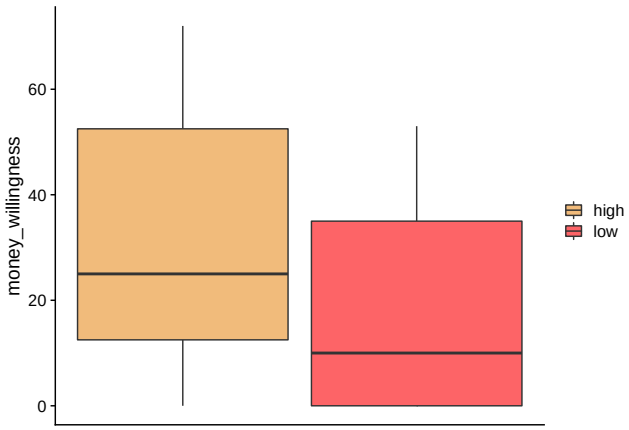

Figure 13. Willingness to spend money on a password manager. Subject groups determined by high vs. low SeBIS scores did not have statistically significant differences in the amount of money they were willing to spend on a password manager (p = 0.340311).

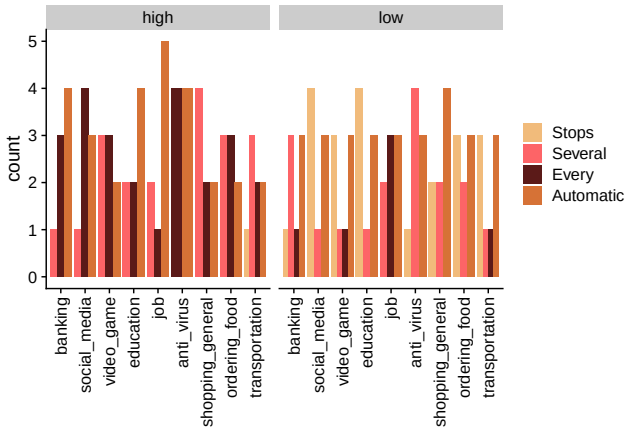

Figure 14. Willingness to update apps by the purpose of the apps in subjects with high vs low SeBIS scores. Over-

all, subject willingness to keep apps updated was significantly different in high scoring vs. low scoring groups ($p = 4.1861654 \times 10^{-7}$).

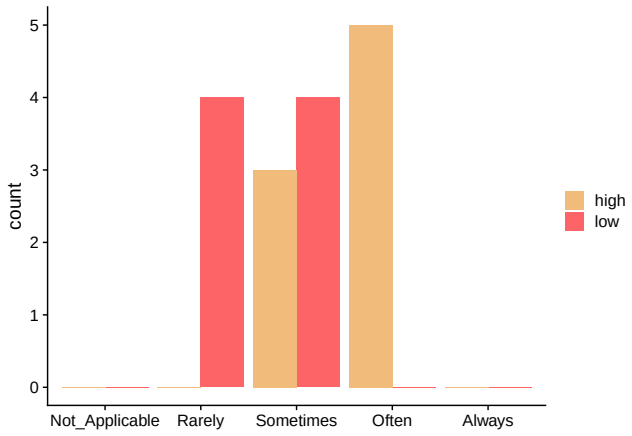

Figure 15. Willingness to verify app permissions are the minimum required for the app to function for high and low SeBIS scoring subjects. Subject willingness to verify that app persmissions are the minimum required for the app to function between high and low scoring groups was significantly different ($p = 0.0068376$).

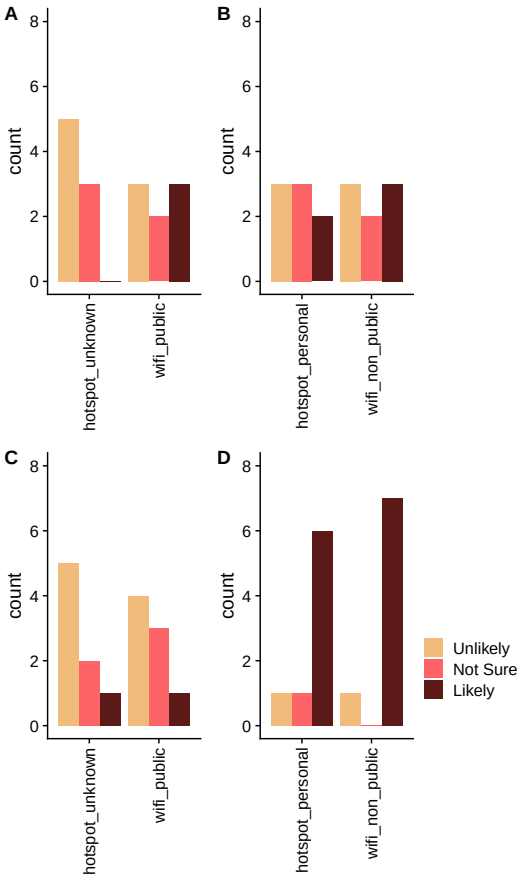

Figure 16. Behavior around internet access while traveling in groups determined by high vs. low scores on the SeBIS. A. Low scoring subjects' preferences for using hotspots from an unknown source or public wifi. B. Low scoring subjects' preferences for using their personal hotspot or waiting until a non-public wifi is available. C. High scoring subjects' preferences for using hotspots from an unknown source or public wifi. D. High scoring subjects' preferences for using their personal hotspot or waiting until a non-public wifi is available. For wifi preferences, high scoring subject intentions to seek public vs. non-public alternatives when seeking an internet connection were significantly different ($p = 0.010101$). Also for wifi preferences, low scoring subject intentions to seek public vs. non-public alternatives when seeking an internet connection were not significantly different ($p = 1$). For hotspot preferences, high scoring subject intentions to seek public vs. non-public alternatives when seeking an internet connection were significantly different ($p = 0.0438228$). Also for hotspot preferences, low scoring subject intentions to seek public vs. non-public alternatives when seeking an internet connection were not significantly different ($p = 0.5213675$).

5. DISCUSSION

5.0.1 *Multi-Factor Authentication Preferences*

After reading the tip sheet from CISA, subjects appeared to be willing to spend a relatively large amount of time setting up MFA for their online accounts. That finding might be due to social desirability bias, due to subjects assumption that the designers of the survey might not respect them if they selected a low number. It could also be due to the number of websites subjects were considering: that result has a different connotation if the subjects were considering spending 33.17 minutes setting up MFA for 100 websites vs. setting up MFA for 5 websites. Further research could further question subjects to determine the reliability and reason for that finding. However, it is useful to consider that for the population considered for this study, reaching at least 75% of individuals might require MFA times that add up to at most ten minutes.

The MFA preferences by type of website (i.e. banking, learning, shopping, and social media) were significantly different. Subjects were most willing to use MFA for banking, although a compromise of any of those website types has a potential risk of exposure of some PII. Judging by those results, using an appeal to financial risk could be beneficial in motivating end-users to adopt MFA.

5.0.2 *Willingness to Use a Password Manager*

Even though subjects had just read a tip sheet from CISA, which they might perceive as an expert source, only about half the subjects were willing to use a password manager. Many subjects were not sure whether they wanted to use a password manager, and few subjects were unwilling to use one. However, most subjects agreed that password managers have financial value. It is worth exploring this value gap further to explain why subjects might feel that password manager services are valuable and yet not be willing to use them. From this study's findings, it appears tip sheets alone might not be enough to sway individuals to adopt password managers.

5.0.3 *Willingness to Update Apps*

Subjects were generally willing to update their apps across different app types at least sometimes, but many subjects

were still unwilling to keep their apps updated automatically or after every request. Furthermore, some subjects were only willing to update after their apps stops working. These data seem to indicate that tip sheets alone are not effective to convince end-users to keep their apps updated. It is possible that end-users suffer from updating fatigue. App designers might consider making automatic updates the norm to avoid security gaps caused by apps that are not updated, or operating system designers to streamline the process of application updates to lower the time and effort required for end-users to update their apps.

5.0.4 Willingness to Verify App permissions

Subjects were not convinced by the tip sheet to verify app permissions are the minimum required for their apps to function. Verifying permissions might require technical knowledge that most end-users do not possess and a time investment that is too high for many end-users. Protecting end-user information privacy by granting minimum permissions might be accomplished by the operating system designers. Automated brute-force testing to check functionality given every combination of permissions could be a requirement for publishing an app or app update. However, in the current surveillance capitalist system, that kind of strategy might be in direct opposition to the motivations behind app development.

5.0.5 Wifi-Seeking Behavior While Traveling

In overall subject-situation encounters related to internet access while traveling, non-privacy seeking responses were significantly different from non-privacy seeking responses. There were more privacy-seeking subject-situation encounters (e.g. Unlikely to use an unknown hotspot) than other available possibilities, but some subjects were still not willing to seek privacy for their internet connection while traveling. It is possible that this data could result because of subjects not being able to afford a private online connection, and further research could determine the extent of that cause of the problem. However, if subjects have private choices available and are simply choosing to use other wireless internet access points, tip sheets are not effective in convincing all end-users to use secure behaviors.

5.1 Grouped Subject Responses

SeBIS score group (high vs. low) results was not related to MFA preferences and password manager preferences. The apparent lack of relationship could be due to a loss of sensitivity due to the adaptation of the SeBIS responses. However, SeBIS score group was related to subject willingness to update apps, verify app permissions, and to the statistical difference between privacy-seeking and non-privacy seeking behavior while considering wireless internet use. Another explanation for these data is that the privacy paradox is exhibited in some situations. That does not mean that behavior categories are useless. Given these results, organizations could test the relationship between categories and behavior in sample populations that are representative of the populations of interest instead of assuming a relationship. One way to accomplish this could be running the scripts that accompany this publication using the survey that accompanies this publication and evaluating the automatically-calculated results.

5.2 Ecological Validity

Also discussed in the limitations section, the subjects in this study are likely not representative of other populations of interest. Further research should examine whether there are any patterns in a representative sample of the US or world population by age or education factors.

5.3 Intervention Effectiveness

Finally, this study examined subject perceptions after reading the tip sheets while not verifying baseline perceptions before reading the tip sheets. Future studies could gather a baseline that would enable comparison of the direct effects of a tip sheet or other intervention. However, the results in this study are arguably more relevant to computer security, because the goal of information privacy and security is to persuade individuals no matter their prior perceptions about the topic. Of course, examining the effectiveness of tip-sheet interventions is also a worthwhile goal and will hopefully be studied by future research studies.

6. CONCLUSIONS

- MFA enrollment should be as quick as possible, since longer enrollmnent times might become a barrier for adoption.
- Appealing to financial risks of online activity might be a successful strategy to promote adoption of MFA.
- Tip sheets might not be enough to convince end-users to use password managers, although subjects seemed to believe password managers are financially valuable.
- End-users are not all willing to keep apps updated, so security updates should be easier for them or happen without the need for their participation.
- In the current environment, it appears verification of minimum app permissions is not a feasible alternative for protecting end-user privacy. That goal might require the intervention by operating system designers to provide app-specific automated testing of permissions.
- Tip sheets do not appear to be sufficient to convince all end-users to seek private wireless internet connections.
- Overall, tip sheets do not appear to be fully effective in convincing all end-users to protect their personal information. Tip sheets should be used in conjunction with other methods to promote secure behavior in end-user populations.
- Prediction of end-user behavior by their behavior-intention category should be used only if a relationship has been found in a sample population representative of the target population, since the relationship does not always exist.

7. APPENDIX: ENTIRE SURVEY INSTRUMENT

7.1 SeBIS questionnaire (24 questions, true false)

1. When I'm prompted about a software update, I install it right away.

2. When my computer wants me to reboot after applying an update or installing software, I put it off.
3. I try to make sure that the programs I use are up-to-date.
4. I manually lock my computer screen when I step away from it.
5. I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
6. I log out of my computer, turn it off, put it to sleep, or lock the screen when I'm done using it.
7. I use a PIN or passcode to unlock my mobile phone.
8. I use a password/passcode to unlock my laptop or tablet.
9. If I discover a security problem, I continue what I was doing because I assume someone else will fix it
10. When someone sends me a link, I open it without first verifying where it goes.
11. I verify that my anti-virus software has been regularly updating itself.
12. When browsing websites, I mouseover links to see where they go, before clicking them.
13. I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
14. I backup my computer.
15. When I hear about websites that have been hacked, I wait to change my passwords until I have been personally notified.
16. I use some kind of encryption software to secure sensitive files or personal information.
17. I do not change my passwords, unless I have to.
18. I use different passwords for different accounts that I have.
19. I do not include special characters in my password if it's not required.
20. When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
21. When I'm done using a website that I'm logged into, I manually log out of it.
22. I submit information to websites without first verifying that it will be sent securely
23. I use privacy software, "private browsing," or "incognito" mode when I'm browsing online.
24. I clear my web browsing history.

7.2 Reading block

Please read through this tip sheet: online privacy `https://www.cisa.gov/sites/default/files/publications/NCSAM_OnlinePrivacy_2020.pdf`

Please write a short paragraph listing the types of tips discussed in the article

7.3 Study Survey Questions

Multi-Factor Authentication (MFA) involves using something you have or something you are (in addition to your username and password) to verify your identity when you log in.

Common ways of using something you have:

- use a separate security token or app
- receive verification texts, calls, or emails
- use a smart card

Common ways of using something you are:

- use your fingerprint
- use facial recognition
- use voice recognition

Are you willing to set up MFA on your online accounts? (yes) On which kinds of online accounts are you using or would you be willing to use Multi-Factor Authentication (MFA)? * social media * banking
* online learning * shopping

Imagine you have 100 minutes of free time. How much time out of those 100 minutes would you be willing to spend setting up MFA for an online account? (text entry, 0 minutes - 100 minutes, numeric verification)

A password manager is an app protected by one main password. It makes password use more secure and convenient. It can

- store your passwords
- generate strong passwords

Would you be willing to use a password manager? (yes)

Please select how you would update apps in these categories: (not applicable (do not use that type of app), never update after installation, update when it stops working, update after more than one request, update after every request, enable automatic updates so that app is constantly updated)

- banking app
- social media app
- video game app
- app required for education
- app required to perform your job
- anti-virus or anti-malware app
- app for buying products
- app for ordering food
- ride-sharing (transportation) app

When you download an app, how often do you intend to verify the types of access permissions the app has are the minimum required? (not applicable, rarely, sometimes, often, always)

What is the red round rubber ball made out of?

- spherical
- oval
- red
- rubber

Imagine you are traveling and you need to find an internet connection to access your bank account online. How likely are you to: (Very likely, somewhat likely, unlikely / would avoid entirely)

- use a public wireless internet connection?
- wait to ask available staff for the public wifi name and login instructions? (yes) How many minutes would you wait to verify that information? (text response, verify numeric)
- wait until you reach a trusted non-public wireless internet connection?
- use your mobile phone as a wireless internet hotspot?
- Connect to a wireless network without asking nearby staff?
- Connect to someone else's mobile phone hotspot that seems to have forgotten to protect it with a password?

How seriously did you take this study? (slider)

References

[1] Acquisti, A. and Grossklags, J. 2005. Privacy and rationality in individual decision making. *IEEE security & privacy*. 3, 1 (2005), 26–33.

[2] Albayram, Y. et al. 2017. "... Better to use a lock screen than to worry about saving a few seconds of time": Effect of fear appeal in the context of smartphone locking behavior. *Thirteenth symposium on usable privacy and security ({soups} 2017)* (2017), 49–63.

[3] Almuhimedi, H. et al. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. *Proceedings of the 33rd annual acm conference on human factors in computing systems* (2015), 787–796.

[4] Al Qahtani, E. et al. 2018. The effectiveness of fear appeals in increasing smartphone locking behavior among saudi arabians. *Fourteenth symposium on usable privacy and security ({soups} 2018)* (2018), 31–46.

[5] Beautement, A. et al. 2008. The compliance budget: Managing security behaviour in organisations. *Proceedings of the 2008 new security paradigms workshop* (2008), 47–58.

[6] Blank, G. et al. 2014. A new privacy paradox: Young people and privacy on social network sites. *Prepared for the annual meeting of the american sociological association* (2014).

[7] Blythe, J.M. et al. 2020. What is security worth to consumers? Investigating willingness to pay for secure internet of things devices. *Crime Science*. 9, 1 (2020), 1.

[8] Bonaccio, S. and Dalal, R.S. 2006. Advice taking and decision-making: An integrative literature review, and implications for the organizational sciences. *Organizational behavior and human decision processes*. 101, 2 (2006), 127–151.

[9] Brown, A.J. 2020. "Should i stay or should i leave?": Exploring (dis) continued facebook use after the cambridge analytica scandal. *Social Media+ Society*. 6, 1 (2020), 2056305120913884.

[10] Dalal, R.S. and Bonaccio, S. 2010. What types of advice do decision-makers prefer? *Organizational Behavior and Human Decision Processes*. 112, 1 (2010), 11–23.

[11] Dupree, J.L. et al. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. *Proceedings of the 2016 chi conference on human factors in computing systems* (2016), 5228–5239.

[12] Egelman, S. and Peer, E. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). *Proceedings of the 33rd annual acm conference on human factors in computing systems* (2015), 2873–2882.

[13] González, F. et al. 2019. Global reactions to the cambridge analytica scandal: A cross-language social media study. *Companion proceedings of the 2019 world wide web conference* (2019), 799–806.

[14] Grossklags, J. and Acquisti, A. 2007. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. *WEIS* (2007).

[15] Hinds, J. et al. 2020. "It wouldn't happen to me": Privacy concerns and perspectives following the cambridge analytica scandal. *International Journal of Human-Computer Studies*. (2020), 102498.

[16] Howard, J.J. et al. 2020. Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making. *Plos one*. 15, 8 (2020), e0237855.

[17] Johnston, A.C. and Warkentin, M. 2010. Fear appeals and information security behaviors: An empirical study. *MIS quarterly*. (2010), 549–566.

[18] Kang, R. et al. 2015. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. *Eleventh symposium on usable privacy and security ({soups} 2015)* (2015), 39–52.

[19] Liu, B. et al. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. *Twelfth symposium on usable privacy and security ({soups} 2016)* (2016), 27–41.

[20] Meshi, D. et al. 2012. How expert advice influences decision making. *PloS one*. 7, 11 (2012), e49748.

[21] Rao, A. et al. 2016. Expecting the unexpected: Understanding mismatched privacy expectations online. *Twelfth symposium on usable privacy and security ({soups} 2016)* (2016), 77–96.

[22] Redmiles, E.M. et al. 2020. A comprehensive quality evaluation of security and privacy advice on the web. *29th {usenix} security symposium ({usenix} security 20)* (2020), 89–108.

[23] Reeder, R. et al. 2011. Poster: Helping engineers design

neat security warnings. (2011).

[24] Shipman, F.M. and Marshall, C.C. 2020. Ownership, privacy, and control in the wake of cambridge analytica: The relationship between attitudes and awareness. *Proceedings of the 2020 chi conference on human factors in computing systems* (2020), 1–12.

[25] Wang, Y. et al. 2014. A field trial of privacy nudges for facebook. *Proceedings of the sigchi conference on human factors in computing systems* (2014), 2367–2376.

[26] Wang, Y. et al. 2013. Privacy nudges for social media: An exploratory facebook study. *Proceedings of the 22nd international conference on world wide web* (2013), 763–770.

[27] Woodruff, A. et al. 2014. *10th symposium on usable privacy and security ({soups} 2014)* (2014), 1–18.

[28] Yaniv, I. and Kleinberger, E. 2000. Advice taking in decision making: Egocentric discounting and reputation formation. *Organizational behavior and human decision processes*. 83, 2 (2000), 260–281.

[29] Zhang, B. and Xu, H. 2016. Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. *Proceedings of the 19th acm conference on computer-supported cooperative work & social computing* (2016), 1676–1690.