McNair Research Journal SJSU

Volume 14 *Spring 2018* Article 10

2018

Investigation of Attitudes Towards Security Behaviors

Daniel Kelley

Recommended Citation

Kelley, Daniel (2018) "Investigation of Attitudes Towards Security Behaviors," *McNair Research Journal SJSU*: Vol. 14 , Article 10.
Available at: http://scholarworks.sjsu.edu/mcnair/vol14/iss1/10

Daniel Kelley

Major: Psychology

Mentor: **Dr. David Schuster**

Investigation of Attitudes Towards Security Behaviors

Biography

Daniel Kelley is a first generation college student that aspires to be a User Experience Researcher. He is currently a Psychology major with a minor in Human Computer Interaction, and hopes to obtain his Masters in Human Factors. His current Research interests are in End User Cyber Security Behaviors and Mobile Apps in Healthcare. He is currently a research assistant in Dr. Schuster's VECTR Lab and seeks to obtain a Ph.D. in Human Factors. Daniel's side interests include playing sports with friends, trying new foods, and listening to music. He is a huge anime fan, and a big fan of Bollywood cinema.

Investigation of Attitudes Towards Security Behaviors

Abstract

Cybersecurity attacks have increased as Internet technology has proliferated. Symantec's 2013 Internet Security Report stated that two out of the top three causes of data breaches in 2012 were attributable to human error (Pelgrin, 2014). This suggests a need to educate end users so that they engage in behaviors that increase their cybersecurity. This study researched how a user's knowledge affects their engagement in security behaviors. Security behaviors were operationalized into two categories: cyber hygiene and threat response behaviors. A sample of 194 San José State University students were recruited to participate in an observational study. Students completed a card sort, a semantic knowledge quiz, and a survey of their intention to perform security behaviors. A personality inventory was included to see if there would be any effects of personality on security behaviors. Multiple regression was used to see how card sorting and semantic knowledge quiz scores predicted security behaviors, but the results were not significant. Despite this, there was a correlation between cyber hygiene behaviors and threat response behaviors, as well as the Big Five personality traits. The results showed that many of the Big Five personality traits correlated with each other, which is consistent with other studies' findings. The only personality trait that had a correlation with one of the knowledge measures was neuroticism, in which neuroticism had a negative correlation with the semantic knowledge quiz. Implications for future research are discussed to understand how knowledge, cyber hygiene behaviors, and threat response behaviors relate.

Technology is becoming a global commodity. More individuals are gaining access to computers, laptops, and smartphones as time passes. In 2008, the Internet connected an estimated 541.7 million computers in more than 250 countries on every continent, including even Antarctica (Pesante, 2008). With recent advancements in technology, many users and companies have begun storing sensitive information on the Internet. For example, companies require employees to perform tasks that require them to use the Internet to communicate and exchange sensitive information, including sensitive employee information and proprietary company information. At the same time, users have sensitive personal information, such as banking information, stored online as well. Symantec reported that 86% of the new threats discovered during the first six months of 2006 were aimed at home users (Furnell, 2007). The Cert-Coordination center at Carnegie Mellon University reported that security attacks increased by 68% from 2003 to 2004 (Kruger & Kearney, 2006). The culprit for most of these security breaches can be traced back to human error and a lack of knowledge (Pelgrin, 2014). In 2013, a Symantec internet security report stated that two of the top three causes of data breaches in 2012 were attributable to human error, such as accidental disclosure or falling for phishing scams (Pelgrin, 2014).

Attacks from hackers have become more frequent and more critical as technology has become more sophisticated (Gutzwiller, Hunt, & Lange, 2016). Across the globe, hackers take advantage of the fact that few users understand the benefit of good cyber hygiene behaviors. Cyber hygiene is proactively minimizing vulnerabilities to one’s system (Symantec, 2017). Cyber hygiene includes behaviors such as scanning a computer for viruses and using strong passwords to help maintain system security (Symantec, 2017). One reason why users do not engage in the use of cyber hygiene behaviors is because of a lack of knowledge of what these behaviors are or the importance of them. In 2007, 87% of respondents in a survey in the United Kingdom said that protecting their computer was a top priority, but nearly the same proportion (83%) felt like they did not have enough knowledge to protect themselves (Furnell, Bryant, & Phippen, 2007). This might be attributed to the lack of understanding of the domino-effect that threats could have on their computer and others. For example, an unprotected user allows hackers to infect not just one computer through phishing emails, but to create botnets of thousands of subsequently infected computers. Not only could user information get stolen, but hackers could leverage botnets to penetrate an organization. This is because many compromised computers provide a more powerful attack vector than one alone. By doing this, hackers can greatly increase their power. With a botnet, hackers could execute a denial of service attack, which is an attack that causes internet traffic to slow down the speed of a server or shut it down completely. This type of attack can be—and has been—used to extort money from online businesses (Ianelli & Hackworth, 2005). This is one way outside parties, as well as society, suffer from user naiveté. Pelgrin (2014) stated that "users are insufficiently trained, their systems are not updated, and users are still not cautious about clicking on links. These basic minimum-security layers, which would dramatically improve our cyber security environment, have not been universally adopted" (p. 2).

The lack of user security knowledge has also been felt by many businesses and civilians. For example, Sony's hack resulted from an employee within the company being tricked to allow hackers to access valuable information. This hack resulted in the theft of 77 million credit card numbers, a $170 million cost for technical fixes, and, ultimately, $1-2 billion in losses from stolen information and legal action (Sheppard, Cranell, & Mourton, 2013). The well-known hack of Target resulted in the loss of millions of dollars as well as personal information. Situations such as these will continue to be possible because the lack of knowledge of most end-users, both at home and within organizations, prevents them from defending themselves against cyber threats effectively.

To combat hackers and breaches, it is important for all users to have knowledge of good security behaviors and the importance of them. In 2006, an Information Security Breaches Survey from the UK was distributed asking businesses, "What would most help UK businesses manage their risks in the future?" (Furnell, 2007, p. 410). The most popular answer (by 62% of respondents) was "more information to the general public about information security risks" (Furnell, 2007, p. 411). This is significant because with this knowledge, users will behave more cautiously online, which improves Internet security. This knowledge is also important because users carry their knowledge into the workforce. If users lack knowledge of good security behaviors at home, then it will impact their work environment at large, and the rate of successful security breaches will continue to increase in society. This research supports this statement by showing how knowledge of cyber threats impacts willingness to engage in security behaviors in personal use of the Internet.

Related Work

User Knowledge

Most security breaches happen because of human error (Pelgrin, 2014); as a result, research on the human aspect of security has increased. User behavior affects organizational cybersecurity through interactions with system administrators and other IT professionals. System administrators are responsible for maintaining security within the company and knowing about outside user threats to their organization's system. This influx of information places a high workload on system administrators. If users had better knowledge of security behaviors, it may lighten the workload of system administrators. These behaviors include use of a firewall, maintenance of data, keeping backups, as well as using anti-virus software. The UK government has encouraged these behaviors in the Get Safe Online Week and Information Security Awareness Week campaigns (Furnell & Clark, 2012). The United States Department of Homeland Security has a cybersecurity awareness month as well that seeks to educate end-users (Department of Homeland Security, 2017). These initiatives create more awareness for users because technological solutions are an incomplete solution to the problem. Furnell and Clark (2012) explain that Google accounts, for example, use a two-factor authentication, a system where the user not only types in their login credentials, but also has to verify their identity with a code sent by text message to their mobile phone or other device. This makes it harder for a hacker to get into the user account, but it also requires the user to engage in extra steps, and they must have their mobile device with them to log-in, which is not ideal for usability. This is not ideal for usability because not everyone has mobile phones and if an individual were to lose their phone or their phone got compromised, they would potentially be locked out of their account or would have to engage in many extra steps to get into their account. Thus, user behavior is an important part in their cybersecurity and their organization's cybersecurity. At the same time, users need usable cybersecurity tools and awareness of how to use them.

Antivirus software is another example of technology providing an incomplete solution if it does not consider user behavior. With antivirus software, users are presented with a myriad of features that are difficult to understand, which leads to disuse (Furnell & Clark, 2012).

However, risky user behavior might not be fully explained by knowledge. Some users that are aware of the potential risks that could happen to their system still partake in risky behavior, such as torrenting from untrusted sources or using websites that contain malware. This can occur if the activity they are engaging in is desirable and outweighs the potential risks to their system. These individuals might not be aware of how these risky behaviors can affect their community at large; they may unwittingly participate in a botnet, for example. With this research, I aim to better understand the human aspect of cyber security by exploring how users' knowledge impacts their behavior online.

Security Behaviors: Cyber Hygiene and Threat-Response

One can distinguish between two types of end-user behaviors that positively impact security. The two types are *cyber hygiene* and *threat response*. Cyber hygiene is proactively minimizing vulnerabilities to maintain system security. Scanning a computer for viruses, backing up data, updating, and using strong passwords are examples of cyber hygiene behaviors (Symantec, 2017). Threat response is the ability to prevent an attack from occurring by responding to a specific threat, as well as being able to stop an occurring attack. Scanning a computer after a virus warning or strange computer activity, avoiding a red flagged website, and completing a system restore to eliminate an attack are all examples of threat response behaviors. Cyber hygiene and threat response are similar, but they are separate concepts. Cyber hygiene behaviors can be thought of as putting on armor before going to battle. The armor maintains the health of one's body, as well as minimizes its vulnerabilities to attack in battle. Examples include updating software and using strong passwords. Threat-response behaviors can be thought of as identifying enemies and avoiding them. It also can be thought of as defending oneself from attack by defeating an enemy on the battlefield. Identifying and avoiding enemies is analogous to avoiding threats online. Defeating the enemy is analogous to using one's security tools to stop an attacker. Both constructs have the same goal of protecting users but are executed for different reasons.

Both of these security behaviors require knowledge. Past research has demonstrated that as an individual gains more knowledge on cyber security, it leads to better security behaviors (Arachchilage & Love, 2014). For example, Arachchilage and Love (2014) explained that well-designed end-user security education helps prevent phishing threats. Their study found that when computer user knowledge was high, users tended to avoid and identify phishing threats. They also found that one of the main reasons users fell for phishing threats was a lack of user knowledge (Arachchilage & Love, 2014). Ben-Asher and Gonzalez (2015) suggested that users tend to be more cautious and aware while using the Internet when they have more knowledge of the consequences of the threats online (Ben-Asher & Gonzalez, 2015). This research seeks to support existing research showing that cybersecurity knowledge leads to more engagement in security behaviors. This further contributes to this work by distinguishing between cyber hygiene and threat-response behaviors.

Mental Models, Semantic Knowledge, and Individual Personality

The concept of "mental model" refers to the way a person understands a domain of knowledge (Gentner & Stevens, 2014). Semantic knowledge, on the other hand, is defined as general knowledge or factual knowledge of objects, word meanings, and other subjects (Patterson, Nestor & Rogers, 2007). The difference between these two pieces of knowledge is that a mental model is subjective to the individual and semantic knowledge is objective and based in facts. For example, a participant might classify phishing as bad in their mental model but are not aware of the definition of phishing or what phishing exactly is. For semantic knowledge there is a right or wrong answer, and for mental models it is more up to the specific individual's interpretation of the domain of knowledge. Both were useful to this study in order to discover how user mental models compare to a more advanced model, as well as to see how much user mental models influence their semantic knowledge.

Research on individual differences of personality in user security is a rapidly developing field. Some research studies have found that certain individuals with specific personality traits are more likely to engage in security behaviors than others. For example, Shropshire, Warkentin, and Sharma (2015) found that conscientiousness and agreeableness are good predictors of information security behavior in regard to security software use. This study also measures how the Big Five Personality traits interact with security behaviors.

Methods

Participants

Participants were undergraduate students at San José State University that came to a lab to complete all the tasks of the study and received course credit for their participation. The sample size was N = 194. The sample size consisted of 66 males and 127 females with 1 individual not indicating their gender identity. The average age of the participants was 18 with a standard deviation of 1.

Materials

Card sorting knowledge measure. Participant cybersecurity knowledge was measured using a card sort. Card sorting was used to understand how users organize information, as well as the richness and accuracy of that knowledge. Card sorting was also used to measure the accuracy and depth of knowledge that users have of Internet security. The terms used for this card sort came from using a culmination of various articles.

The terms selected were terms that most frequently appeared in literature and were the most highly recommended from security experts. The Department of Homeland Security (2018), Get Safe Online (Get Safe Online, 2018), and the articles “152 simple steps to stay safe online: security advice for non-tech savvy users” (Reeder, Ion, Consolvo, 2017) and “Current Trend of End Users’ Behaviors Towards Security Mechanisms” were used to create the card sort terms (Hausawi, 2016). The card sorting was quantified by comparing participant card sorts to an advanced card sort. There were 57 cards or terms, each with one concept from a list of protective and non-protective behaviors. The advanced card sort was based on the advice given by Reeder, Ion, and Consolvo (2017). The card sort was a guided card sort with *threats* and *protection* being the two labels that were provided. The labels were developed from the terms that were acquired from the previously listed articles in this paragraph, generating a set of both positive and negative terms. This study investigated whether participants could correctly distinguish between the good terms that are beneficial to their online security and the bad terms that are harmful to their system security. Participants were instructed to place the terms that they believed were harmful to their online security into the *threats* pile, and the terms that were beneficial to their online security into the *protection* pile.

Semantic knowledge test. As a second measure of participant knowledge, a series of 16 questions was presented to assess the semantic knowledge of each participant. 14 multiple choice questions that had two questions with six options, five questions with five options, three questions with three options, and four questions with four options were used. The 14 multiple choice questions were derived from the Pew Research Center's cyber security quiz (Olmstead & Smith, 2017). Two multiple choice questions with four options each were taken from Microsoft's cybersecurity IQ quiz (Microsoft, 2017). Combined there were a total of 16 questions.

Confidence. User confidence was measured with two questions asked after the card sort task:

1. On a scale of 1-5, how confident are you in the accuracy of your card sort? The scale ranged from 1 (*not very confident*) to 5 (*very confident*).
2. If given the chance would you want to resort them? This question was dichotomous, with participants responding either 1 (*yes*) or 2 (*no*).

SeBIS survey. Intention to engage in security behaviors was measured by using Egelman and Peer's Security Behaviors Intentions Scale (2015). The survey had 16 questions and asked users about their attitudes toward security behaviors. The measure used for this study had two subscales for security behaviors instead of the original four subscales used in the Egelman and Peer study. One measure was cyber hygiene and the other measure was threat response. The rule used for this study for classifying each category was that if the question asked how frequently an individual took proactive measures to maintain their security, it was classified as a cyber-hygiene behavior; if it asked about responding to a possible threat, it was classified as threat response. The survey used a five-point Likert-type scale and had categories of threats. The scales measured attitudes toward choosing passwords, device securement, staying up-to-date, and proactive awareness (Egelman 2015). Items were measured with Likert scales and used statements such as, "I use a password/passcode to unlock my laptop or tablet" (p. 5). The anchors used for the study were 1 (*never*), 2 (*rarely*), 3 (*sometimes*), 4 (*often*), and 5 (*always*) (Egelman & Peer 2015). As used in the original study, the Cronbach's alpha calculated was .801 for all of the sub-scales, as well as good discriminant validity between privacy concerns of users and security behaviors (Egelman & Peer, 2015).

Big five personality inventory. Participants completed John and Srivastava's Big Five Personality Inventory (John & Srivastava, 1999). The inventory contained 44 items and measures an individual on the Big Five Factors of personality. Each of the factors are divided into personality characteristics. This research used the Big Five Personality Inventory to observe if there are any interaction effects between personality, knowledge, and behavior.

Results

Multiple Regression Model

Two multiple regression analyses were conducted to test the hypothesis that end-user knowledge would predict intent to engage in security behaviors. First, a multiple regression test was used to see how well card sorting and semantic knowledge quiz scores predicted cyber hygiene behavior scores. The multiple regression model was not significant, $R^2 = .001$, $F(2, 162) = .118$, $p = .889$. Next, a multiple regression test was used to see how well card sorting and semantic knowledge quiz scores predicted threat response behavior scores. The results for card sorting and semantic knowledge scores combined on threat response behaviors was not significant, $R^2 = .02$, $F(2,179) = 2.18$, $p = .116$.

Correlational Analysis

To supplement the multiple regression analysis, correlations among study variables were computed (see Table 1). The sample size varied because of missing data. A total of 88 participants did not complete all the tasks thoroughly. For the card sorting measure data, three participants were missing. For cyber hygiene behaviors, data 26 participants were missing. For threat response behaviors data, nine participants were missing. A total of 39 left one or more items blank on the personality inventory. These participants' data was missing because they left questions on the survey and personality inventory blank. The three participants for the card sort did not finish their card sort. As a result, participants that had missing data were not included in the analysis for the aforementioned variables. The correlational analysis revealed a positive correlation between cyber hygiene behaviors and threat response behaviors (see Table 1). Additionally, positive correlations were found between openness and extraversion, openness and agreeableness, openness and conscientiousness, conscientiousness and agreeableness. Negative correlations were found between the semantic knowledge quiz and neuroticism, neuroticism and extraversion, neuroticism and agreeableness, neuroticism and conscientiousness. Neuroticism was defined by John and Srivastava (1999) as an individual that has personality facets related to anxiety, shyness, and impulsiveness. There were no significant effects for confidence (M = 3.52, SD = .77).

Table 1

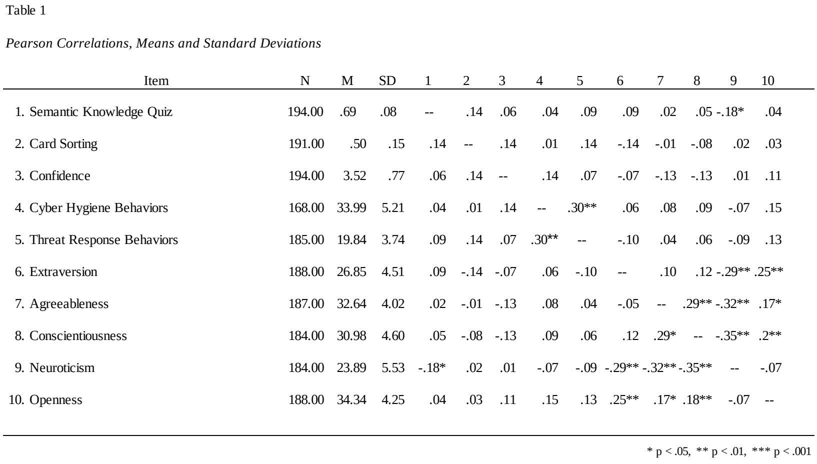


Table 1

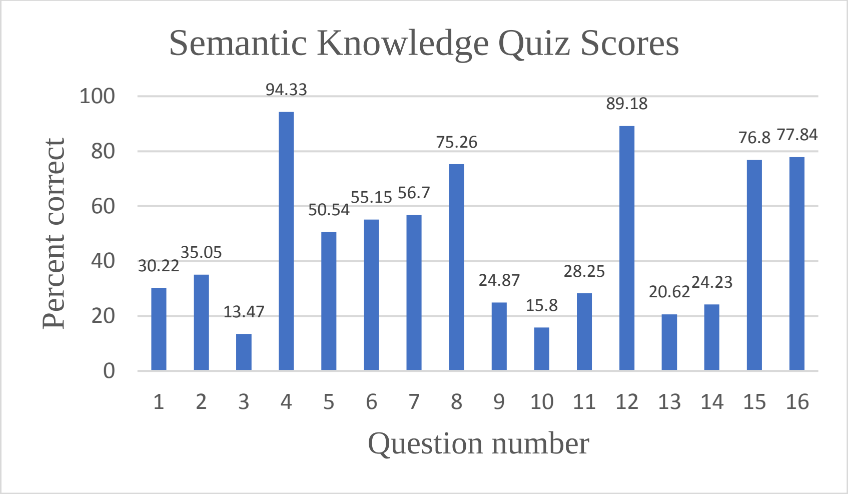
Pearson Correlations, Means and Standard Deviations

Item	N	M	SD	1	2	3	4	5	6	7	8	9	10
1. Semantic Knowledge Quiz	194.00	.69	.08	--	.14	.06	.04	.09	.09	.02	.05	-.18*	.04
2. Card Sorting	191.00	.50	.15	.14	--	.14	.01	.14	-.14	-.01	-.08	.02	.03
3. Confidence	194.00	3.52	.77	.06	.14	--	.14	.07	-.07	-.13	-.13	.01	.11
4. Cyber Hygiene Behaviors	168.00	33.99	5.21	.04	.01	.14	--	.30**	.06	.08	.09	-.07	.15
5. Threat Response Behaviors	185.00	19.84	3.74	.09	.14	.07	.30**	--	-.10	.04	.06	-.09	.13
6. Extraversion	188.00	26.85	4.51	.09	-.14	-.07	.06	-.10	--	.10	.12	-.29**	.25**
7. Agreeableness	187.00	32.64	4.02	.02	-.01	-.13	.08	.04	-.05	--	.29**	-.32**	.17*
8. Conscientiousness	184.00	30.98	4.60	.05	-.08	-.13	.09	.06	.12	.29*	--	-.35**	.2**
9. Neuroticism	184.00	23.89	5.53	-.18*	.02	.01	-.07	-.09	-.29**	-.32**	-.35**	--	-.07
10. Openness	188.00	34.34	4.25	.04	.03	.11	.15	.13	.25**	.17*	.18**	-.07	--

* p < .05, ** p < .01, *** p < .001

To investigate the properties of the semantic knowledge quiz, an item analysis was conducted (see Figure 1).

Figure 1. Average percent correct per question



For questions four, eight, 12, 15, and 16, over 75 percent of participants gave the correct answer. These questions account for five out of a total of 16 questions asked. This suggests that the majority of participants could easily answer approximately a third of the items on the quiz (M = .69, SD = .08).

Discussion

There are several possible explanations as to why the multiple regression failed to achieve significance. The first explanation relates to the measures that were developed for the study from other materials. Some questions on the semantic knowledge quiz might have been too easy; as a result, the semantic knowledge of participants might not have been truly represented. For example, one question asked what it is called when one uses stolen information for ransom, and the correct option included the term ransomware. Participants might have been more prone to pick ransomware because it shares the same word with the question. This is a limitation involved in developing a new measure of cybersecurity knowledge, which is a domain that changes very rapidly. In future research, this measure should be refined with a more challenging knowledge test.

Despite the limitations, there were a few correlations found in the study. There was a strong correlation between cyber hygiene and threat response behaviors. On the surface, this correlation may suggest that there is little difference between the two types of items on the survey. Cyber hygiene and threat response may reflect one construct, or the measure used in the study may not adequately distinguish between these two concepts. Another explanation is that these may be independent factors with a relationship among them that is yet to be explained. It also makes sense that individuals who take more proactive steps to secure themselves will also be more willing to engage in threat response.

There was a significant negative correlation between neuroticism and semantic knowledge quiz scores. This could be because individuals that are neurotic tend to be more anxious and compulsive (Costa & MacCrae, 1992). As a result of this, the more neurotic an individual is, the less Internet secure they might be because of their anxiety, which might cause them to ignore security alerts or Internet security information because it increases their anxiety. On the other hand, an individual who is neurotic might be more Internet secure because they are motivated to learn more about Internet security to ease their anxiety.

Many of the personality traits correlated with each other. The correlations observed in this study generally reflect what other studies have found. For example, a meta-analysis conducted on the Big-Five personality traits showed that neuroticism is correlated to conscientiousness, which is the same correlation that was found in this study (Van der Linden, te Nijenhuis, & Bakker, 2010).

Conclusion

This study shows that there is a relationship between neuroticism and knowledge about cyber security. This study also shows that there is more to be investigated between cyber hygiene and threat response behaviors in order to see exactly how these variables are related. Based on the results of this study, one could infer that an individual that scores high for neuroticism would be less cyber secure. On the other hand, an individual that is low in terms of neuroticism would be more likely to be cyber secure. End-user behavior is an important issue in cyber security, and it is crucial to continue conducting research in this field to help create a more secure internet for all.

References

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38,* 304–312. Retrieved from http://www.sciencedirect.com/science/article/pii/S0747563214003331

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48,* 51–61. Retrieved from http://www.sciencedirect.com/science/article/pii/S0747563215000539

Costa, P. T., & MacCrae, R. R. (1992). Revised NEO personality inventory (NEO PI-R) and NEO five-factor inventory (NEO-FFI): Professional manual. Psychological Assessment Resources, Incorporated.

Department of Homeland Security. (n.d.). Retrieved from https://www.us-cert.gov/security-publications

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5257–5261. ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2858265

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873–2882. ACM. Retrieved from: https://blues.cs.berkeley.edu/blog/2015/01/21/scaling-the-security-wall-developing-a-security-behavior-intentions-scale-sebis-chi-15/

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404807000363

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983-988.

Gentner, D., & Stevens, A. L. (2014). *Mental models*. Psychology Press.

Get Safe Online. (n.d.). Retrieved from https://www.getsafeonline.org/protecting-your-computer/physical-security2/

Hausawi, Y. M. (2016). Current Trend of End-Users' Behaviors Towards Security Mechanisms (pp. 140–151). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-39381-0_14

Good Cyber Hygiene. (n.d.). Retrieved from https://won.norton.com:80/internetsecurity-how-to-good-cyber-hygiene.html

Gutzwiller, R., M. Hunt, S., & S. Lange, D. (2016). *Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts*. https://doi.org/10.1109/COGSIMA.2016.7497780

Ianelli, N., & Hackworth, A. (2005). Botnets as a vehicle for online crime. *Forensic Computer Science IJoFCS*, *19*. Retrieved from https://www.researchgate.net/profile/Chris_Chatwin/publication/234151501_Extracting_Evidences_from_Filesystem_Activity_Using_Bayesian_Network/links/545d66930cf295b5615e6c6b.pdf#page=21

John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of Personality: Theory and Research* (Vol. 2, pp. 102–138). New York: Guilford Press.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289-296.

Microsoft. (2017). Test Your Internet Security IQ. Retrieved from http://go.microsoft.com/?linkid=9713967

Olmstead, K. & A. Smith. What Americans Know About Cybersecurity. (2017). Retrieved from http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Patterson, K., Nestor, P. J., & Rogers, T. T. (2007). Where do you know what you know? The representation of semantic knowledge in the human brain. *Nature Reviews Neuroscience*, *8*(12), 976.

Pelgrin, W. (2014). A Model For Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership. In Melissa E. Hathaway (Ed.), *Best Practices in Computer Network Defense: Incident Detection and Response* (pp. 107-117). Amsterdam: IOS Press.

Pesante, L. (2008). Introduction to information security. *Carnegie Mellon University*. Retrieved from.

Reeder, R., Ion, I., & Consolvo, S. (2017). 152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users. *IEEE Security & Privacy*. Advance online publication. Retrieved from https://ieeexplore.ieee.org/document/7950834/

Sheppard, B., Crannell, M., & Moulton, J. (2013). Cyber first aid: proactive risk management and decision-making. *Environment Systems and Decisions*, *33*(4), 530–535. Retrieved from http://link.springer.com/article/10.1007/s10669-013-9474-1

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191.

Van der Linden, D., te Nijenhuis, J., & Bakker, A. B. (2010). The general factor of personality: A meta-analysis of Big Five intercorrelations and a criterion-related validity study. *Journal of research in personality*, *44*(3), 315-327.