Investigation of Attitudes Towards Security Behaviors

SJSU SAN JOSÉ STATE UNIVERSITY

Daniel Kelley, David Schuster, Katherine Quinto, Christopher Conetta
San José State Univesity, Department of Psychology

VECTR Lab

Introduction

- 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, even Antarctica (Pesante, 2008). With the recent advancements in technology, many users and companies have begun storing sensitive information on the internet.

- As a result, attacks from hackers have become more frequent. The culprit for most of these security breaches can be traced back to human error and a lack of knowledge (Pelgrin, 2014). Symantec's 2013 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).

- Research examining this problem isn't as prolific, as the research examining technological designs to help solve the problem of human error. Little research has been done on how a user's knowledge relates to responding to threats online, and very little research has observed how personality affects user knowledge and security behaviors online. This study intends to take a closer look into these areas.

Security Behaviors

- There are two types of security behaviors cyber hygiene and threat response. Cyber hygiene is proactively minimizing vulnerabilities to maintain system security. 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 for viruses, backing up data, updating, and using strong passwords are examples of cyber hygiene behaviors (Symantec, 2017).

- 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.

- This study measures how knowledge, and individual differences impacts an individual's engagement in security behaviors.

Methods

- Participants were undergraduate students at San José State University and consisted of 66 males, and 127 females with 1 individual leaving this section blank. The average age of participants was 18.

- Card sorting was 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.

- Confidence was measured by asking participants how confident were they in their card sort, 1 (not very confident), 5 (very confident) and if given the chance would they resort them 1(yes) and 2 (no).

- As a second measure of knowledge, 16 multiple choice questions was presented to assess the semantic knowledge of each participant. The 16 questions were derived from the Pew Research Center's (2017) cybersecurity quiz and Microsoft's cybersecurity quiz (2017).

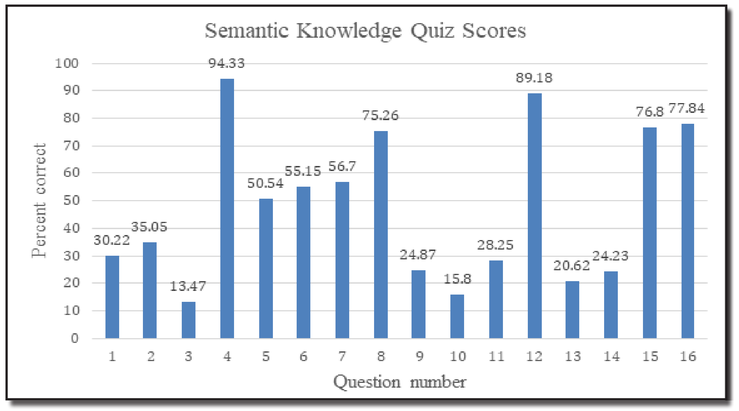
- Engagement in security behaviors was measured by using Egelman and Peer's Security Behaviors Intentions Scale (2015). The survey had 16 questions and asked users how frequently do they engage in security behaviors.1 being never and 5 being always.

- Participants completed John and Srivastava's Big Five Personality Inventory (John & Srivastava, 1999). This research used the Big Five Personality Inventory to observe if there are any interaction effects between personality, knowledge, and behavior.

Results

- Two multiple regression analyses were conducted to test the hypothesis that end user knowledge would predict frequency in engagement of security behaviors. The multiple regression model was not significant for both measures of knowledge on predicting security behaviors scores.

- To supplement the multiple regression analysis, correlations among study variables were computed. The correlational analysis showed that there were correlations between personality, gender, semantic knowledge quiz scores and security behaviors.



Discussion

- There was a correlation between cyber hygiene and threat response behaviors. These behaviors may be independent factors with a relationship among them that is yet to be explained.

- There were many significant correlations with gender. On average males tended to be more confident, have higher semantic knowledge quiz scores, engage in more threat response behaviors, and were less neurotic than female participants. These findings show that there are some gender differences in relations to cyber security between men and women. This might be because of societal gender roles, in which men are viewed as protectors, therefore take it upon themselves to learn more about cybersecurity.

- Individuals that are high on neuroticim tend to perform worse on semantic knowledge quiz scores, however those that are low on neuroticis tend to score higher. This could affect a company's decision for hirability.

References

- Pelgrin, W. (2014). A Model For Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership. Pesante, L. (2008). Introduction to information security. Carnegie Mellon University. Retrieved March, 10, 2013. Good Cyber Hygiene. (n.d.). Microsoft. (2017). Test Your Internet Security IQ. 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(pp. 2873–2882). ACM. 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.