Leah Drew
ENGL 211C
9/11/19

Part 2: Research Synthesis (First Draft)

The study "Personality as a Predictor of Cybersecurity Behavior" was aimed at finding links between the "Big Five" personality traits and cybersecurity behavior. The "Big Five" are considered in psychology to be one of the most accurate ways of measuring personality, and these traits are conscientiousness, openness, agreeableness, neuroticism, and extraversion (Shappie, Dawson, & Debb, 2019, p. 2). The study makes a distinction between intended and actual cybersecurity behavior, as people often don't act according to their intentions or beliefs in the moment. The average user may intend to be secure in their actions, but may still do things that are risky due to laziness, oversight, or ignorance of the best online practices..

The study found that conscientiousness, openness, and agreeableness were the main influencers of secure online behavior, with conscientiousness affecting the most. This is likely because conscientiousness is also correlated with self-efficacy. These findings are consistent with previous studies that concluded that conscientiousness is the main factor behind secure online behavior, but they also suggest that openness is a predictor as well. Although agreeableness seemed significant, in the hierarchical analysis it was not, meaning that this topic needs further testing. Because the sample was made up of college students, the study notes that the results may be skewed in favor of the younger population. Cybersecurity is a very broad topic that encompasses many variables and factors, and this study only tested a few of these behaviors, which means that neuroticism and extraversion might be correlated with other variables not tested for. The authors suggest that subsequent studies should develop a more comprehensive model to gain a better understanding. The study concludes that businesses could encourage more secure behavior by taking steps to raise the self-efficacy of users because of its relationship with conscientiousness and openness (Shappie, Dawson, & Debb, 2019).

Leah Drew
ENGL 211C
9/11/19

In an article published by Infosec, Penny Hoelscher agrees that the Big Five personality traits are useful tools for managing cybersecurity. People known as "black hat" hackers, who are classic cybercriminals, have a high amounts of openness because they like being challenged (2019). Hoelcher suggests that businesses should use decoy software that is difficult to hack into in order to catch cybercriminals without risking their information. "Gray hat" hackers, who are best defined as hackers who aren't looking for personal gain but still act unethically, tend to have higher amounts of neuroticism. According to Hoelcher, in order to mitigate damage from gray hats, "certain language use…can identify neurotic-related text, which could help identify scams in much the same way email filters strip spam from a user's inbox" (2019).

In her article "The Psychology of Cyberthreats" Stephanie Pappas writes that while many businesses may try to manage cybersecurity by imposing restrictions on users, too much restriction results in users taking risky shortcuts. For example, requiring long, complex passwords that are difficult to remember may result in users writing their passwords down and keeping them somewhere hackers could access (2019). She suggests that the best way to approach issues like these is not to impose restrictions, but to also give specific recommendations on how to easily meet these requirements, such as using mnemonics.

The rise of smart devices has made cybersecurity increasingly more difficult to manage. Many users expect that because their devices are "smart" that they're automatically more secure, which leads to them making more risky choices (Pappas, 2019). Few people realize that a device that includes voice recognition software could easily be hacked to record conversations. A hacked smart car could even be used to cause a crash, endangering people's lives. Devices that are designed in this way are constantly recording and storing personal data, and the companies that market these devices don't go into detail about security risks. According to Pappas, "the

marketing of these devices downplays security and privacy concerns," meaning that these companies rely on an illusion of security to advertise their business (2019). The author suggests that warning users about these risks and stressing the importance of secure behavior might help reduce the impact of this misconception.

Works Cited

Hoelscher, P. (2019, February 5). The Psychological Profile of a Hacker With Emphasis on Security Awareness. Retrieved from https://resources.infosecinstitute.com/the-psychological-profile-of-a-hacker-with-emphasis-on-security-awareness/

Pappas, S. (2019, February). The psychology of cyberthreats. Monitor on Psychology. Retrieved from https://www.apa.org/monitor/2019/02/cyberthreats

Shappie, A., Dawson, C., & Debb, S. (2019). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media Culture*, Psychology of Popular Media Culture, 2019. Retrieved September 9, 2019, from https://psycnet.apa.org/fulltext/2019-28368-001.pdf.