Leah Drew
9/20/19
ENGL 211C

Part 2: Research Synthesis

According to “The Human Side of Cybercrime” by Mitchell Waldrop, underground cybercriminal networks are extremely sophisticated and structured in a way that makes them hard to crack. Networks operate similarly to a business; many even have a customer service wing. The fact that most members of these networks construct an alias to use online makes it difficult to identify and prosecute them compared to traditional criminal rings (Waldrop, 2016, p. 166-167).

In “Leveraging Behavioral Science to Mitigate Security Risk,” Pfleeger and Caputo write about the aspects of behavior science that are exploited by cybercriminals and the strategies that could be used to reduce the impact of cyberattacks. Among these findings is the “identifiable victim” effect, in which humans are more likely to offer help to a specific, identifiable victim, as opposed to something more abstract like a business (2012, p. 604). This also means that users are more secure in their behavior when there are personal consequences involved. “Control bias” is a cognitive bias in which people think that they have more control over situations than they actually do, which means that users are less inclined to take protective measures like running virus scans. The bystander effect can also be exploited by cybercriminals and leaves holes in a security system. When a cyber-event occurs, users feel like they don’t need to take action because there are other people able to help. “Affect heuristic” is another concept that can be exploited by cybercriminals; when people are influenced to have a good feeling about a situation, they perceive it as being low-risk, so they’re more inclined to trust it (Pfleeger & Caputo, 2012, p. 605-606).

According to the article, businesses can counter these phenomena with measures that influence the perception of users. The identifiable victim effect can be negated by imposing more personal consequences on users. The bystander effect can be negated by redesigning the system to reward and encourage users who take action instead of assuming someone else will, and affect heuristic can be influenced by designing the system in a way that requires a more critical approach and rewarding employees who take the time to assess the risk involved in a situation (Pfleeger & Caputo, 2012, p. 604-606).

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).

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).

These are not the only ways attackers can take advantage of human perception. According to Cybenko, Giani, and Thompson, hackers are known to intentionally manipulate users through a process known as “cognitive hacking” (2002, p. 50). One of the easiest ways to achieve this is through misinformation—for example, defacing or “spoofing” a legitimate website in order to communicate something that’s not true. The authors suggest several methods of countering these kinds of attacks, including collaborative filtering methods and using linguistic analysis to determine whether or not information is legitimate (Cybenko, Giani & Thompson, 2002, p. 55).

Leah Drew
9/20/19
ENGL 211C

According to “The Human Side of Cybercrime,” it’s important to understand the behavioral science behind the actions of both cybercriminals and their victims (Waldrop, 2016, p. 164). According to the article, cybercriminals prey on employees of a business by exploiting their trust in authority and the fact that they’re most likely preoccupied. Generally, when an employee gets an official-looking email from someone posing as a trusted source, they are inclined to follow the instructions in the email, which leaves a gaping security hole attackers can use to infect networks with viruses. Businesses tend to counteract this by tightening restrictions on employees through more complex authentication. However, the tighter the restrictions, the more likely employees are to search for ways of getting around them, which attackers will also take advantage of (Waldrop, 2016, p. 165).

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.

Leah Drew
9/20/19
ENGL 211C

Works Cited

Cybenko, G., Giani, A., & Thompson, P. (2002). Cognitive hacking: A battle for the mind. *Computer, 35*(8), 50-56. Retrieved from https://ieeexplore.ieee.org/document/1023788/authors#authors

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

Pfleeger, S., & Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. Retrieved from https://www.sciencedirect.com/search/advanced?docId=10.1016%2Fj.cose.2011.12.010

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.

Waldrop, M. M. (2016). The human side of CYBERCRIME. *Nature, 533*(7602), 164-167. Retrieved from http://proxy.lib.odu.edu/login?url=https://search.proquest.com/docview/1789281700?accountid=12967