Leah Drew
9/27/2019
ENGL 211C

Part 3: Argument/Refutation/Critique

The purpose of this paper was to examine the relationship between cybersecurity and psychology, or more specifically, what aspects of psychology are risk factors for cybersecurity events. In my research I found that several factors influence cybersecurity: the Big Five personality traits, cognitive biases and heuristics, misinformation, and the exploitation of flawed password security. In the field of cybersecurity, most writing is based on finding problems and developing solutions. The aim in the end is to make systems more secure; the solution is given more weight than the problem, while someone who studies psychology would consider the opposite true. Cybersecurity is still an emerging field, and studying the intersection of it and psychology is even newer. Because of this, there is some disconnect in the way scholars that study either topic write about this intersection.

The four scholarly articles that I found were a mixture of original research and synthesis of other research. The studies that I read were more objective and focused on psychology, and they used more psychological terms than the articles that were focused on cybersecurity. These articles were clearly meant for psychologists who were already familiar with this style of writing. Secondary sources used more technical jargon in order to apply the research to cybersecurity and explain how the information provided could be used to the advantage of specialists in the field. Because these articles gave recommendations, there was more room for bias and subjective language.

"The Psychological Profile of a Hacker With Emphasis on Security Awareness" and "The Psychology of Cyberthreats" are both popular sources. The first one is published by Infosec, a website that provides cybersecurity training and certifications for professionals. The language

used in this article is easier for non-experts to read and understand. However, it seemed like it was intended for people who had some interest in pursuing a career in cybersecurity, so it was structured more similarly to a crash course than an overview for a general audience. The second article is published by the American Psychological Association in their magazine "Monitor on Psychology." This article was more informal and clearly meant for a general audience, and the information given related more to what the average user could do to be more secure online.

While articles rarely directly contradicted each other, some authors seemed to interpret the same concepts differently than others. "Leveraging Behavior Science to Mitigate Cybersecurity Risk" cited several studies that researched the effectiveness of graphical passwords and came to the conclusion that they were easier for users to remember, and could be used as a solution to password security. Meanwhile, "The Psychology of Cyberthreats" cited several studies on the same topic with similarly inconclusive results, and came to the conclusion that using graphical passwords would not fix the issue of users being insecure with their passwords. Because "The Psychology of Cyberthreats" was published in 2019, it's possible that this conclusion is based on more current evidence, making it a more reliable source instead of the contradiction being due to the author's bias.