Adrian N
an9905@rit.edu
CSEC.468.01
Risk Management for Information Security
Project Group – Social Engineering

Social Engineering cyberattacks are a kind of psychological attack that exploits weaknesses in human cognitive functions. A good defense against social engineering attacks requires a deeper understanding of what aspects of human cognition are exploited by these attacks, why humans are susceptible to these kinds of attacks, and how we can minimize or at least mitigate their damage. In the paper titled, “Human Cognition Through the Lens of Social Engineering Cyberattacks” human cognition is reviewed through the lens of social engineering cyberattacks. The paper then proposes an extended framework of human cognitive functions to accommodate social engineering cyberattacks. In section 2.2 of the paper, it discusses what will be in primary focus, the three short-term factors: workload, stress, and vigilance. In the paper it states, “These attacks often leverage behavioral and cultural constructs to manipulate a victim into making a decision based on satisfaction (gratification), rather than based on the best result(optimization). For example, one behavioral construct is that most individuals would trade privacy for convenience, or bargain release of information for a reward”. This short excerpt sums up the victim cognition through the lens of social engineering cyberattacks as it describes how the attacker goes at his victim using psychological warfare of sorts versus other attacks in the cyber world that are much more technical. In all, this paper helps apply to some aspects of risk management because this gives us a whole new perspective on how to mitigate risks, in regard to social engineering. This gives a new definition to social engineering as this paper helped explore the science behind these attacks, leaving all the technical matters behind. This helped us recognize the psychological process behind the attacks and how these victims react. In terms of our project, this paper helps give way for a potential section of the paper in which we go in depth about social engineering in a broad attacking sense, and how these psychological factors go into play. We could also speak about this when mentioning a potential defense plan, or training for potential employees/playbook. Additionally, it is a pretty in-depth paper that can be cited in our project to highlight the science behind manipulating emotions.

References

Montañez, R., Golob, E., & Xu, S. (1AD, January 1). *Human cognition through the lens of social engineering cyberattacks*. Frontiers. Retrieved October 8, 2021, from https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01755/full.