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

The idea of having a good cyber security protection program remains at the forefront of many organizations' information and communication technology strategy. Most of the time however, these organizations are not as secure as they think they are. These organizations usually fall to simple tactics in comparison to others like social engineering attacks. The lack of social engineering awareness is a huge concern in the context of human cyber security risks. The paper titled, "Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues" helps us understand how modern day, 2019, organizations are dealing with social engineering and what is working and what is not. In the paper it states, "With innovative and interactive education, training, and awareness programs, corporations seek to prepare their staff with the most current prevention techniques to evade social engineering threats. The measures undertaken are comprised of training materials, policy and regulatory frameworks, and training on the safety measures to be taken before and after attacks." This is a perfect example of what we want to know in terms of how current day companies are protecting themselves against social engineering. This sums up the fact that there is no perfect security system to counter social engineering threats that these organizations are subjected to but training the human employee. This is most likely the reason why companies choose to invest money into this type of training versus developing technical tools to contain the possible damages caused by these attacks. Another thing we learned is that it is better if the security training varies according to the needs of the business, market pressures, business modernization, prerequisites, and budget available to the firm. However, we must keep in mind that once these attackers are aware of the measures taken by these organizations, they can always develop new techniques that staff are unfamiliar with. In all, this paper helps apply to all aspects of risk management because this tells us the steps real big organizations do to mitigate risks, in regard to social engineering. In terms of our project, this paper helps give way for the potential end of the paper in which we will discuss how a company should defend themselves against social engineering attacks, and how different companies with different potential investments could plan. On top of this it is a pretty in depth paper that can be cited in our project to highlight real life modern day examples;

References

Skinner, G., & Aldawood, H. (n.d.). *(PDF) reviewing cyber security social engineering training ...* Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Retrieved October 1, 2021, from https://www.researchgate.net/publication/331848369_Reviewing_Cyber_Security_Social_Engineering_Training_and_Awareness_Programs-Pitfalls_and_Ongoing_Issues.