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

In an organization, technical vulnerability is not only the cause of cyber-attack. The "Human" is the most vulnerable in the cyber security chain. In recent years humans are being manipulated to extract confidential information and the technique is so-called as "Social Engineering". Social Engineering is a form of art employed by cybercriminals exploiting the psychology of people to gain access or divulge confidential information. Social engineering attacks are not detected easily by the most advanced security software and hardware as it manipulates the human physiology, not the implemented security mechanism. Social engineering attacks exploit human vulnerabilities to achieve sensitive information and can happen in one or more steps. Social engineers use the common pattern to achieve the desired objective, which typically involves four phases. In the paper titled, "Systematic Review on Social Engineering: Hacking by Manipulating Humans" it states, "1) Research: Gathering information about the target; 2) Hook: Maintaining the relationship with the target: 3) Play: Manipulating the information and executing the attack; 4) Exit:" This quote describes the four phases social engineers do in terms of manipulating humans to achieve their final goal. This paper also speaks on the methods of information gathering in which require technical skills while others might require the sot skills of manipulating human psychology. This connects to my paper as my group, and I are focusing on social engineering for our final project. On top of this my specific section of the paper is about the psychology behind these social engineering attacks. This paper can be used as a reference as it helps paint a picture of how social engineering attack work in general and how these engineers gather information on certain targets in which they then intend to use in order to manipulate their victim. This will help relate to the paper I will write as I aim to speak about how the attacker analyzes the information gathered and develops an action plan to approach the target. After this the social engineer looks for some of the target's greediness, lack of moral duty, awareness level about social engineering and weak policy against attacks.

References

Sekhar Bhusal, C. (2021). Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, *12*(01), 104–114. https://doi.org/10.4236/jis.2021.121005