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

Social Engineering can be defined as a process by which an attacker, follows various manipulation techniques to obtain sensitive or private information from the victim along trying to access physical or digital assets of the victim. For us to understand social engineering, we must first understand the different attack scenarios that may occur in a regular workday. In the paper titled, “Understanding and Deciphering of Social Engineering Attack Scenarios” we can analyze how social engineering attacks pattern from the data gathered. There are five phases according to the paper which are: Gather, Medium, Scenario, Persuasion, and Result. Phase 1 touches on gathering information and generating game storyline. In this phase, the attacker will collect information about the victim including cell phone numbers, account information, email, friends etc. This leads to the storyline creation in which the attacker will design a scenario tailored for the victim which seems real. The next phase is where they will contact the victim aka the medium phase. They will for example attack by calling, by spoofing to have the number in the same area to look more real or from a government department. Next, the attacker will enter phase 3 where they will execute the pre-made tactic. This is where the attacker will explain the cause for call/email with the victim. This is where most of the convincing occurs, and uniqueness of social engineering comes into play as every storyline is different. Then the attacker will enter the persuasion phase by taking advantage of psychology weaknesses. This is where the attacker will attack/target the feelings or emotions of the victim to get the required actions to be performed. Lastly, the attacker will enter phase 5 which is when they achieve their goal. In this phase the social engineer will need to finish the deal and requires the victim to transfer either information or money or install a file which can be used to get access using the backdoor. This paper helps put social engineering scenarios into a playbook of sorts as it describes exactly how these attacks operate by dividing it up into five phases. If we know all the phases, we can help defend against social engineering attacks better, and keep organizations safe. This paper also segues into how I can conduct further research by doing in depth analyses of the different phases. I can deep dive into how phase four works, and how the social engineer will manipulate the victim and how they trigger the victims’ emotions, or weaknesses to receive what they sought after.

References

Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., & Wei, Z. (2021, May 2). *Understanding and deciphering of social engineering attack scenarios*. Wiley Online Library. Retrieved September 24, 2021, from https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.161.