

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

Social engineering is an attack vector that manipulates victims into giving up confidential information or performing an action that breaks usual security standards. With the success rate of these types of cyber attacks, it is vital we understand and acknowledge the information out there. The unorthodox style of attack is what makes these engineers so effective, so if one were to understand the science behind the attack they would be much more prepared and safe which is the ultimate goal in the computer security workspace. The paper I chose to read speaks upon the psychological triggers behind social engineering. It speaks on the fact that social engineering depends on the victim's logical thinking toward the information given by the cybercriminal and how well the victim can be persuaded. It also speaks on the 2014 SONY pictures hack which is the main reason I chose this article, in order to understand how psychology played a role in a big breach. In the paper it states, "On November 24, 2014, Sony Pictures had discovered they were hacked (VanDerWerff & Lee, 2015). The attackers took terabytes of private data, deleted original copies, and left messages threatening to release the stolen information if Sony did not comply with the attackers' demands... The GOP first scouted LinkedIn for system administrator employees at Sony. After finding system administrator employees, the GOP sent spear phishing emails to those employees. The spear phishing emails appeared to be from Apple and demanded the victims to verify their Apple ID credentials because of suspected unauthorized activity. The victims gave away their credentials due to the psychological triggers of authority and diffusion of responsibility." This quote really sums up the conflict between SONY and these attackers and how psychological factors played a role in a big hack. This obviously connects with my paper as I chose to deep dive into how psychology is used in social engineering attacks, and how knowing so could help prevent attack efforts. This paper also pertains to Risk Management as a whole, because it shows how a big company like SONY could be vulnerable to simple non-technical attacks like phishing emails etc.

References

Kancherla, J. (2020, April 24). *Motivational and Psychological Triggers in Social Engineering*.
Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3750474