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

With the constant increasing importance of and dependence on IT systems in our daily life, from home devices to work-computers the security of these systems is also rising in priority. The term Social Engineering is used at least in two different contexts – information security and political science. For now, we will focus on the psychological aspect, as we can informally state that it describes a phenomenon where people are influenced into taking a particular action which may be against their own best interest. One of the first steps into a social engineering attack is a technique called baiting. In the paper titled "Social Engineering" it states, "A technique in which the attacker places a 'bait' for the victim to take on their own initiative – the typical example being leaving one or more USB flash drives, containing a malicious executable, in a spot, where the victim is likely to notice them. Then, motivated by curiosity or greed, the victim may take the 'bait' and unwittingly help the attacker's payload cross a trust or security boundary that the attacker himself/herself cannot – for example a physical barrier with adequate access control" (Papazov, 143). This quote shows the concept of baiting. This is the type of social engineering attack where a scammer uses a false promise to lure a victim into a trap which may steal personal and financial information or inflict the system with malware. This pertains to risk management because as an organization social engineering attacks are very prevalent and can cause infinite harm to the organization. This must be mitigated to the best of the organizations ability because it cannot really be mitigated technically, rather through employee training etc. In terms of my paper, I am focusing on the psychology behind social engineering attacks as a whole and this can be used as a reference. This paper talks a little bit of the technical side behind social engineering attacks in terms of steps and the process. This can be applied to my paper in a psychology aspect as the baiting and phishing fall under the psychology behind these social engineering attacks as it is the art of exploiting human emotion rather than technical hacking techniques, to gain access to these systems.

References

Papazov, Y. (n.d.). *Social Engineering*. Retrieved March 7, 2019, from https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-IST-143/EN-IST-143-08.pdf