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

The advancements that have been made in modern day technology have put more pressure on humans in the field who are more and more accessible and reachable. These people's information is out there, whether it be on social platforms or online services that are unable to fully protect said information. Communication systems are some of the most vulnerable as they can be easily attacked through social engineering attacks. These kinds of attacks focus on tricking individuals who work in the field into giving up vital information that the attackers can then use to get into systems or use as blackmail for a ransom. In the paper titled *Advanced Social Engineering Attacks* it states, "One example is the so-called baiting attack: Attackers leave malware-infected storage media in a location where it is likely to be found by future victims. Such "road apples" could, e.g., be a USB drive containing a Trojan horse [48]. Attackers additionally exploit the curiosity of people by adding tempting labels to these road apples (storage media), such as "confidential" or "staff lay-off 2014". This is one example of a social engineering attack called baiting. Although this paper identifies and describes most of the attacks in the socio-technical engineering space, I focused on the specific social engineering attacks such as baiting. Baiting is important as it is somewhat like the first step. This specific type of attack pokes at people's curiosity to trick them into clicking a link that contains some sort of malware via email. The paper also speaks on phishing which is used when an attacker aims for a large user group, like spam. According to these attackers, the ideology is that if enough emails are sent, eventually enough people will be fooled for the attack to be profitable. This was then adapted to be more lucrative into 'spear-phishing' attacks. These are more highly targeted messages that are carried out after some initial data mining. By incorporating this social data, the attacker's success rate skyrocketed. These all apply to risk management as a risk manager must address the possibility of a social engineer breaching the system that they had worked so hard to implement. On top of this, it is one thing to secure a computer using programs or firewalls etc., but one of the hardest things to address is human behavior. This paper has a broad overview of social engineering in general and gives us a basic description of the different social engineering attacks used. Since our paper is about mitigating and/or controlling social engineering risks this paper helps us understand how we should go about things in regards to educating potential workers on how these tactics are used and constantly evolving, as well as potentially testing the workers from time to time to see if they are acting fast and proper.

Reference Page

Krombholz, K. K., Hobel, H. H., Huber, M. H., & Weippl, E. W. (2014, July 17). *Advanced Social Engineering Attacks*. Research Gate. https://www.researchgate.net/publication/267340031_Advanced_social_engineering_attacks