Online Activity #3

Ahsan Syed

[Aksyed2@myseneca.ca](mailto:Aksyed2@myseneca.ca)

Saturday – 22nd July 2017

**What do you think about Social Engineering?**

Social Engineering is a clever hacking strategy that may be used by two types of hackers: the ones that are not very technical or the efficient ones, who like to take shortcuts and get work done ASAP. Overall, I think social engineering is a type of fraud and people should be cautious about it.

**What is social engineering? What human nature/habits does social engineering leverage?**

Social Engineering is lying to manipulate people into exposing information that they otherwise would not provide. Basically, tricking someone to reveal information under false pretenses that is often illegal.

Socail shame, embarrasment, peer pressure, fear, loss of social capital and many more are the human natures that social engineering leverages. Attackers take advantage of their preys social reputation to get what they want. They put their preys in situations, where they wont be able to reject or enforce security on the attacker. These habits humans have, make us vulnerable to dangerous social engineer attacks and we should take the smallest of precautions to be secure.

**What are some common types of social engineering?**

The msost common types of social engineering are as of follows:

Phishing: This is a strategy in which attackers use shortened or embed links that redirect users to suspicious websites in URLs that appear legitimate. This type of attack is usually done to obtain personal information (i.e. usernames, addresses, SIN, contact info). Some phising emails are poorly crafted but the ones that are crafted in a legitimate fashion are hard to distinguish.

Baiting: This is a strategy where attackers promise an item or good for the information the victim provides. For example, a baiter may offer free downloads to some software, music, or movie if the victim provides their login credentials to a certain website.

Pretexting: This is a strategy in which attackers try to build a credible story that leaves little room for doubt on the part of their target. This method is used to access non-sensitive and sensitive information. For example, an attacker acts like an external IT services auditor and manipulates a company’s physical security into letting him into the building.

Quid-Pro-Quo: This is a strategy similar to Baiting but instead of trading goods, attackers tend to exchange services in order for their victime to share classified information.

Tailgating: This is a strategy that attackers tend to use in mid-sized businesses, where they engage in conversations with employees and use this show of familiarity to get passed security. In large companies, this usually doesn’t work as security keys are required at multiple enterances.

**Do you think Social Engineering is an effective hacking method? And why?**

Yes I believe it is an effective hacking method. Regardless of it being a crime most of the time, social engineering is a method hackers tend to use as last resort. Some organziations have the best of best security systems/firewalls which can be really hard to break and the only way to go passed them is by illegally accessing login credentials of one of the employees. This is also handy because it tends to save a lot of time for some attackers as some systems are really hard to break into.

**How to protect us from Social Engineering?**

Few ways to be protected are as follows:

* Don’t open email that are received from untrustable sourses. If you have doubts, contact friends, family, or whoever that might be related to that email topic to verify that email content before opening it.
* On the web, don’t try to be kind and give strangers the benefit of the doubt.
* Keep everything secure. Especially, initial laptop screen.
* Have anti-virus software installed on your PC to protect it from virus scams brought by emails, and other transferable tools.
* Have good understanding of companys privacy policy to know under what circumstances you can and should let a stranger into the building.