University of Regina
Computer Science

Social Engineering in Information Technology

Group Members

Student name	Student number
Bao Cao	200363431
Corey Safinuk	200375142

Progress of the project

In general, our team has completed half of the written components of our project. The outline of our project and our works can be found below. Up to this stage, Corey Safinuk has finished writing component for some backgrounds of social engineering (history and famous social engineers) and two social engineering methods which relate to a technique called “fishing”. Bao Cao has finish writing component for four social engineering technique: Quid Pro Quo, Pretexting, Tailgating and Baiting. For the completion of our project, we may reassess the rest of the outline (the parts that we haven’t done yet) and decide which part will be done by who. When the writing component is done, we will combine our works, reformat it in order to create a complete report. We intent to record our presentation in the form of a two-minute video which will be uploaded on Youtube.

Unfortunately, because of our working schedule, we cannot combine our works for this week assignment. On Sunday March 11, Corey works in the morning until evening and Bao Cao works from the evening until midnight. Therefore, we have to submit our work separately but we will submit the same outline and the progress of our project. The referenced sources will be different since each of us submit our works separately.

Outline

1. History of Social Engineering

- Nowadays social engineering is about information privacy on the Internet. However, the term social engineering appeared in history before the computer era.
- Examples of famous social engineers

2. Common Techniques in Social Engineering (terminologies)

- Phishing: Definition and examples. Personal opinions. Variances of phishing: Vishing and Spear phishing
- Quid Pro Quo: Definition and examples. Personal opinions.
- Pretexting: Definition and examples. Personal opinions.
- Tailgating: Definition and examples. Personal opinions.
- Baiting: Definition and examples. Personal opinions.

3. How to prevent from social engineering attacks

- Phishing
- Qui Pro Quo
- Pretexting
- Tailgating
- Baiting

4. Laws that relate to social engineering

- Canadian laws
- U.S laws
- Other countries

References:

Bisson, David. “5 Social Engineering Attacks to Watch Our For”. The State of Security. Mar 23, 2015. https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Nadeem, M Salman. “Social Engineering: What is pretexting?”. Mailfence. Jan 30, 2018. https://blog.mailfence.com/pretexting/

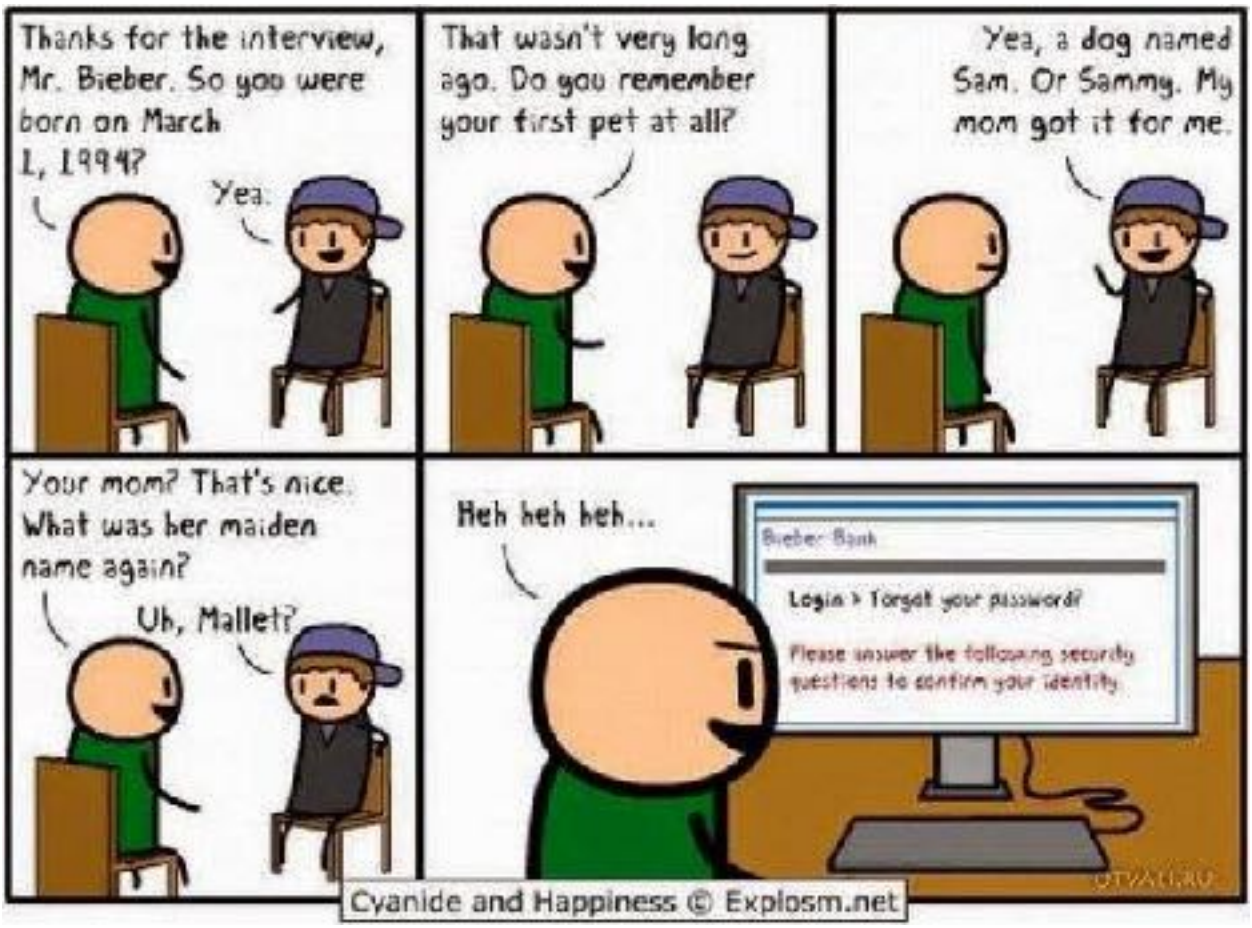
Nadeem, M Salman. “Social Engineering: What is pretexting?”. Mailfence. Jan 30, 2018. https://blog.mailfence.com/what-is-tailgating/

CNN Wire Staff. “Cyberattack in 2008 prompted new Pentagon cyberdefense plan”. CNN. Aug 25, 2010. http://www.cnn.com/2010/TECH/innovation/08/25/pentagon.cyberattack/

Kepes, Ben. “Business Software in the App Age”. Thought Leader, Computerworld. Jan 5, 2016. https://www.computerworld.com/article/3002703/security/some-scary-insights-into-cybersecurity-risks-or-what-happens-when-you-drop-200-usb-sticks-in-public.html

Wang, Christina. “Information Security and Pop Culture: How Real-Life Social Engineering Techniques are Used in Movies and Television”. BetterCloud. March 8, 2016. https://www.bettercloud.com/monitor/information-security-and-pop-culture/

Quid Pro Quo



In Latin, quid pro quo means “something for something”. In social engineering, an attacker who uses quid pro quo promises a benefit (can be a form of a service) in exchange for information.

One of the most common quid pro quo methods involve attackers who impersonate as IT service people. The attackers will call as much number as they can find to offer IT support with the hope that there is a victim who has the same problem and needs help. When the attacker finds his victim, he will pretend helping solve the problem and either ask the victim for personal information or trick them to install malware which requires the victim bypass his anti-virus softwares.

Another way of using quid pro quo which doesn’t require complicated methods such as calling every number to find a victim, the attackers can just simply create a survey and convince victims to share their information in other to win a prize (sometime the prize is really simple such as a pen or a bar of chocolate). This attacking method seems simple and easy to avoid. However, in the modern society where most of us cannot live with out the Internet and social networks, people get used to exchanging their personal information for awards and recognitions, which makes this attack effective.

Reference: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Pretexting

Pretexting is another form of social engineering - probably the form that most people have encountered - where attackers create a fabricated scenario in order to obtain victim's personal information.

Most of the time, attackers impersonate authorities such as police, insurance investigators to make the scenario more serious. One example which came from my landlord's friend is his friend's wife received a call which announced that her husband won a lottery, therefore they needed her husband's phone number. A couple days later, she received a call from her husband's number. However, the other side wasn't her husband but declared himself RCMP officer. The caller announced that her husband had been arrested so in order to bail him out, the wife had to transfer an amount of money into an account number. Fortunately, her husband was sleeping upstairs. Therefore she knew that was fraud and didn't fall for that. There was a time when my former employer received a call announced that there was something wrong with his account so he had to bring his bank card to a specific location in order to get it done. However, he knew the call was just a fraud because the address that the caller required him to go to was a household address.

Another form of pretexting attack is emailing. Attackers will send emails - which are fabricated to make an expression that the emails come from authorized organization such as banks or government organizations - to victims and these emails will require victims enter their login information. This form of pretexting attack and the form of tricking victims on phone are similar

to scamming and quid pro quo. However, pretexting doesn't promise any award or try to get victims click on to something, instead, pretexting attackers build their trust with their victims by impersonating authorities (most of the time, the attackers create fear and urgency which have a huge effect on human in terms of psychology). Once the trust is built, attackers can easily obtain their victims' private data.

Reference: https://blog.mailfence.com/pretexting/

Tailgating

Tailgating or "Piggybacking" is another type of social engineering which is used specifically to get entry to a restricted area secured by electronic access control. The goal of this method is to steal valuable property or information inside that area.

The main factor which makes this method successful is it exploits courtesy. A common scenario is when the attacker disguises himself as a delivery guy and waits in front of the restricted area. When an authorized person gets access into the area, the attacker will follow and ask the person to hold the door for the attacker. By courtesy, the authorized person will hold the door by which the attacker gains access into the area. In more sophisticated scenarios, the attacker may try to trick the victim by creating an uncomfortable situation or providing a fake piece of identification. In the example in the image, the attacker will ask the security guard to get identification from his pocket. The guard could do that except it would create an uncomfortable situation. Therefore by courtesy, the security guard will let the attacker pass.

However, this type of attack is less effective than other types. Most of the time, people learn about tailgating from TV shows and movies rather than run into a realistic case. In large size organizations, authentication stage is really serious which makes this attack impossible to

perform. In small size companies where staffs know each other well and know how their business operates, it's hard for an attacker to gain access into the area without causing any notice. This method may work in places where the number of staffs changes regularly because it takes time for these employees to know each other and know how their workplace operates. An example which comes directly from my workplace. The process of firing and hiring occurs so frequently that managers don't change the passkey to employees' room, which creates access for not only current employees but former employees who can just come to the workplace as customers.

Reference: https://blog.mailfence.com/what-is-tailgating/

Baiting

Baiting is a type social engineering which focuses on human curiosity by using physical items such as flash drives or CD-ROMs. When the victim uses these devices on his computer, he will install malware or ransomware inadvertently, which grants the attacker the ability to control the system or exploit it.

To make the attack more effective, the attacker can disguise his baits with company logos or titles which create curiosity. Similar to tailgating, this type of attack seems unrealistic and can be seen most of the time on TV shows and movies. However, in 2008, there was a serious

cyberattack against the U.S military which came from an infected flash drive put in a laptop. (http://www.cnn.com/2010/TECH/innovation/08/25/pentagon.cyberattack/) In 2016, a social experiment was proceeded in which 200 USB sticks were dropped in public places and surprisingly, almost 20% of them were picked up and plugged into a device (https://www.computerworld.com/article/3002703/security/some-scary-insights-into-cybersecurity-risks-or-what-happens-when-you-drop-200-usb-sticks-in-public.html).

This method is dangerous because it takes advantage of curiosity and greed which some people cannot resist. In addition, this attack doesn't require victims to provide information or click to a link. When the infected device is plugged into a computer, an auto-run script will run automatically and grant access to the attacker.

Reference: https://www.bettercloud.com/monitor/information-security-and-pop-culture/