CS 470 Problem Set 04

# Exercises

## Based on the following characteristics of a scam, identify the Social Engineering tactic employed. Describe how you would detect such an attack and how you would mitigate against it.

1. In the Nigerian Scam, the victim is asked to put forth a small sum of "trust money" in exchange for a large prize in the end.

**Attack**: Reciprocation

**Detection**: The attack can be detected the attacker asking for something in return for a disproportionate gift in return

**Mitigate**: one could provide training to explain the tactics of the attack and that no prize is coming at the end.

1. A phishing e-mail has the appearance of a legitimate e-mail from your bank.

**Attack**: Authority

**Detection**: Understand how bank uses e mail communication

**Mitigate**: Authenticate the attacker. Imposters are unable to respond to authentication demands while individuals with genuine authority can produce credentials.

1. In the Nigerian Scam, the attacker sends a picture of himself in which he is depicted as being your gender, age, and race.

**Attack**: Likening

**Detection**: The attack can be detected by noticing that the attacker is trying to make themselves appear to be like you or someone you would be friends with.

**Mitigate**: Likening attacks can be mitigated by the victim being suspicious of overtures of friendship

1. In the Nigerian Scam, the attacker offers his SSN, bank account number, phone number, and more.

**Attack**: Commitment

**Detection**: Attacks is leverage people’s desire to be seen/ see others as trustworthy

**Mitigate**: Avoid making casual commitments and abandoning a commitment if it is not advantageous to keep it.

1. "This house has been on the market for only one day. You will need to make a full price offer if you want to get it.”

**Attack**: Scarcity

**Detection**: One can realize that the attack is using social pressure to act now. The more the attacker can make me feel that I must act the more desirable it will become.

**Mitigate**: This attack can be mitigated by being aware of this effect and the victim asking himself if the action would be equally desirable without the rushing

1. "Take the car for a test drive. You can even take it home for the weekend if you like. No obligation...”

**Attack**: Reciprocation

**Detection**: One could identify that the attacker is attempting to create a social situation where the victim is to feel gratitude for the attacker so they will want to do something for the attacker in return.

**Mitigate**: The victim needs to recognize the social pressure and consciously reject it. They can recognize that any expression of gratitude is appropriate

1. You get an e-mail from your bank informing you that your password has been compromised and to create a new one..

**Attack**: Reverse Engineering

**Detection**: One can detect the attack by understanding their banks procedure on contacting them on specific events.

**Mitigate**: One could have a policy that they will call their bank and speak with a Customer representative to confirm if any questionable email is received stating it is from their bank

# Problems

## What types of malware makes the most use of social engineering tactics?

**Phishing/Spam** - Generally uses all the practices of social engineering to encourage you to open an attachment

**Trojan** - Says it’s something it isn’t, or at least doesn’t disclose its intentions

**Adware** - They try to pressure you into buying things

Any type of **virus** as it they are propagated through user interactions

## What types of malware makes the least use of social engineering tactics?

**Worms** - They self propagate

**Rootkit** - They must remain hidden as to not alert the user to their presence

**Botnets** - THey use known issues with unpatched devices to install themselves on your computer, then they need to remain undetected

## Which of the following individuals is most likely to try to social engineer you? A teacher? A salesman? A politician? A parent?

**Teacher** - Announcements about getting started early because it’s a large assignment to convince you to start early on a large assignment

**Salesman** - Use sales tactics such as scarcity to convince you to make a purchase

**Politician** - Spam, pressure to sign up for mailing lists, using values you have to convince you to vote for them, etc.

**Parent** - I social engineer with my kids probably every day. I use various tactics to try and convince them to do basic life things like clean up their toys, eat dinner, etc.

## For each of the following scenarios, describe how you would mitigate against the Social Engineering attack. Try to employ as many of the defense mechanisms as possible

1. You are negotiating the price of a car with a salesman, and he attempts to close the sale by using scarcity: "If you walk off the lot the deal is off."

**Physical** - Request to talk to a different salesman

**Training** - Know the value of the vehicle you’re looking at so you know what it’s worth, and what a deal on it would be

**Reaction** - Recognize that he is using a sales tactic and come back with a buyer tactic such as saying “then I wont bother coming back tomorrow”

**Inoculation** - Practice negotiations with a friend/family member prior to the event many times

**Policy** - Set a budget for the car before and don’t be willing to go

1. The bank tells you by phone that your password has been compromised and you need to create a new one. What do you do?

**Physical** - Open your banking website and verify that your password hasn’t been compromised. Then reset it through the website just to be safe.

**Training** - Know the policies of you bank, and check if they ever call to talk about password resets (usually they don’t)

**Reaction** - Recognize that people on the phone may not always be who they say they are and approach the conversation with a healthy amount of skepticism.

**Inoculation** - Watch YouTube videos of spam callers asking for bank information, to help know what it seems like when they are calling

**Policy** - Know the policy of your bank regarding password security

1. You are the manager for the registrar's office. You are very concerned about student PII being disclosed through social engineering attacks.

**Physical** - Make sure the software and operating system are secure and up to date

**Training** - Train the people in the registrar’s office what PII is, and who it can be disclosed to

**Reaction** - Recognize what attacks might be used against a registrar’s office, and look for key indicators of social engineering attacks when being asked about PII

**Inoculation** - Have random social engineering attacks on members of the staff, especially new members.

**Policy** - Have a formal policy about how PII is handled, and make sure all staff members are aware of that policy.

# Challenges

## What types of social engineering attacks are your children likely to face? How can you protect them against such attacks?

One attack that our children are likely to face is the conformity attack. Conformity is a special type of commitment attack where one is leveraging an implied commitment made by society rather than by the individual. For example, a teenage kid may feel that they must wear name brand clothes to school as they feel the social pressure that one must wear name brand to fit in at school. To protect kids against this attack one could teach them that social pressure does not define their value or their ability to make friends

Another attack that children will be faced with is likening. Likening is the process of an attacker behaving in a way to appear like a member of a trusted group. Some kids may employ this attack to cheat or to use the other child for some benefit. A child could be protected against this attack be helping them to recognize and be suspicious where there is a one-sided friendship.

Another attack that children are faced with is scarcity. Scarcity attacks occur when the attacker can introduce the perception of scarcity of an item that is of a high perceived value. This type of attack on children is common around Christmas time. For example, the hatchimals toy a few years back was in scarcity which led to a high demand from kids, and parents paying high amounts to third party sellers in a desperate act to get the toy. One can protect kids from falling victim to this attack by explaining that the toy or item will still be around even if it is not under the Christmas tree that year.