Lab - Social Engineering

# Objective

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

# Resources

* Computer with internet Access

# Instructions

## Research Social Engineering Examples

Social engineering, as it relates to information security, is used to describe the techniques used by a person (or persons) who manipulate people to access or compromise information about an organization or its computer systems. A social engineer is usually difficult to identify and may claim to be a new employee, a repair person, or researcher. The social engineer might even offer credentials to support that identity. By gaining trust and asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

### Question:

Use any internet browser to research incidents of social engineering. Summarize three examples found in your research.

**2020 Twitter Bitcoin Scam**

One of this year’s recent cyber attacks was the Twitter Bitcoin scam, proving that not even the social media giants are impervious to cyber breaches.

Prominent Twitter users with the trusted blue verification checkmark Tweeted “double your Bitcoin” offers, telling their followers that they would double donations made on a select link. Well-respected leaders, celebrities, and big brands like former U.S. President Barack Obama, media billionaire Mike Bloomberg, tech creators Apple, and more were among the Twitter accounts affected. Because the accounts targeted had millions of followers, the bad actors received hundreds of contributions within mere minutes— reportedly totaling over $100K in Bitcoin, according to The BBC.

But how did cybercriminals breach so many high-profile users’ accounts in one swoop? Through a series of highly-targeted social engineering attacks. Bad actors manipulated Twitter employees to infect them with malware. From there, they made their way through Twitter’s internal systems and gained administrative access to a wealth of verified users’ passwords.

Lesson Learned

Twitter employees were the company’s biggest weakness, falling for social engineering exploits that allowed the bad actors a backdoor into highly-sensitive login information.

**2014 Sony Pictures Phish**

Sony Pictures Entertainment found itself the bullseye of the North Korean government after its launch of a new movie, "The Interview." North Korean individuals were in outrage over the Sony film, with a comedic plot about the assassination of the North Korean leader, Kim Jong Un, making the film production company a purposeful target in social engineering exploit.

Bad actors sent phishing emails to Sony executives, posing as Apple and asking the C-suite to verify their Apple IDs. Once the employees clicked on the spoofed link to the phony verification page and entered their credentials, the cyber criminals had what they needed. One executive used the same password for his Apple ID as he did his Sony account, giving the hackers all they needed to breach the company infrastructure.

The bad actors digitally dug through Sony’s systems and stole confidential documents, which they leaked online, including details of recent film productions and private employee data, according to The Washington Post.

Lesson Learned

Controversial content can be triggering to certain audiences, and Sony’s failure to consider how a comedy about a foreign country might play out ultimately made them a prime target for revenge. When pushing out new content, be sure to consider how your audiences could react to it. If neutrality is hard to achieve, weigh the risks of a bold launch with the help of a risk analysis.

**2013 Yahoo Customer Account Breach**

A few years back, Yahoo had every single customer account compromised in a social engineering exploit. A remarkable three billion users had their Yahoo’s credentials exposed, some of which were sold on the dark web with the intention of launching further attacks on individuals compromised. Because of its scale and exposure of the data, this is often considered one of the worst cyber attacks of the 2000s.

The attack occurred as the result of an error by a high-privilege engineer, who clicked into a phishing email. Noticing a theme here with these top hacks of the decade? Phishing scams live large and cause immense damage.

What makes this attack worse is that Yahoo underestimated the number of accounts breached, reporting only 500 million affected. It wasn’t for another four years that it was revealed the true extent of the exploit: that literally everyone who had an account at the time of the attack was affected. Obviously, this was far too late to protect affected users from possible repercussions of the breach.

Lesson Learned

Once again, it’s clear that social engineering tactics, specifically phishing schemes, are something to be taken extremely seriously. This popular form of cyber attack takes advantage of human’s natural inclination to trust, fooling individuals into granting bad actors access to entire digital infrastructures.

Type your answers here.

## Recognize the Signs of Social Engineering

Social engineers are nothing more than thieves and spies. Instead of hacking their way into your network via the Internet, they attempt to gain access by relying on a person’s desire to be accommodating. Although not specific to network security, the scenario below, described in Christopher Hadnagy’s book, *The Art of Human Hacking*, illustrates how an unsuspecting person can unwittingly give away confidential information.

*"The cafe was relatively quiet as I, dressed in a suit, sat at an empty table. I placed my briefcase on the table and waited for a suitable victim. Soon, just such a victim arrived with a friend and sat at the table next to mine. She placed her bag on the seat beside her, pulling the seat close and keeping her hand on the bag at all times.*

*After a few minutes, her friend left to find a restroom. The mark [target] was alone, so I gave Alex and Jess the signal. Playing a couple, Alex and Jess asked the mark if she would take a picture of them both. She was happy to do so. She removed her hand from her bag to take the camera and snap a picture of the “happy couple” and, while distracted, I reached over, took her bag, and locked it inside my briefcase. My victim had yet to notice her purse was missing as Alex and Jess left the café. Alex then went to a nearby parking garage.*

*It didn’t take long for her to realize her bag was gone. She began to panic, looking around frantically. This was exactly what we were hoping for so, I asked her if she needed help.*

*She asked me if I had seen anything. I told her I hadn’t but convinced her to sit down and think about what was in the bag. A phone. Make-up. A little cash. And her credit cards. Bingo!*

*I asked who she banked with and then told her that I worked for that bank. What a stroke of luck! I reassured her that everything would be fine, but she would need to cancel her credit card right away. I called the “help-desk” number, which was actually Alex, and handed my phone to her.*

*Alex was in a van in the parking garage. On the dashboard, a CD player was playing office noises. He assured the mark that her card could easily be canceled but, to verify her identity, she needed to enter her PIN on the keypad of the phone she was using. My phone and my keypad.*

*When we had her PIN, I left. If we were real thieves, we would have had access to her account via ATM withdrawals and PIN purchases. Fortunately for her, it was just a TV show."*

*Remember: “Those who build walls think differently than those who seek to go over, under, around, or through them." Paul Wilson - The Real Hustle*

### Question:

Research ways to recognize social engineering. Describe three examples found in your research.

Asking for immediate assistance

Asking you to donate to a charitable cause

Asking you to "verify" your information

Responding to a question you didn't ask

Type your answers here.

## Research Ways to Prevent Social Engineering

### Questions:

Does your company or school have procedures in place to help to prevent social engineering?

CUNY does have specific guidelines to prevent social engineering attacks.

Type your answers here.

If so, what are some of those procedures?

CUNY has these guidelines and many more on their website (https://president.baruch.cuny.edu/legal-and-labor/fraud-and-scam-prevention/)

* DO NOT reply to unexpected or unusual email from any sender
* DO NOT reply to email with any personal information or passwords
* If you have reason to believe that the request is real, call the institution or company directly
* DO NOT click a link or open an attachment in an unsolicited email message. If you have reason to believe the request is real, type the web address for the company or institution directly into your web browser

Type your answers here.

Use the internet to research procedures that other organizations use to prevent social engineers from gaining access to confidential information. List your findings.

Awareness Training. Phishing Simulations. Prevent Pre-Texting. Prevent Scam Emails Using Gateways. Put Good Processes in Place (BEC/CEO Fraud Prevention). Have a Good Social Media Policy on Privacy and Posting. Secure Mobile Devices. Set up Privileged Access and 2FA

# Answer Key

## Research Social Engineering Examples

Use any internet browser to research incidents of social engineering. Summarize three examples found in your research.

Answers will vary depending on current events. Some of the examples: Asking you to donate to charitable fundraisers or other causes, notifying you that you are a winner, posing as a boss or coworker, or asking you for urgent help.

## Recognize the Signs of Social Engineering

Research ways to recognize social engineering. Describe three examples found in your research.

Answers will vary. Some of the ways to recognize social engineering: beware of any downloads, usually foreign offers and prizes are fake, and research the facts before acting.

## Research Ways to Prevent Social Engineering

Does your company or school have procedures in place to help to prevent social engineering?

Answers will vary.

If so, what are some of those procedures?

Answers will vary. For example: Spam filters are set to high. The devices have up-to-date software. You are required to access the network via VPN only.

Use the internet to research procedures that other organizations use to prevent social engineers from gaining access to confidential information. List your findings.

Answers will vary. Some of the examples: Monitor for the latest breaches, secure physical access, and provide training to recognize social engineering.

End of Document