Social Engineering: Tips and Tricks to Reduce Being “Gotten”

If you have heard/seen these (or variations on these) . . .

- "I'm traveling in London and I've lost my wallet. Can you wire some money?"
- “I’m out of office. Remind me how to send a wire transfer.”
- "Someone has a secret crush on you! Click this link to find who it is!"
- "Did you see this video of you? Open the attachment!"
- "This is Chris from tech services. I've been notified of an infection on your computer."
- "You have not paid for the item you recently won on eBay. Please click here to pay."
- “….oh look. Someone dropped a flash drive. Wonder what’s on it?”

. . . you were (probably) a target for a social engineering attack.

Social engineering attacks can take many forms. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Most users should be familiar with email phishing scams (a form of social engineering) and have been taught not to open attachments from unknown or untrusted sources or to visit untrusted web sites. However, there are other ways that a perpetrator might try to gain access to information or systems. Below are several examples of social engineering methods.

IMPERSONATION

In this situation, the perpetrator pretends to be someone else - for example, impersonating a senior manager from your organization or someone from the ITS Help Desk. The impersonation may occur over the telephone, in person, or via email. The perpetrator may try to make you feel obligated to assist, or under pressure to follow their directions. They may use intimidation or a false sense of urgency to seek your cooperation – prompting you to react before you’ve fully thought through the consequences.

SYSTEMS AND PHYSICAL ACCESS

All too often, people will hold the door open for someone entering into a secure area or building without even knowing who the individual is or asking where they are going. The unauthorized individual may pretend to be a delivery person, a visitor, or even a fellow employee.

SHOULDER SURFING

This scenario refers to the ability of a perpetrator to gain access to information by simply watching what you are typing or seeing what is on your computer screen. This is known as “shoulder surfing,” and can also be done by looking through a window, doorway, or simply listening in on conversations.

BAITING

This scenario involves a perpetrator asking a variety of seemingly innocuous questions designed to probe for information. The attack is often done over the telephone but can also be done in person. Small amounts of facts are interjected at the right time into the conversation to make requests for information sound legitimate. Information you know could be valuable to the perpetrator--whether that information is about your work environment, fellow employees, projects, or personal information--must be handled with extreme care.

SURVEYS

Many of us have no doubt been recipients of requests to participate in surveys—whether online, via telephone or otherwise. The surveys may be for legitimate purposes or might be a scam. In either case, be aware of unwittingly disclosing information that may be used inappropriately. For example, disclosure of details about Metro could prove extremely useful to someone with malicious intent.

DUMPSTER DIVING

Searching through trash (“dumpster diving”) is a method used by perpetrators to obtain sensitive information.

SOCIAL MEDIA & NETWORKING WEBSITES

Use discretion when posting information online or commenting about anything on social networking sites. Once information is posted, it can potentially be viewed by anyone and may not be retracted afterwards. The more information you post, the more information is available for a perpetrator to use in an attempt to conduct a social engineering attack.

RECOMMENDATIONS

The scenarios above represent just a few types of social engineering attempts you may encounter. Additional tips to protect against these attacks include:

- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

- Don't fall for "Act NOW!" false urgency requests. Go slow and pay keen attention to fine details in emails and messages. Never let the urgency in attacker’s message cloud your judgment.

- Turn in "lost" USBs or other devices to management or IT and DO NOT access them.

- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.

- Take advantage of any anti-phishing features offered by your email client and web browser.

- Reject requests for online tech support from strangers no matter how legitimate they may appear.

- Avoid being greedy on the web. If you never participated in a lottery, it goes without saying that you can never be the winner. If you never lost money, why would you accept a refund from the FBI?

- Never give out your password to anyone, even if they claim to be from “technical support.”

- Beware of fear tactics such as "Help me or the boss is going to be mad!!".

- Be aware of your surroundings. Make sure you know who is in range of hearing your conversation or seeing your work. Computer privacy screens are a great way to deter shoulder surfing in public places.

- If you don’t know someone who is in a restricted area, look for a badge or a visitor pass. If you are unsure about their authorization or access permission, report the situation to the appropriate staff.

- Before you throw something in the trash, ask yourself, “Is this something I would give to an unauthorized person or want to become publicly available?” If you are not certain, always err on the side of caution and shred the document or deposit it in a secure disposal container.

- If you receive a survey request, you should contact the sponsoring organization to ensure the survey is legitimate. Then check with your supervisor or appropriate individual, such as your privacy or security officer to determine if it is ok to respond to the survey. If you do respond, make sure you are not sharing sensitive or confidential information with unauthorized individuals or organizations.

- Be aware of your department’s data classification, destruction and retention policies.