Troy Dixon
Spring 2025
independent Essay

Deceptive Attacks

Previously, you learned about the dangers of socially engineered deceptive attacks. In this reading, you will review this topic and learn about a few more types of socially engineered deceptive attacks. Social engineering attacks are unique as compared to other types of attacks. Social engineering requires cybercriminals to use psychology to trick victims into providing information to the cybercriminal. In other types of cyber attacks, the cybercriminals use computers and other digital tools to hack computers and networks without engaging and deceiving individual victims.

Cybercriminals may use deceptive attacks to disguise their identities, intents, and motives. Through social engineering techniques, these cybercriminals attempt to trick victims into revealing private information, such as a credit card number or login credentials. The cybercriminal might disguise their identity by pretending to be from a reputable organization or to be an individual that the victim might trust, like a friend or work colleague. Socially engineered deceptive attacks can happen through websites, email, text messaging, phone calls, in-person interactions, and more. Cybercriminals often find deception through social engineering to be an easy means for hacking a computer system, simply because many technology users are not aware that this type of threat exists. Others may be aware of the potential for a deceptive cybercriminal attack, but are not sure how to recognize the deception and, further, to prevent themselves from being deceived

Social engineering attacks have increased in recent years. These attacks have changed how organizations approach their cybersecurity policies. It is important for organizations to train their employees on how to recognize a deceptive attack. A single employee that is tricked into entering their company login and password into a fake login window could create an opportunity for a catastrophic criminal attack against an organization's network.

Deceptive attacks over the internet

There are many types of social engineering attacks. Some of the more common attacks include:

- **Phishing:** A cybercriminal may use email and text messaging to "fish" or phish for victims that will take the cybercriminal's bait. One basic type of phishing bait may include a convincing story to trick the victim into replying to the email with personal or sensitive information. Another common phishing scam includes using "clickbait" links. These phishing messages entice victims to click on a link by using bait such as popular pet videos, gossip, news scandals, opportunities to win money or prizes, lewd images or videos, etc. If the recipient clicks on the link, they become victim to the next phase of the malicious attack, which could be some type of forced download of malware, ransomware, viruses, keyloggers, trackers, and more.
- **Spoofing:** Cybercriminals use this technique to alter the header on phishing emails in order to appear to originate from a legitimate business or reputable person. For example, a spoofed email might use a fake header that appears to be from a bank. The body of the email might ask the victim to click a given link to log into their bank account to fix a "problem". The link leads to the cybercriminal's fake website that looks identical to the bank website and exists only to

collect the bank login credentials from victims. The fake website might even give the victim an error message and forward them to the real bank to try to login again. This technique keeps the victim from immediately recognizing they have been scammed because the second login attempt on the real website is usually successful.

- **Spear phishing:** A cybercriminal might use details about a victim's life to win the victim's trust. For example, the criminal might first purchase data from a social media platform that provides personal information about the platform's users. The cybercriminal then uses this data to target or "spear" specific individuals. The cybercriminal could select a name from a user's friends list and create a spoofed email that appears to be from that friend. The spoofed email may say something as simple as, "look at this photo I found of you online!" The email may also include an attachment or a clickbait link that leads to the next stage of the attack.
- **Whaling:** When a cybercriminal wants to spear phish a big target or "whale," they will spend more time and effort deceiving the victim. A whale target is typically someone in a position of power, such as a wealthy and/or famous person, an executive of a company, or a high-level government employee. The whale is targeted because of the likelihood that they have the ability to pay high ransomware fees, trade valuable information or confidential data, or may be vulnerable to blackmail.
- **Vishing:** Cybercriminals use Voice over IP (VoIP) to make phone calls or leave voice messages pretending to be from reputable companies in order to trick victims into revealing personal information, such as banking details and credit card numbers. Although telephone scams have been running for decades, vishing with VoIP makes it easier for cybercriminals to hide their true identity. VoIP calls are significantly more difficult to trace than landline calls.

Targeted and in-person deceptive attacks

- **Shoulder surfing:** This malicious attack might have a specific victim or organization as their target. Shoulder surfing happens when a person looks over a victim's shoulder to watch them enter login credentials, credit card numbers, or other sensitive information. For example, a temporary contractor for an organization may look over the shoulder of an employee to watch the employee enter their login info. The temporary employee's goal might be to steal credentials in order to illegally obtain confidential company data or plant ransomware.
- **Tailgating:** This in-person attack is a form of social engineering in which an unauthorized party gains physical access to a restricted area by simply following a person or group of persons who have authorized access. For example, a criminal wanting to gain physical access to an organization's computer network might dress in business clothing and follow a group of coworkers coming back from lunch. One member of the group may use their key card to open the door, then hold the door open for the rest of the group, as well as the criminal who is dressed and behaving as though they belong in the building. The criminal may even have a fake ID card to show anyone who questions them.
- **Impersonation:** This attack might happen over email, text messaging, or a phone call. The attacker impersonates someone who should have access to an organization's computer network. For example, the attacker might call the IT Support team to request help with a password reset.

Alternatively, the attacker might pretend to be a member of an organization's IT Support team. They may call an employee to ask them to change some settings on their computer to fix a fake problem. These changes are intended to open a door for the cybercriminal to gain access to the organization's network.

- **Dumpster Diving:** This in-person attack involves the attacker literally digging through the trash of an individual or organization to hunt for confidential information, like financial or customer information. Shredding all confidential documents is an easy way to prevent this type of attack.
- **Evil twin:** This type of attack involves the cybercriminal installing Wi-Fi routers that appear to belong to an organization's network. These Wi-Fi access points may not require a password and might appear to offer a stronger signal than the real Wi-Fi router. When victims connect to the fake Wi-Fi access point, the cybercriminal gains access to the victim's wireless transmissions, which can include login credentials and other sensitive information.

As an IT Support professional, it is important to train the people and organizations you support on how to identify and protect from socially engineered attacks. These training sessions should be offered to all new employees, contractors, and anyone else who may have access to the organization's network. Additionally, the training sessions should be repeated on a frequent schedule as new, more sophisticated cybercrime techniques emerge. One best practice method for keeping network users always on alert for attacks, is for IT Support staff to periodically stage harmless attacks that target network users. This method is used to test how effective the training classes have been and how long the users are able to recall how to protect themselves against an attack. Instead of stealing the user's private information, the harmless attack makes users aware that they fell for a scam, and provides reminders on how to protect themselves against real cybercriminal attacks in the future.