LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.2.4 - Misinformation and Impersonation

Lesson Overview:

Students will:

- Compare and contrast different types of social engineering techniques.

Guiding Question: What are misinformation and impersonation and how can they be used with social engineering?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.2 - Explain common threat vectors and attack surfaces

- Human vectors/social engineering
  - Misinformation/disinformation
  - Impersonation
  - Business email compromise
  - Brand impersonation

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Misinformation and Impersonation

Misinformation/Disinformation

In the context of cybersecurity, misinformation and disinformation refer to the spread of false or misleading information with the intent to deceive, manipulate, or compromise the security of computer systems or users.

Misinformation is the dissemination of inaccurate or false information, often unintentional. In the realm of cybersecurity, it could involve spreading incorrect details about a security vulnerability, a software update, or the nature of a particular threat. Misinformation can lead to confusion and poor decision-making, potentially putting systems at risk.

Unlike misinformation, ***disinformation*** is intentionally false information spread with the purpose of causing harm, confusion, or manipulating individuals or systems. In the context of cybersecurity, disinformation might involve spreading fake security alerts, creating false narratives about cyber threats, or manipulating public perception to divert attention from actual security issues.

Both misinformation and disinformation can contribute to an insecure cyber environment by creating a lack of trust, confusion among users, and diverting attention from real security issues. It's crucial for individuals and organizations to be vigilant, verify information from reliable sources, and stay informed about the evolving landscape of cybersecurity threats.

Impersonation and Tailgating

Impersonation is exactly as it sounds, but in the world of cybersecurity, the intent is to gain access to personal information. Impersonation uses social engineering, such as dumpster diving and personalization, to fool someone into unwittingly providing sensitive data to attackers or transferring money to a fraudulent account. An attacker may impersonate a person of authority or a person with a need to access a sensitive area. Oftentimes, impersonators will demand action or access immediately by making it appear to be an emergency or time sensitive. This sense of urgency should be a warning sign.

Although exaggerated at times, examples can be found in films like James Bond, Mission Impossible, the Ocean's series, or Catch Me If You Can. Commonly-used tactics include overwhelming the victim with technical jargon (which makes the target feel stupid), verbally attacking the target as if the impersonator were someone superior in rank (makes the target feel inferior), or employing an "over-friendliness" attitude (which makes the target feel like helping "a friend").

Tailgating, also known as piggybacking, is a social engineering attack where one tries to gain entry to a restricted area without the proper authentication. The attacker may simply follow behind someone who is authorized to access the restricted area.

Attackers increase their likelihood of success by attempting to blend in with their surroundings. Wearing similar clothing as other employees would not stand out to a security guard. Appearing as a third-party repairman can also be a successful deception, e.g., telephone/elevator repair, fire inspector, or plumber.

A deliveryman would also allow for easy access. People want to be helpful, so if someone were to carry boxes of donuts or FedEx boxes, since their hands are full, people would hold open doors for them.

Having a security guard or team with a set of guidelines for entry would greatly reduce the risk of tailgating. The introduction of a visitor policy will help security notice who belongs and who does not. Encouraging security to question visitors helps deter would-be tailgaters. A mantrap helps enforce a "one scan, one entry" guideline for access to a restricted area. An access control vestibule (also referred to as a sally port, air lock, or mantrap) is a physical security system composed of a small space with two sets of interlocking doors installed in a way that one set of doors must be closed before the other set can open.

Business Email Compromise

Business email compromise (BEC) is a type of cyberattack where an attacker gains access to or compromises a business email account to conduct fraudulent activities. The goal of BEC is often financial gain through activities such as unauthorized fund transfers, invoice fraud, or obtaining sensitive business information.

In a typical BEC scenario, the attacker might use various tactics to compromise an email account, such as phishing, social engineering, or malware. Once they have access to the account, they can monitor email communications, gather information about the organization's business processes, and impersonate key personnel.

Common BEC tactics include:

- CEO Fraud: The attacker poses as a high-level executive, such as the CEO, and requests financial transactions or sensitive information from employees.
- Invoice Fraud: The attacker manipulates or creates fake invoices, tricking employees or vendors into making payments to fraudulent accounts.
- Employee Impersonation: The attacker pretends to be a trusted employee, such as someone from the finance department, and requests fund transfers or sensitive information.

BEC attacks can be sophisticated and difficult to detect, as they often involve social engineering and exploiting trust within an organization. To mitigate the risk of BEC, organizations should implement strong email security measures, conduct employee training on recognizing phishing attempts, and establish clear verification processes for financial transactions or sensitive requests.

Brand Impersonation

Brand impersonation refers to the act of mimicking or imitating a legitimate brand or company, often with the intent to deceive or defraud individuals. In the context of cybersecurity, brand impersonation is commonly associated with phishing attacks.

In a brand impersonation attack, malicious actors can use emails, websites, or social media. Attackers may send emails that appear to be from a well-known and trusted brand, using similar logos, colors, and language to deceive recipients. Attackers could fake websites that closely resemble the official websites of legitimate brands. These sites may be used to collect sensitive information from users or distribute malware. Impersonation can also occur on social media platforms, where attackers create fake profiles or pages that mimic those of reputable brands. These fake profiles may be used to spread misinformation,

conduct phishing, or engage in other malicious activities.

The goal of brand impersonation is often to trick individuals into divulging sensitive information, such as login credentials or financial details, or to spread malware. Users and organizations need to stay vigilant, verify the authenticity of communications or websites, and be cautious about clicking on links or providing personal information, especially when the source seems suspicious or unexpected.

Hoaxes

The simple definition of a ***hoax*** is a deception, either humorous or malicious. Most hoaxes are not real threats but can be portrayed as real. Although most hoaxes are not real, they are still a waste of time and effort. These hoaxes are typically emails, such as chain letters, depicting horrific events, urban legends, or malware. Some hoaxes can be an attempt to get money by phishing for login information. The attackers may pose as law enforcement or governmental agents. Their intent is to mislead and frighten victims, hoping to get the victims to forward the hoax to friends and family. For the hoaxes that pose no real danger, they may waste as much time and money as a real virus would.

Defense

It's important to understand that impersonation attacks are typically more sneaky and convincing than phishing attacks (as discussed in the previous section). Verification is key. Although time-consuming, checking credentials, calling the supposed third party for proof, or asking a manager or a known person from the claimed department could all very well protect against a successful impersonation attack. It may be quite often (seemingly all the time) that each instance is verified, but a secure facility will resist the urge to stop verifying. Each verification is not a "win" or "lose" to ensure a person is who they claim to be. It is a policy that should be celebrated for keeping the organization secure. Finally, ignore the saying "Never say never." Never volunteer information or provide personal details to someone unknown.