Lab - Explore Social Engineering Techniques

Objectives

Part 1: Explore Social Engineering Techniques

Part 2: Create a Cybersecurity Awareness Poster

Introduction

Cybersecurity is critical because it involves protecting unauthorized access to sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property (IP), and sensitive systems. Social engineering is a broad range of malicious activities accomplished by psychologically manipulating people into performing actions or divulging confidential information. In this lab, you will explore social engineering techniques, sometimes called human hacking, which is a broad category for different types of attacks.

Required Resources

PC or mobile device with internet access

Background / Scenario

Recent research reveals that the most common types of cyberattacks are becoming more sophisticated, and the attack targets are growing. The purpose of an attack is to steal information, disable systems or critical services, disrupt systems, activities, and operations. Some attacks are designed to destroy information or information systems, maliciously control a computing environment or its infrastructure, or destroy the integrity of data and/or information systems. One of the most effective ways an attacker can gain access to an organization's network is through simple deception. In the cybersecurity world this is call social engineering.

Social Engineering Attacks

Social engineering attacks are very effective because people want to trust other people and social engineering attacks are not the kind of attack that the average user guards against; users are concerned with botnets, identity theft or ransomware. These are big external threats, so they do not think to question what seems to be a legitimate-looking message.

Baiting

Baiting relies on the curiosity or greed of the victim. What distinguishes baiting from other types of social engineering is the promise of an item or good that hackers use to entice victims. Baiters may offer users free music or movie downloads if the users surrender their login credentials to a certain site. Baiting attacks are not restricted to online schemes. Attackers can exploit human curiosity with physical media like USB drives.

Shoulder Surfing

Shoulder surfing is literally looking over someone's shoulder to get information. Shoulder surfing is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form or enter a PIN number at an ATM machine. Shoulder surfing can also be done long distance with the aid of modern cell phones, binoculars, or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. There are even screen shields that make shoulder surfing much more difficult.

Pretexting

Pretexting is using deception to create a scenario to convince victims to divulge information they should not divulge. Pretexting is often used against organizations that retain client data, such as financial data, credit card numbers, utilities account numbers, and other sensitive information. Pretexters often request information

from individuals in an organization by impersonating a supervisor, helpdesk clerk, or client, usually by phone, email, or text.

Phishing, spear phishing, and whaling attacks

In phishing attacks, the attackers try to obtain personal information or data, like username, password, and credit card details, by disguising themselves as trustworthy entities. Phishing is mainly conducted through emails and phone calls. Spear phishing is more targeted version of the phishing, in which an attacker chooses specific individuals or enterprises and then customizes their phishing attack to their victims to make it less conspicuous. Whaling is when the specific target is a high-profile employee such as a CEO or CFO.

Scareware and ransomware

Ransomware attacks involve injecting malware that encrypts a victim's critical data. The cyber criminals request a ransom to be paid to decrypt the data. However, even if a ransom is paid, there is no guarantee the cyber criminals will decrypt the information. Ransomware is one of the fastest growing types of cyberattack and has affected thousands of financial organizations, government agencies, healthcare facilities, even schools and our education systems.

Scareware takes advantage of a user's fear by coaxing them into installing fake antivirus software.

Tailgating

Tailgating tricks the victim into helping the attacker gain unauthorized access into the organization's physical facilities. The attacker seeks entry into a restricted area where access is controlled by software-based electronic devices or human guards. Tailgating can also involve the attacker following an employee closely to pass through a locked door before the door locks behind the employee.

Dumpster diving

In the world of social engineering, dumpster diving is a technique used to retrieve discarded information thrown in the trash to carry out an attack on a person or organization. Dumpster diving is not limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes, it can also involve electronic information left on desktops, or stored on USB drives.

Instructions

Part 1: Explore Social Engineering Techniques

Step 1: Explore Baiting, Shoulder Surfing, and Pretexting.

The National Support Center for Systems Security and Information Assurance (CSSIA) hosts a **Social Engineering Interactive** activity. The current link to the site is https://www.cssia.org/social_engineering/. However, if the link changes, try searching for "CSSIA Social Engineering Interactive".

Click **Next** in the interactive activity, and then use the content to answer the following questions.

What is baiting? Did you click on the USB drive? What happened to the victim's system?

What is Shoulder Surfing? What device was used to perform the shoulder surfing? What information was gained?

What is Pretexting? What type of information did the cybercriminal request? Would you fall victim?

Step 2: Explore Phishing/Spear Phishing and Whaling

Phishing is designed to get victims to click on links to malicious websites, open attachments that contain malware, or reveal sensitive information. Use the interactive activity to explore different phishing techniques.

In this phishing example, what is the ploy the attacker uses to trick the victim to visit the trap website? What is the trap website used to do?

What is the difference between phishing and spear phishing or whaling?

Step 3: Explore Scareware and Ransomware

Scareware is when victims are deceived into thinking that their system is infected with malware and receive false alarms prompting them to install software that is not needed or is itself malware. Ransomware is a type of malware that threatens to publish the victim's data or encrypts the victim's data preventing access or the ability to use the data. Victims are prevented from accessing their system or personal files until they make a ransom payment to regain access.

What data does the attacker claim to have in this example? Would you fall for this deception?

What is the attacker requesting the victim do to get the data back?

What is tailgating?

Give three ways to prevent social engineering attacks?

Part 2: Create a Cybersecurity Awareness Poster

Use Powerpoint to create a poster that will make others aware of the different social engineering techniques used to gain unauthorized access to an organization or the organization's data.

Pick from: Baiting, Shoulder Surfing, Pretexting, Phishing, Scareware, Ransomware, Tailgating or Dumpster Diving.

The poster should depict the techniques used and how users can avoid one of these social engineering attacks. Also include directions on where the poster should be placed within the organization.

Answer Key

Part 1: Explore Social Engineering Techniques

Step 1: Explore Baiting, Shoulder Surfing, and Pretexting.

What is baiting? Did you click on the USB drive? What happened to the victim's system?

Baiting is using a false promise to gain a victim's interest to lure them into a trap that steals their personal information or infects their systems with malware. Yes – the system is compromised by malware.

What is Shoulder Surfing? What device was used to perform the shoulder surfing? What information was gained?

Shoulder surfing is looking over someone's shoulder while they are using a computer and visually capturing logins or passwords or other sensitive information. A Cell Phone. Login and Password information

What is Pretexting? What type of information did the cybercriminal request? Would you fall victim?

Pretexting is when an attacker establishes trust with their victim by impersonating persons who have right-to-know authority and asking questions that appear to be required to confirm the victim's identity, but through which they gather important personal data. Information requested name, work role, etc.

Step 2: Explore Phishing/Spear Phishing and Whaling

In this phishing example, what is the ploy the attacker uses to trick the victim to visit the trap website? What is the trap website used to do?

The phishing scheme sends a fake notice that the victim has recently attempted to withdraw funds from their account while in another country: $174.99. The scheme is designed to steal the victim credentials including username and password.

What is the difference between phishing and spear phishing or whaling?

Spear phishing is more targeted version of the phishing, in which an attacker chooses specific individuals or enterprises and then customizes their phishing attack to their victims to make it less conspicuous. Whaling is when the specific target is a high-profile employee such as a CEO or CFO.

Step 3: Explore Scareware and Ransomware

What data does the attacker claim to have in this example? Would you fall for this deception?

> Facebook Login

> Credit Card Details

> Email Account Login

No, now that you know what scareware is, you know better than to call an unknown number or share your account information.

What is the attacker requesting the victim do to get the data back?

Please call the attacker within the next 5 minutes to prevent your computer from being disabled.

Call: 44-8000-903-274

What is tailgating?

Tailgating is when an attacker who lacks the proper authorization follows a victim with authorized credentials through a door or other secure building access point into a restricted area.

Give three ways to prevent social engineering attacks?

Think before you act - Never share personal information over the phone, email, or on unsecure websites. Do not click on links, download files, or open email attachments from unknown senders.

Stay aware of your surroundings – Be skeptical of links to web forms that request personal information, even if the email appears to come from a legitimate source. Never click on or enter sensitive information into a pop-up.

Keep your accounts and devices safe - Use antivirus software, and spam filters, and update and patch your devices regularly.

Part 2: Create a Cybersecurity Awareness Poster

Use Powerpoint to create a poster that will make others aware of the different social engineering techniques used to gain unauthorized access to an organization or the organization's data.

The poster should depict the techniques used and how users can avoid one of these social engineering attacks. Also include directions on where the poster should be placed within the organization.