Social Engineering Awareness

Common Social Engineering Techniques

Phishing emails:

Phishing emails are one of the most common types of social engineering attacks. Phishing emails are designed to trick users into revealing sensitive information, such as passwords or credit card numbers. Phishing emails often appear to be from legitimate organizations, such as banks, credit card companies, or government agencies.

Here are some tips to help you identify phishing emails:

Be suspicious of emails that ask for personal information, such as passwords, credit card numbers, or Social Security numbers.
Check the sender's email address carefully. Phishing emails often come from addresses that are similar to legitimate addresses, but with minor changes.
Hover over links in emails before clicking on them. This will show you the actual URL of the link, which may be different from the URL displayed in the email.
Be careful about opening attachments in emails. Phishing emails often contain attachments that contain malware.
Vishing attacks:

Vishing attacks are phone calls where the attacker pretends to be from a legitimate organization. Vishing attacks often attempt to trick users into revealing sensitive information or performing actions that could compromise security.

Here are some tips to help you identify vishing attacks:

Be suspicious of phone calls that ask for personal information, such as passwords, credit card numbers, or Social Security numbers.
Never give out your personal information to someone who calls you out of the blue.
If you are unsure about the legitimacy of a call, hang up and call the organization back at a number you know is legitimate.
Smishing attacks:

Smishing attacks are text messages where the attacker pretends to be from a legitimate organization. Smishing attacks often attempt to trick users into clicking on malicious links or revealing sensitive information.

Here are some tips to help you identify smishing attacks:

Be suspicious of text messages that ask for personal information, such as passwords, credit card numbers, or Social Security numbers.

Never click on links in text messages from unknown senders.
If you are unsure about the legitimacy of a text message, contact the organization directly.
Other social engineering techniques:

In addition to phishing, vishing, and smishing attacks, there are many other social engineering techniques that attackers can use. Some common social engineering techniques include:

Baiting: Baiting involves leaving a valuable item, such as a USB drive or gift card, in a public place in the hope that someone will pick it up and connect it to their computer.
Pretexting: Pretexting involves creating a false identity or scenario in order to gain someone's trust. For example, an attacker might pose as a customer support representative or a law enforcement officer.
Impersonation: Impersonation involves pretending to be someone else, such as a trusted colleague or friend.
How to protect yourself from social engineering attacks:

The best way to protect yourself from social engineering attacks is to be aware of the common techniques that attackers use. If you are suspicious of an email, phone call, or text message, do not click on any links or reveal any sensitive information. Instead, contact the organization directly using a known phone number or website address.

Here are some additional tips to help you protect yourself from social engineering attacks:

Keep your software up to date. Software updates often include security patches that can help protect you from known vulnerabilities.
Use a strong password manager to generate and store unique passwords for all of your online accounts.

Enable two-factor authentication (2FA) whenever possible. 2FA adds an extra layer of security to your accounts by requiring you to enter a code from your phone in addition to your password when logging in.
Be careful about what information you share online. Avoid sharing personal information on social media or other public websites.
Be careful about opening attachments in emails or clicking on links in text messages. If you are unsure about the legitimacy of an attachment or link, do not open it or click on it.

Social engineering is the practice of manipulating people into performing actions or divulging confidential information. Attackers use a variety of techniques to exploit human psychology, such as fear, greed, and curiosity. Social engineering attacks can be carried out in person, over the phone, via email, or through social media.

Common social engineering techniques

Phishing: Phishing is a type of social engineering attack that uses fraudulent emails or text messages to trick people into revealing confidential information, such as passwords or credit card numbers.
Vishing: Vishing is a type of social engineering attack that uses fraudulent phone calls to trick people into revealing confidential information or performing actions that could compromise security.
Smishing: Smishing is a type of social engineering attack that uses fraudulent text messages to trick people into revealing confidential information or performing actions that could compromise security.
Baiting: Baiting is a type of social engineering attack that involves leaving a valuable item, such as a USB drive or gift card, in a public place in the hope that someone will pick it up and connect it to their computer.
Pretexting: Pretexting is a type of social engineering attack that involves creating a false identity or scenario in order to gain someone's trust. For example, an attacker might pose as a customer support representative or a law enforcement officer.
Impersonation: Impersonation is a type of social engineering attack that involves pretending to be someone else, such as a trusted colleague or friend.
How to protect yourself from social engineering attacks

Be aware of the common social engineering techniques. The more you know about social engineering attacks, the better equipped you will be to spot them.
Be suspicious of unsolicited emails, phone calls, and text messages. If you receive an email, phone call, or text message from someone you don't know, be suspicious. Legitimate organizations will not contact you out of the blue asking for personal information.
Do not click on links in emails or text messages from unknown senders. If you are curious about the link, hover over it to see the actual URL. If the URL does not match the website it appears to be from, do not click on it.
Do not open attachments in emails from unknown senders. Email attachments can contain malware that can infect your computer.
Use strong passwords and enable two-factor authentication (2FA) for all of your online accounts. Strong passwords are at least 12 characters long and include a mix of upper and lowercase letters, numbers, and symbols. 2FA adds an extra layer of security to your accounts by requiring you to enter a code from your phone in addition to your password when logging in.
Be careful about what information you share online. Avoid sharing personal information on social media or other public websites.
Practical tips for social engineering awareness

Conduct regular security awareness training for all employees. This training should cover the common social engineering techniques and how to spot them.
Implement phishing simulation exercises. Phishing simulation exercises can help employees learn how to identify and avoid phishing emails.
Use security information and event management (SIEM) tools to monitor for suspicious activity. SIEM tools can help you identify potential social engineering attacks by monitoring your network for unusual activity.

Use social engineering tools to test your own security posture. Social engineering tools can help you identify vulnerabilities in your security posture that could be exploited by attackers.
Tools and commands for social engineering awareness

Phishing simulation tools: There are a number of phishing simulation tools available, such as KnowBe4 and PhishMe. These tools can be used to create and send phishing emails to your employees to test their awareness of phishing attacks.
SIEM tools: SIEM tools such as Splunk and LogRhythm can be used to monitor your network for suspicious activity, such as unusual login attempts or network traffic.
Social engineering tools: There are a number of social engineering tools available, such as Kali Linux and Metasploit. These tools can be used to test your own security posture by simulating social engineering attacks.