PHISHING AWARENESS TRANNING

Content

- What is phishing?
- Social Engineering tactics.
- How does phishing Work?
- Types of Phishing Attack.
- Mitigation.

What is phishing?

Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware or otherwise exposing themselves to cybercrime. Phishing attacks are a form of social engineering.

Social Engineering Tactics

- A **social engineering attack** is a cybersecurity attack that relies on the psychological manipulation of human behavior to disclose sensitive data, share credentials, grant access to a personal device or otherwise compromise their digital security.
- Social engineering attacks pose a great threat to cybersecurity since many attacks begin on a personal level and rely on human error to advance the attack path. By invoking empathy, fear and urgency in the victim, adversaries are often able to gain access to personal information or the endpoint itself. If the device is connected to a corporate network or contains credentials for corporate accounts, this can also provide adversaries with a pathway to enterprise-level attacks.
- With cyber criminals devising ever-more manipulative methods for tricking people and employees, organizations must stay ahead of the game.

How does phishing work?

Phishing often uses social engineering techniques to trick users into performing actions such as clicking a link or opening an attachment, or revealing sensitive information. It often involves pretending to be a trusted entity and creating a sense of urgency, like threatening to close or seize a victim's bank or insurance account.

Types of Phishing Attack

1. Email phishing
2. Spear phishing
3. Whaling
4. Smishing and vishing
5. Angler phishing

1. Email phishing

- Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organization and sends thousands of generic requests.
- The fake domain often involves character substitution, like using ‘r’ and ‘n’ next to each other to create ‘rn’ instead of ‘m’.
- In other cases, the fraudsters create a unique domain that includes the legitimate organization's name in the URL. The example below is sent from ‘olivia@amazonsupport.com’.

2. Spear phishing

- There are two other, more sophisticated, types of phishing involving email.
- The first, spear phishing, describes malicious emails sent to a specific person.
- Criminals who do this will already have some or all of the following information about the victim:
- Their name.
- Place of employment.
- Job title.
- Email address; and
- Specific information about their job role.

3. Whaling

- Whaling attacks are even more targeted, taking aim at senior executives. Although the end goal of whaling is the same as any other kind of phishing attack, the technique tends to be a lot subtler.
- Tricks such as fake links and malicious URLs aren’t helpful in this instance, as criminals are attempting to imitate senior staff.
- Whaling emails also commonly use the pretext of a busy CEO who wants an employee to do them a favor.

4. Smishing and vishing

- With both smishing and vishing, telephones replace emails as the method of communication.
- Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.
- One of the most common smishing pretexts are messages supposedly from your bank alerting you to suspicious activity.

5. Angler phishing

- A relatively new attack vector, social media offers several ways for criminals to trick people. Fake URLs; cloned websites, posts, and tweets; and instant messaging (which is essentially the same as smishing) can all be used to persuade people to divulge sensitive information or download malware.
- Alternatively, criminals can use the data that people willingly post on social media to create highly targeted attacks.

MITIGATION

- These sneaky cyber tricks can lead to some serious trouble, like compromising personal information or falling victim to scams.
- That’s why it’s essential to be proactive and have some solid phishing mitigation strategies up your sleeve. Don’t worry, though; we’ve got you covered! In this guide, we’ll walk you through some practical tips and tricks to keep those phishing attempts at bay and protect yourself and your data online. So, let’s dive in and stay one step ahead of those pesky phishers!

THANK YOU