Familiarity with Phishing Attacks

Introduction: Explanation of phishing and its various forms

Phishing is one of the oldest threats on the internet and a major vehicle for enabling the majority of cybercrime IC3's latest cybercrime report shows that phishing has the highest victim count among cybercrimes reported in the US. Phishing involves executing cybercrimes by leveraging social engineering techniques.

Phishing involves attempting to trick individuals into divulging sensitive information, such as usernames, passwords, credit card numbers, or other personal information, by pretending to be a trustworthy entity in electronic communication. While phishing can manifest through text messages, social media, or phone calls, the term "phishing" primarily pertains to attacks delivered via email. These deceptive emails have the capacity to reach millions of users directly and can easily blend in with the vast number of legitimate emails that busy users regularly receive. The consequences of falling victim to phishing can include the installation of malware like ransomware, system sabotage, or unauthorized access to and theft of intellectual property and financial assets. Organizations of any size and industry are vulnerable to phishing attacks, which can take the form of either broad-scale campaigns seeking to collect passwords or generate quick financial gains, or the initial stage of a focused assault against a specific company. In targeted attacks, commonly known as spear phishing, attackers leverage information about the organization or its employees to craft highly convincing and realistic messages.

- **Methods of Phishing:**

Phishing can be carried out through different channels, including email, text messages, social media, and phone calls. While it can occur via various means, the term "phishing" is commonly associated with email-based attacks.

- **Email as the Main Vector:**

Phishing emails are highlighted as a significant threat, capable of reaching millions of users directly. The term is often used specifically in the context of deceptive emails, which can easily blend in with legitimate emails in users' inboxes.

- **Potential Consequences:**

Phishing attacks can lead to various negative outcomes, including the installation of malware (such as ransomware), system sabotage, and the theft of intellectual property or money.

- **Organizational Impact:**

Organizations of any size and type are susceptible to phishing attacks. These attacks can range from mass campaigns aimed at collecting passwords or making easy money to targeted attacks focused on stealing sensitive data.

- **Mass Campaigns vs. Targeted Attacks:**

Phishing attacks may be part of mass campaigns with broad objectives or the initial step in targeted attacks against specific companies. Targeted attacks, often referred to as spear phishing, involve personalized messages based on information about the targeted organization or its employees.

- **Spear Phishing:**

The concept of spear phishing is introduced, emphasizing the use of specific information about individuals or organizations to create more convincing and realistic phishing messages.

Identification: Tips for identifying phishing attempts

- **Emails Demanding Urgent Action.** Phishing emails are typically those that threaten dire consequences or the loss of an opportunity if no action is taken quickly. This tactic is frequently used by attackers to force recipients to respond quickly before they have a chance to review the email for any errors or inconsistencies.

- **Emails with Grammar and Spelling Mistakes.** Spelling and grammar errors in emails are another indicator of phishing emails. Many businesses use spell-checking software by default on emails they send out to make sure the grammar is proper. Users of email programmes that are browser-based can use web browser capabilities like autocorrection and highlight.

- **Emails with an unfamiliar greeting.** Coworkers typically begin their emails with an informal greeting. One should be suspicious of those that begin with "Dear" or contain words that are not generally used in casual conversation. These are from sources that are not familiar with the workplace interaction style that your company uses.

- **Discrepancy in Email Addresses, Links & Domain Names.** Another method of identifying phishing is to look for discrepancies in domain names, email addresses, and links. Compare the sender's address to other emails you received from the same company. To verify the legitimacy of a link, move the mouse pointer over it and observe what appears.

- **Suspicious Attachments.** Emails with attachments should always be treated suspiciously – especially if they have an unfamiliar extension or one commonly associated with malware (.zip, .exe, .scr, etc.), they are unexpected or you do not recognize the sender.

- **Emails requesting Login Credentials or critical information.** Emails originating from an unexpected or unfamiliar sender that requests login credentials, payment information or other sensitive data should always be treated with caution, It is possible to develop fictitious login sites that resemble the real thing and send emails with links that take recipients to the bogus website.

- **Too good to be true emails** are those which incentivize the recipient to click on a link or open an attachment by claiming there will be a reward of some nature. If the sender of the email is unfamiliar or the recipient did not initiate the contact, the likelihood is this is a phishing email.

Immediate Actions: Step-by-step first response actions once crypto-jacking is detected

According to Europol's guidelines, If an individual clicks on something, there are potential consequences:

- **Malware Infection:** Opening attachments or clicking on links may lead to a malware infection on their system.
- **Unauthorized Access:** Providing login credentials could grant criminals access to sensitive information.
- **Financial Compromise:** Sharing bank details might result in criminals gaining access to their finances.

If someone realizes or suspects that he/she has fallen victim to a phishing email, a few steps need to be taken:

- **Account passwords should be changed**, especially if a phishing attack that spoofed a login portal is encountered. The email might have contained a link redirecting to a page that appeared familiar, asking for login credentials. While seeming legitimate, logging in on this fake page may have sent the credentials to the attacker. If this occurs, the compromised passwords should be changed across relevant accounts.
- **Disconnect** from the network any computer or device that's infected with malware.
- Phishing incidents should be **reported** immediately. As these attacks are often executed in bulk, targeting individuals with similar traits, reporting promptly can prevent further compromises. Incidents should be reported to the IT service desk or in accordance with the organization's cyber incident response policies, aiding the information security team in gathering crucial information about the attack.
- **Alert others colleagues**

Phishing attacks often happen to more than one person in a company.

- A **thorough investigation** of the phishing attack is essential. IT teams need to conduct a preliminary investigation upon receiving the report to determine the attack's scope and severity. Besides assessing the number of affected individuals, efforts should be made to remove the phishing email from users' inboxes. Consequences, ranging from compromised email accounts to unauthorized access to the organization's network, should be thoroughly examined. Victims should also be cautious of potential identity theft and take necessary measures, such as blocking or monitoring other accounts for unusual activities.

- **Regulatory authorities and law enforcement** should be informed Depending on the severity, filing a case with the appropriate law enforcement agency, may be necessary.

- **Remediation strategies** should be discussed with the IT team. To prevent future incidents, organizations must ensure that employees are well-informed about likely attack methods. Comprehensive security education and training can enhance employee readiness, and internal phishing scam simulations can be effective in identifying and avoiding phishing emails. Technical safeguards, such as email filtering, sandboxing, machine learning models, and browser isolation, should be considered by the IT team to enhance email security beyond basic spam filtering provided by email service providers like Microsoft Outlook, Gmail, and Apple.

To mitigate these risks, should be considered the following actions:

- **Utilize Antivirus Software**: Install antivirus software on all electronic devices.
- **Keep Software Updated**: Ensure that both security software and operating systems receive regular updates.
- **Create Unique Passwords:** Establish unique passwords for each online account.
- **Exercise Caution**: It's advisable to think twice before clicking on links or opening attachments, as criminals may attempt phishing or smishing attacks. If uncertain, it is recommended to refrain from clicking, opening, or providing financial information.
- **Direct Access to Online Banking**: Access online banking directly through official webpages or apps, avoiding third-party links.
- **Regularly Check Financial Accounts**: Monitor financial accounts for suspicious activity or unauthorized charges. Setting up alerts and security measures with their bank can provide notifications about transactions, preventing unexpected access and money transfers. Collaboration with the bank is essential for implementing these protective measures.

Reporting Protocols: Who and how to report the incident to authorities or internal IT departments

Reporting a cyber incident is crucial to address and mitigate potential threats. The specific steps and authorities to report to may vary based on the victim’s location, the nature of the incident, and the policies of organization. Here are some general guidelines:

Internal IT Department:

- **Contact IT Helpdesk or Service Desk:**

- Inform the organization's internal IT department as soon as possible.
- Provide details about the incident, such as when it occurred, any suspicious emails or messages, and actions that may have been taken.

External Authorities:

- **Law Enforcement:**

If the incident involves criminal activities such as hacking, fraud, or theft, it is crucial to report the incident to a local law enforcement agency. Law enforcement agencies have the expertise and authority to investigate and take action against criminal activities. Reporting the incident promptly helps in initiating investigations and may contribute to preventing further harm.

Reporting Guidelines:

The sooner an incident is reported, the quicker and more effectively it can be addressed.

- **Follow Organizational Policies:**

As many, organizations have specific protocols for reporting security incidents, comply with the internal incident reporting policies of the organization.

- **Document the Incident:**

A comprehensive account of the incident, complete with timestamps, detailed descriptions of activities, and pertinent communications and screenshots, needs to be documented.

- **Preserve Evidence:**

Logs, emails, or any other relevant data that might assist in the investigation, should be preserved.

- **Use Secure Channels:**

When reporting the incident, use secure and official communication channels to prevent further compromise.

- **Involve Higher Management if Necessary:**

Depending on the severity of the incident, inform higher management within an organization.

This project was funded by the European Union's Internal Security Fund - Police Programme under Grant Agreement No 101038738