Phishing Awareness Training

By: Farah Ahmed Othman

Overview

- Introduction
- Different Types of Phishing
- How to recognize phishing emails,websites, and social engineering tactics
- How to avoid phishing emails,websites, and social engineering tactics

Introduction

•Phishing is a kind of CyberAttack in which malevolent actors send messages purporting to be reliable sources or individuals. Phishing messages trick a user into doing things like downloading a malicious file, opening a malicious link, or disclosing private information like login credentials.

A message sent via email, social media, or another electronic communication method is the fundamental component of a phishing attack.

•Public resources, particularly social networks, can be used by phishers to learn more about their victim's background, both personally and professionally. These sources are used to obtain details about the potential victim, including name, occupation, email address, and hobbies and pastimes. With this data, the phisher can then craft a trustworthy fake message.

The victim typically receives emails that seem to be from a reputable person or business. Malicious attachments or links to malicious websites are used to carry out attacks. Attackers frequently create fake websites that seem to be run by reliable organizations, such as the victim's bank, place of employment, or university. Attackers try to obtain sensitive data, such as payment details or usernames and passwords, through these websites.

Different Types of Phishing

1.Email phishing

This kind of phishing assault is the most prevalent one. Attackers send emails that seem to be from reliable sources, such as internet businesses, banks, or social networking platforms. These emails frequently have an urgent feel to them, asking the recipient to download an attachment or click on a link in order to confirm details or claim a prize.

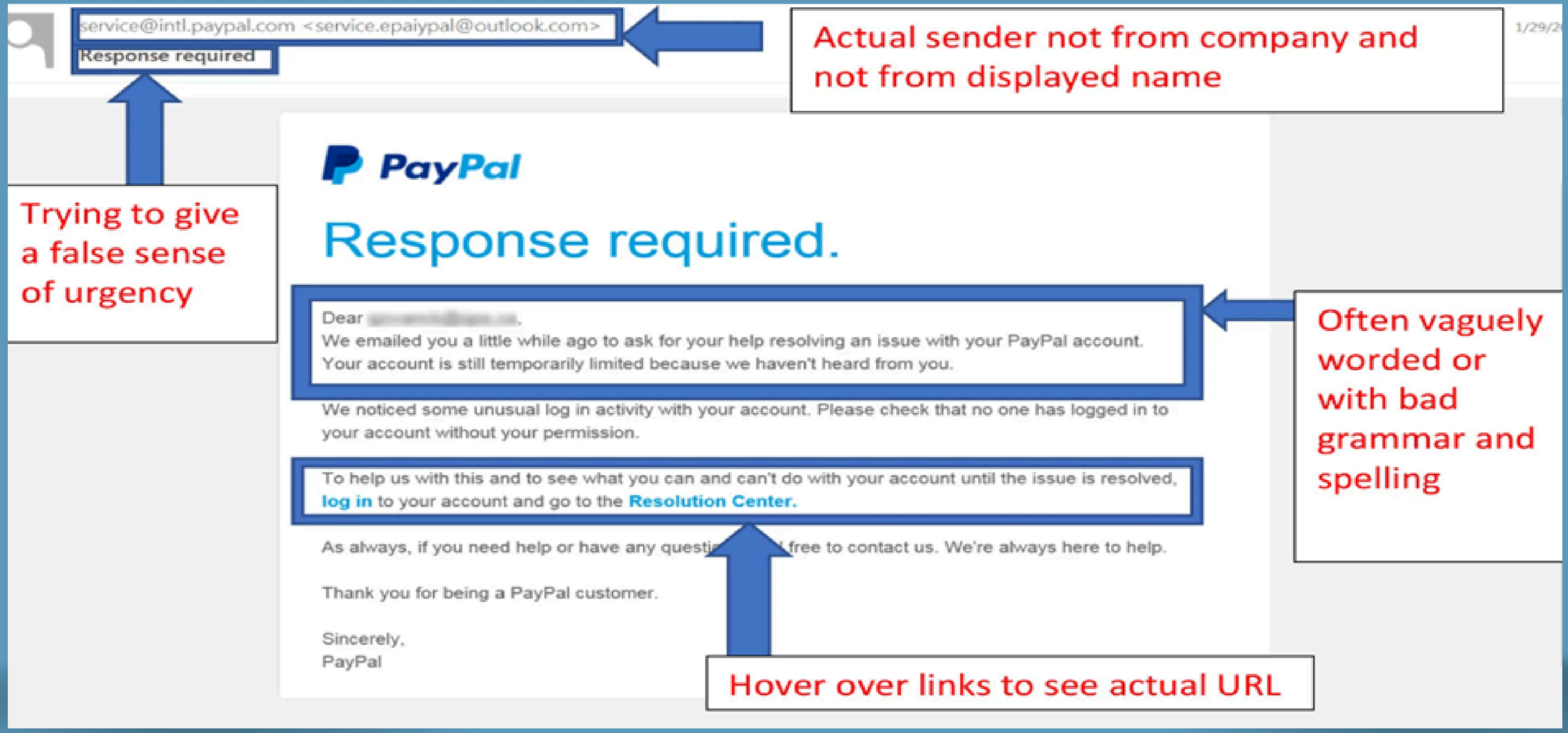
2.Spear Phishing

phishing is targeted at specific individuals as opposed to regular phishing, which targets a wider audience. Attackers use personal information to make their emails seem more credible by customizing them to a particular person or business. Attacks of this kind are frequently employed in corporate espionage or to obtain access to particular systems.

3.Whaling

One form of spear phishing called "whaling" targets prominent people such as executives or senior management in an organization. The emails are designed to look like important business correspondence and frequently deal with fictitious tax returns, subpoenas, or other legal issues.

Anatomy of a Phishing Email



4.Smishing

Smishing, also known as SMS phishing, is the practice of sending phony text messages that seem to be from reliable sources. Usually, these messages include a phone number or link that leads to a scammer acting as an official representative or a phony website.

5.Vishing

Vishing, often known as voice phishing, happens over the phone. Attackers phone victims and pose as representatives of respectable companies, including banks or government agencies, in an attempt to coerce them into sending money or divulging personal information.

6.Clone phishing

Clone phishing involves hackers making a nearly exact replica of a real email that the target has already received. Malicious attachments or links are present in the copied email, and the attack frequently seems to originate from a reliable person.

How to recognize phishing emails

01

1. Suspicious Sender Address: Verify the email address associated with the sender. Phishing emails frequently originate from addresses that resemble real ones but may contain additional characters or little spelling errors

02

2. Generic Greetings: Frequently, phishing emails begin with "Dear Customer" or "Dear User" rather than your name.

03

3. Urgent or Threatening Language: Be cautious when responding to emails that incite anxiety or a sense of urgency, such as alerts concerning account closures or security lapses.

04

4. Suspicious Attachments or Links: Steer clear of downloading attachments or clicking links from unidentified or dubious sources. Before clicking, hover over links to get the full URL.

05

5. Spelling and Grammar Errors: A lot of phishing emails have punctuation, spelling, or grammar errors

How to avoid phishing emails

1. Use Email Filters : Turn on the spam filters that your email provider offers. These can be used to recognize and weed out possible phishing emails.

2. Verify Sources : Contact the organization directly using a reputable phone number or official website to independently confirm the email's validity.

3. Be Skeptical : Always treat unsolicited emails with caution, particularly if they seem urgent or offer incentives.

4. Keep Software Updated : To guard against malware and other risks, make sure your email client, browser, and security software are up to date.

5. Teach Others and Yourself : Keep up with the most recent phishing tactics, and teach your loved ones, acquaintances, and coworkers how to spot and steer clear of phishing frauds.

How to recognize phishing Websites

01

* Search for misspellings: Phishing websites frequently employ URL that resemble authentic websites but have minor misspellings or extra characters.
* Check the domain: Make sure the domain name matches the official website and is correct.

02

*Poor design quality: Phishing sites often have low-quality graphics, fonts, and overall design compared to legitimate websites.
*Suspicious pop-ups and ads: Abnormal or excessive pop-ups may raise suspicions.

03

*Spelling and grammar errors :Well-written content is a hallmark of legitimate websites, whereas phishing sites frequently have glaring faults.

04

*Inadequate contact details: Reputable websites often offer a physical address, phone number, and email address.
*Inactive hyperlinks: Test a few of the website's links. It's a red flag if a large number of them are broken or point to irrelevant pages

05

*Examine the following website: Search for user reviews and comments. Reputable websites will be active on social media, in forums, and review sites.

How to avoid phishing Websites

1. Employ security software:
* Use anti-virus and anti-phishing programs : Use anti-phishing tools and make sure your antivirus software is up to date.
*Browser extensions : Install browser extensions that have the ability to identify and prevent phishing websites.

2. Be Wary of Emails:
*Avoid clicking on dubious links : Steer clear of clicking on links or downloading attachments from emails that are unfamiliar or unwanted.
* Confirm the sender: Examine the email address of the sender thoroughly. Phishing emails frequently originate from addresses that look real.

3. Two-Factor Authentication (2FA) should be enabled: To increase security and make it more difficult for phishers to access your accounts, turn on two factor authentication (2FA).

4. Educate Yourself and Others:
* Stay informed : Keep up-to-date with the latest phishing tactics and share information with friends, family, and coworkers.

5. Make use of bookmarking:
* Bookmark reliable websites : To minimize the likelihood of seeing a phishing website, use bookmarks instead of inputting the URL to access regularly frequented websites.

How to recognize social engineering tactics

01

1. Pretexting: To get information, the attacker fabricates a situation. Confirm the identification of anyone requesting private or sensitive data.

02

2. Baiting: Alluring promises (like free software or movie downloads) that result in malware. Offers that look too good to be true should be avoided.

03

3. Quid Pro Quo: Attackers request information in return for a service or other advantage. Check the validity of these offers before accepting them.

04

4. Tailgating: Unauthorized people enter security locations after authorized personnel. Make sure that nobody enters restricted areas unless they are allowed.

05

5. Impersonation: Attackers assume the identity of a reliable person, like a coworker or a superior. Always use official channels to confirm identity.

How to avoid social engineering tactics

1. Be Skeptical: Exercise caution while responding to unwanted communications. Something is probably off if it feels that way.

2. Verify Identities: Make sure that anyone requesting sensitive information or access is who they say they are by using official methods.

3. Education and Training: Consistently teach yourself and your staff how to spot social engineering ploys. Phishing attack simulations can be an effective teaching tool.

4. Make Robust, Distinct Passwords: Steer clear of utilizing the same password on several websites. To remember secure, one-of-a-kind passwords, use a password manager.

5. Activate Two-Factor Authentication (2FA): Give your accounts an additional layer of protection to ward off illegal access.

THANK YOU!