PHISHING AWARENESS TRAINING CODEALPHA INTERNSHIP

Phishing attacks, recognizing and avoiding phishing emails, websites, and social engineering tactics.

OVERVIEW

1 Introduction

2 Types of Phishing Attacks

3 Phishing Attacks in Social Media

4 Ways to Detect Phishing Attacks

5 Prevention of Phishing Attacks

What is a Phishing Attack ?

- Phishing is a type of cybercrime in which an attacker impersonates a legitimate individual or organization by presenting themselves as an official entity through email or other communication channels. It involves the fraudulent collection of sensitive information from the victim and its subsequent misuse.

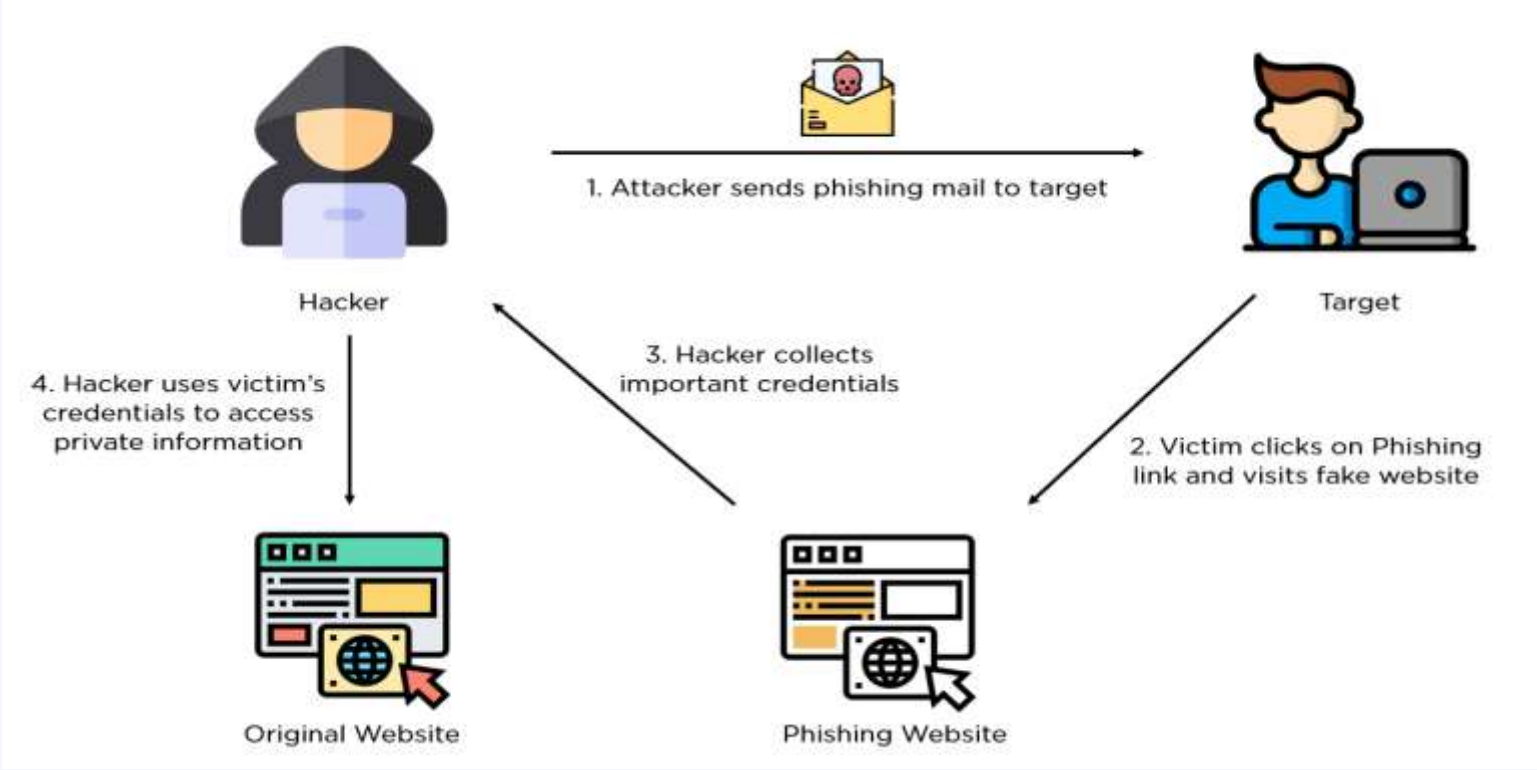
- In this form of attack, the attacker sends deceptive emails containing malicious links or attachments that can perform actions such as stealing login credentials or account details. Social engineering is the most commonly used technique by attackers to trick victims into revealing personal information and account credentials.

- Phishing attacks often exploit the victim's trust, creating a sense of urgency or offering rewards to prompt quick actions. These attacks can lead to severe consequences, such as identity theft, financial loss, or unauthorized access to sensitive data. It is crucial to remain vigilant and verify the authenticity of any unsolicited communication to prevent falling victim to phishing scams.

What is a Phishing Attack ?

- In general, the information that is stolen by a phishing attack is either an User account number, User passwords and user name, Credit card information, Internet banking information.
- Phishing is mainly used in email hacking. The process can be seen in the image beside.
- The Cycle of Phishing Attacks considering the example of Phishing E-Mail can be seen in the beside image.

WHAT IS A PHISHING ATTACK ?



Types of Phishing Attacks

DECEPTIVE PHISHING

- Deceptive phishing is a type of cyber attack where scammers create fake emails or websites that look like they come from trusted sources, such as banks or social media platforms.
- They aim to trick individuals into providing sensitive information like usernames, passwords, or financial details.
- The attackers often use urgency or threats to make victims act quickly without verifying the legitimacy of the communication.

❖ **Spear Phishing**

- Spear phishing is a targeted form of phishing where attackers customize their messages for specific individuals or organizations.
- Unlike general phishing, which casts a wide net, spear phishing involves in-depth research to make messages appear highly personalized and trustworthy.
- It often involves social engineering tactics and is more sophisticated than traditional phishing attempts.

Types of Phishing Attacks

CLONE PHISHING

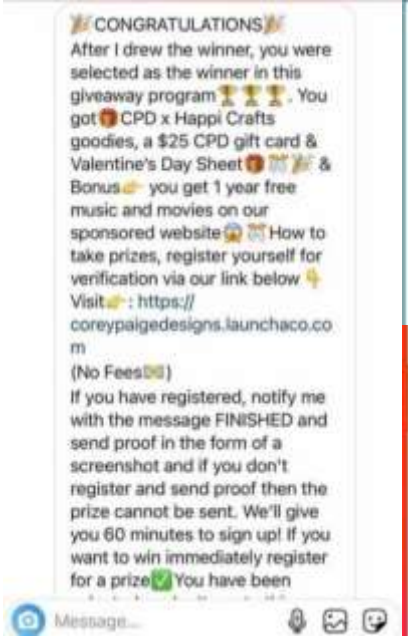
- Clone phishing is a specific type of phishing attack where cybercriminals create a nearly identical or "cloned" copy of a legitimate email or website.
- The cloned content typically mimics a legitimate message or webpage from a trusted source, such as a bank, social media platform, or a reputable organization.
- Clone phishing relies on the familiarity of the duplicated content to deceive recipients, making it challenging for them to distinguish between the genuine and the malicious.

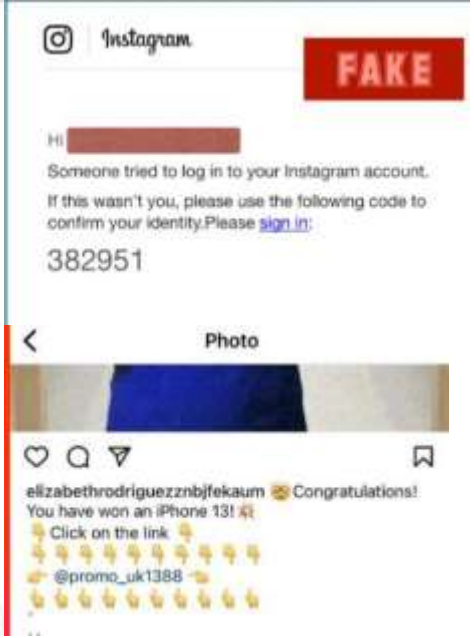
❖ **Whaling**

- Whaling refers to a specific type of phishing attack that targets high-profile individuals or executives within an organization.
- Whaling aims to trick these influential figures into taking actions that could compromise sensitive information or financial assets.
- Whaling attacks typically involve social engineering tactics and careful research to make the fraudulent communications appear legitimate.

PHISHING ATTACKS IN SOCIAL MEDIA

- Launching a giveaway via a fake brand account.
- Impersonating an official account and contacting you via DM or email with a warning or request for information.
- Making you a tempting offer and providing a link that directs you to a website scammers control.
- Fake 2FA codes





Ways to detect Phishing Attacks

USE A CUSTOM DNS SERVICES

- It involves leveraging a specialized Domain Name System provider that offers enhanced security features.
- These services can filter out known malicious domains, block access to phishing sites, and provide real-time analysis to identify emerging threats.
- Custom DNS allows organizations to set up tailored security policies, log and report DNS activities and also adds an extra layer of protection against phishing attacks by preventing users from accessing potentially harmful websites.

❖ **Use your Browser's phishing list**

- Your browser's phishing protection utilizes a list of known malicious websites to warn and block users from accessing potential phishing sites in real-time.
- Ensure this feature is enabled, stay updated with browser versions, and pay attention to warnings issued by the browser.

Ways to detect Phishing Attacks

USE SITES TO CHECK LINKS

- When working on any site or any program there is a popping of different kinds of links, orin case you're presented a link or which you are not so sure, you can copy and check it on a number of different site
- Use URL Scanners: Services like VirusTotal or URLVoid analyze links against multiple security databases.
- Link Analysis Tools: Tools like CheckShortURL or GetLinkInfo help analyze and preview shortened URLs

❖ **Use your own Ninja skills**

- Look for secure connections: This is usually identified by a green area in the address bar, along with https in URL.
- Look at the domain of URL Look at the domain that it should not be modified or changed.

Preventing Phishing Attacks

GUARD AGAINST SPAM

- Enable Built-in Spam Filters: Ensure that the spam filters in your email service are activated and configured effectively.
- Use Advanced Threat Protection (ATP): Consider advanced security solutions that provide additional layers of protection against advanced threats.
- Implement Multi-Factor Authentication (MFA): Add an extra layer of security to prevent unauthorized access, even if credentials are compromised.

❖ **Communicate personal information only via phone or secure web sites**

- In this type of phishing prevention, the user should be aware of while conducting online transactions, look for the secured sign on the browser status bar or" https." URL where the "s" stands for "secure" rather than' http."

Preventing Phishing Attacks

DO NOT CLICK ON LINKS, DOWNLOAD FILES OR OPEN ATTACHMENTS IN EMAILS FROM UNKNOWN SENDER

- It is always best to secure any data properly such as bank details any social media details, in emails also open the attachment only if when you are expecting them and known what that attachment contains even if you the sender
- It's essential to verify the sender's identity and use email filters to
- identify and block suspicious emails.

❖ **Sound security policies**

- In the big organizations or companies, you should set some rules as to how you should respond to strange or out of place emails and requests.
- Your company’s policy should also show people what to do in case they see something out of place.
- Verifying information over the phone adds an extra layer of security.

REFERENCES

- https://ieeexplore.ieee.org/abstract/document/8852647
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742
- https://ieeexplore.ieee.org/abstract/document/9529789
- https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full
- https://www.sciencedirect.com/science/article/abs/pii/S0957417418302070


Thank
you!