-CODE ALPHA

PHISHING AWARENESS

- PHISHING IS TYPE OF CYBER ATTACK 🤦 🔒

PRESENTED BY : ROHINI KAMBLE

What is Phishing Attack

A **phishing attack** is a type of cybercrime where attackers attempt to trick individuals into revealing sensitive information, such as login credentials, credit card numbers, or personal details, by impersonating a trustworthy entity. Phishing attacks are typically carried out through email, social media, phone calls, or fake websites. These attacks often look legitimate, making it difficult for the victim to recognize that they are being deceived.

TYPES OF PHISHING ATTACK

- Email Phishing
- Spear Phishing
- Whaling
- Vishing (Voice phishing)
- Smishing (SMS phishing)

❑ Email Phishing

Description: The most common type of phishing, where attackers send fraudulent emails that appear to come from a legitimate source (like a bank, company, or government organization). These emails often contain urgent requests, such as needing to verify account details or reset a password.

Characteristics:

- Generic greetings like "Dear Customer."
- Suspicious links that lead to fake websites.
- Attachments that may contain malware or viruses.

❑ Spear Phishing

Description: A more targeted form of phishing. Unlike generic email phishing, **spear phishing** is directed at specific individuals or organizations. Attackers use personalized information (such as names, job titles, or organizational details) to make the attack seem more legitimate.

Characteristics:

- Highly personalized emails.
- Custom-built messages tailored to the victim's profile or role in an organization.
- Often used to gain access to confidential or corporate data.

❑ Smishing (SMS Phishing)

Description: A phishing attack carried out via SMS (text messages). The attacker sends fraudulent text messages that appear to be from a legitimate source, asking the recipient to click on a malicious link or provide personal information.

Characteristics:

- Text messages that ask recipients to follow a link or call a number.
- Often includes time-sensitive requests or offers to trick victims into acting quickly.
- Messages may look like they are from banks, delivery services, or government agencies.

❑ Angler Phishing

Description: A newer form of phishing that exploits social media platforms. Attackers create fake social media accounts or websites that look like legitimate brands or customer service accounts. They then engage with users who may be seeking help, directing them to fake websites or asking for sensitive information.

Characteristics:

- Attackers impersonate legitimate companies or organizations on platforms like Twitter, Facebook, or Instagram.
- Often involves fake customer service accounts that respond to questions or complaints.
- Links sent via social media messages lead to fraudulent websites designed to steal information.

❑ Whaling

Description: This is a type of spear phishing that specifically targets high-profile individuals, such as executives or key personnel in a company (often referred to as the "big fish"). The attackers may pose as trusted partners, vendors, or even internal employees to gain access to sensitive information or financial resources.

Characteristics:

- High-level, executive targets (CEOs, CFOs, etc.).
- The attack is often more sophisticated and may involve legal or business jargon.
- Aimed at stealing large amounts of money or confidential company information.

❑ Vishing (Voice Phishing)

Description: Vishing involves phone calls or voicemail messages instead of emails. The attacker impersonates a trusted entity (like a bank or government official) and attempts to convince the victim to divulge personal or financial information.

Characteristics:

- Phone calls from someone claiming to be from a legitimate organization.
- Often creates a sense of urgency, such as claiming the victim's bank account has been compromised.
- May ask the victim to enter personal information using an automated system or talk directly to a scammer.

.

HOW PHISHING ATTACK HAPPENED

A phishing attack typically follows a series of steps designed to deceive victims into revealing sensitive information. Here's a breakdown of how a phishing attack usually happens:

1. Preparation and Planning:

•**Researching the Target:** Phishers often gather information about their target. This could involve researching an individual's or organization's habits, interests, and digital footprints on social media or websites to make the attack more convincing.

•**Creating Fake Communication:** The attacker then creates a message that looks like it's from a trusted entity, such as a bank, tech company, or government agency. This message might be an email, text (smishing), or even a phone call (vishing).

2. Delivery of the Phishing Message:

•**Email (Most Common):** The most frequent method of phishing is through email. The attacker sends an email that looks legitimate. This might involve:

- **Spoofing the sender's address** to resemble a known contact or company.
- **Creating a compelling subject line** to grab attention, such as "Urgent: Account Suspended!" or "Your Prize Awaits."

3. Deceptive Content and Urgency:

•The phishing message often contains a **sense of urgency**, making the recipient feel they need to act quickly to resolve an issue (e.g., an account has been locked, or a prize needs to be claimed immediately).

•The message may also include:

- A **link to a fraudulent website** designed to look like a legitimate one (e.g., a fake bank login page or social media account recovery page).
- A **malicious attachment** that, when opened, installs malware or ransomware on the victim's device.
- **Requests for personal information**, like usernames, passwords, credit card numbers, or Social Security numbers.

4. Exploiting the Victim:

•**Clicking on a Link:** If the victim clicks on a link in the phishing message, they are taken to a **fake website** that looks almost identical to a real one (e.g., a bank's login page). The attacker uses the site to capture the victim's login credentials.

•**Opening an Attachment:** If the message contains an attachment, opening it might install **malware** on the victim's device. This could enable the attacker to steal information, monitor activities, or gain unauthorized access to personal data.

5. Stealing Information:

•Once the victim enters their sensitive information, the attacker collects it and can use it for various malicious activities, such as:

- **Accessing bank accounts** or making unauthorized transactions.
- **Stealing identities** and committing fraud.
- **Selling the information** on the dark web.

AWARENESS ABOUT PHISHING ATTACK

Awareness about phishing attacks is crucial for protecting personal and organizational data from cybercriminals. Phishing is one of the most common and effective methods of cyberattacks. Here's an overview of phishing attacks and how you can stay aware to protect yourself:

1. What is Phishing?

Phishing is a type of cyberattack where attackers use deceptive messages (usually emails, text messages, or phone calls) to trick individuals into providing sensitive information such as passwords, bank details, or personal identification numbers (PINs). The attacker often impersonates a trusted entity, such as a bank, company, or government agency, to create a sense of legitimacy.

Common Phishing Techniques:

- **Impersonating Trusted Sources:** Attackers often pose as reputable companies, such as your bank, social media platforms, or government services, making the message look authentic.
- **Urgency and Threats:** Phishing messages frequently create a sense of urgency or fear, such as "Your account has been compromised!" or "Immediate action required!" to trick the victim into acting quickly without thinking.
- **Malicious Links:** Phishing emails often include links that appear to lead to legitimate websites, but when clicked, they redirect to fake websites designed to steal your login credentials or infect your device with malware.
- **Attachments with Malware:** Phishing emails may include attachments that, when opened, install malware on your device. This malware could steal information, spy on you, or damage your system.

Signs of a Phishing Attack:

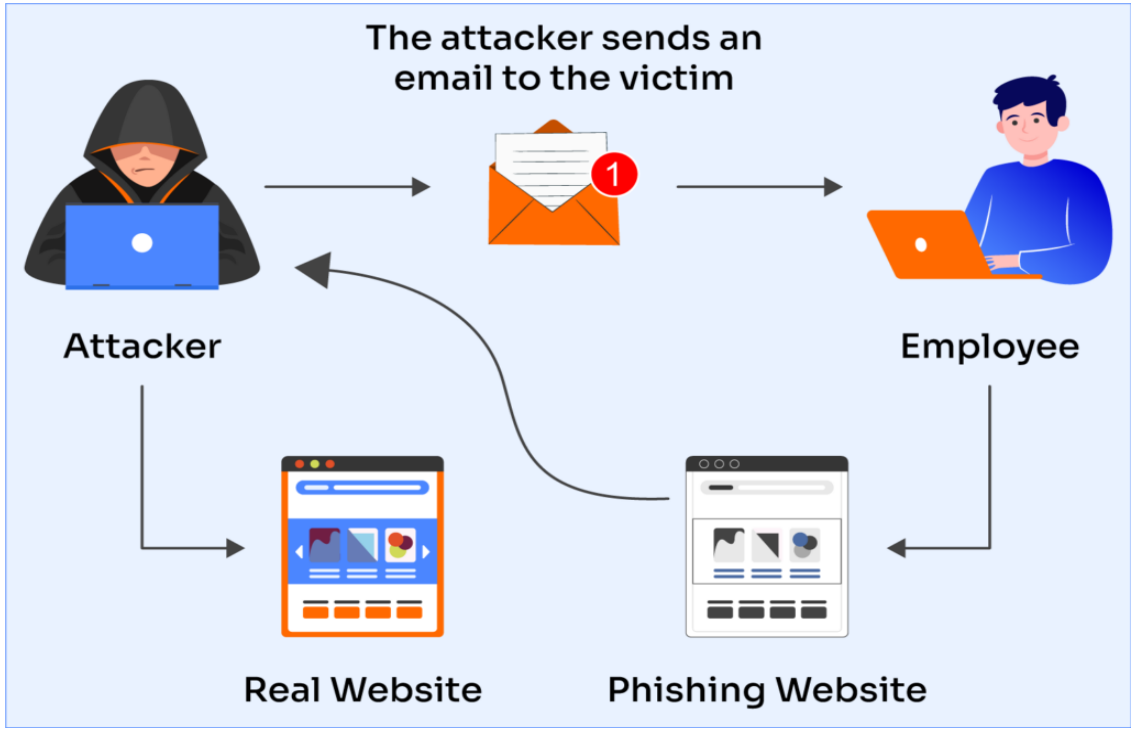
•**Suspicious Sender:** Check the sender's email address carefully. Often, phishing emails will have slight misspellings or unfamiliar domains.

•**Generic Greetings:** Phishing emails often use generic greetings such as "Dear Customer" or "Dear User" rather than using your name.

•**Urgent Requests:** Any email or message that creates a sense of urgency or threatens consequences if you don't act quickly is suspicious. Always take a moment to verify before clicking anything.

•**Unusual Links or Attachments:** Hover over any links to see where they lead before clicking. Never download attachments from unknown or unsolicited sources.

•**Spelling and Grammar Mistakes:** Many phishing emails contain noticeable spelling, punctuation, or grammar errors, which can be a red flag.



How to Protect Yourself from Phishing:

- **Verify the Source:** If you receive an unsolicited email or message from a company, bank, or government agency, don't click on any links or download attachments. Instead, contact the organization directly using known, legitimate contact details.
- **Check the URL:** Before entering personal information, check the website's URL. Authentic websites start with "https://" and have a secure lock symbol in the address bar. Be cautious of websites that have misspelled URLs or strange domain names.
- **Avoid Clicking on Links or Attachments:** Never click on links or open attachments in unsolicited emails, especially if they seem too good to be true or urge immediate action.
- **Enable Two-Factor Authentication (2FA):** Protect your online accounts with two-factor authentication whenever possible. This adds an extra layer of security even if your login details are compromised.
- **Keep Software Updated:** Ensure that your operating system, antivirus software, and browsers are up to date. Security patches help protect your system from malware and other vulnerabilities that phishing attacks can exploit.
- **Use Anti-Phishing Tools:** Many email providers, browsers, and security software offer built-in phishing protection, such as warning messages about suspicious links or websites.
- **Educate and Train Yourself and Others:** Regularly educate yourself and others (especially employees, in a workplace setting) about how to identify phishing attacks and handle suspicious emails or messages.

What to Do if You Suspect a Phishing Attack:

- **Do Not Respond or Click Anything:** If you suspect an email or message is a phishing attempt, do not respond or click any links. Simply delete the message.
- **Report It:** If you receive a phishing email, report it to the legitimate organization (e.g., your bank or email provider). Many organizations have specific channels for reporting phishing.
- **Change Your Passwords:** If you've clicked on a link or entered your credentials on a suspicious site, change your password immediately. If you've used the same password elsewhere, change those as well.
- **Run Antivirus Software:** If you suspect your device is compromised, run antivirus software to scan for malware and remove any threats.

Why Phishing is Effective:

- **Psychological Manipulation:** Phishing attacks often rely on human psychology, such as fear, curiosity, or greed. Victims are tricked into acting impulsively, which is why phishing attacks can be so effective.
- **Ease of Execution:** Phishing attacks are relatively easy for cybercriminals to carry out. All they need is access to a mass email list and the ability to create convincing fake messages.

CONCLUSION

Awareness is key to preventing phishing attacks. By understanding how phishing works, recognizing the signs, and adopting best practices for online security, individuals and organizations can significantly reduce the risk of falling victim to these scams.
Stay cautious, and always verify the authenticity of suspicious communications.

THANK YOU