PHISHING AWARENESS TRAINING MODULE

IMPORTANCE OF CYBERSECURITY

PREVALENCE OF PHISHING ATTACKS

Presented by Priyanshi Das

INTRODUCTION TO PHISHING AS A CYBER ATTACK

DEFINITION:

- "Phishing is a type of cyber attack where attackers impersonate legitimate organizations or individuals through email, text messages, or websites to steal sensitive information such as usernames, passwords, credit card numbers, and other personal data."

- "These deceptive messages often appear to be from trusted sources, such as banks, online services, or even colleagues, making it challenging to recognize their fraudulent nature."

The main motive of the attacker behind phishing is to gain confidential information like:

- Password
- Credit card details
- Social security numbers
- Date of birth

EXAMPLES:

Common types include email phishing, spear phishing, and smishing (SMS phishing).

PURPOSE OF PHISHING AND HOW IT WORKS ?

PURPOSE:

The goal of phishing is to deceive individuals into providing confidential information or installing malicious software.

WORKING:

- Initial Contact: The attacker sends a fraudulent message, typically via email, SMS, or social media.
- Deception: The recipient is tricked into clicking a malicious link or opening an infected attachment.
- Action: The victim is either asked to provide sensitive information on a fake website or unknowingly installs malware.
- Exploitation: The attacker uses the stolen information for fraudulent activities or gains unauthorized access to systems.

TYPES OF PHISHING

TYPES:

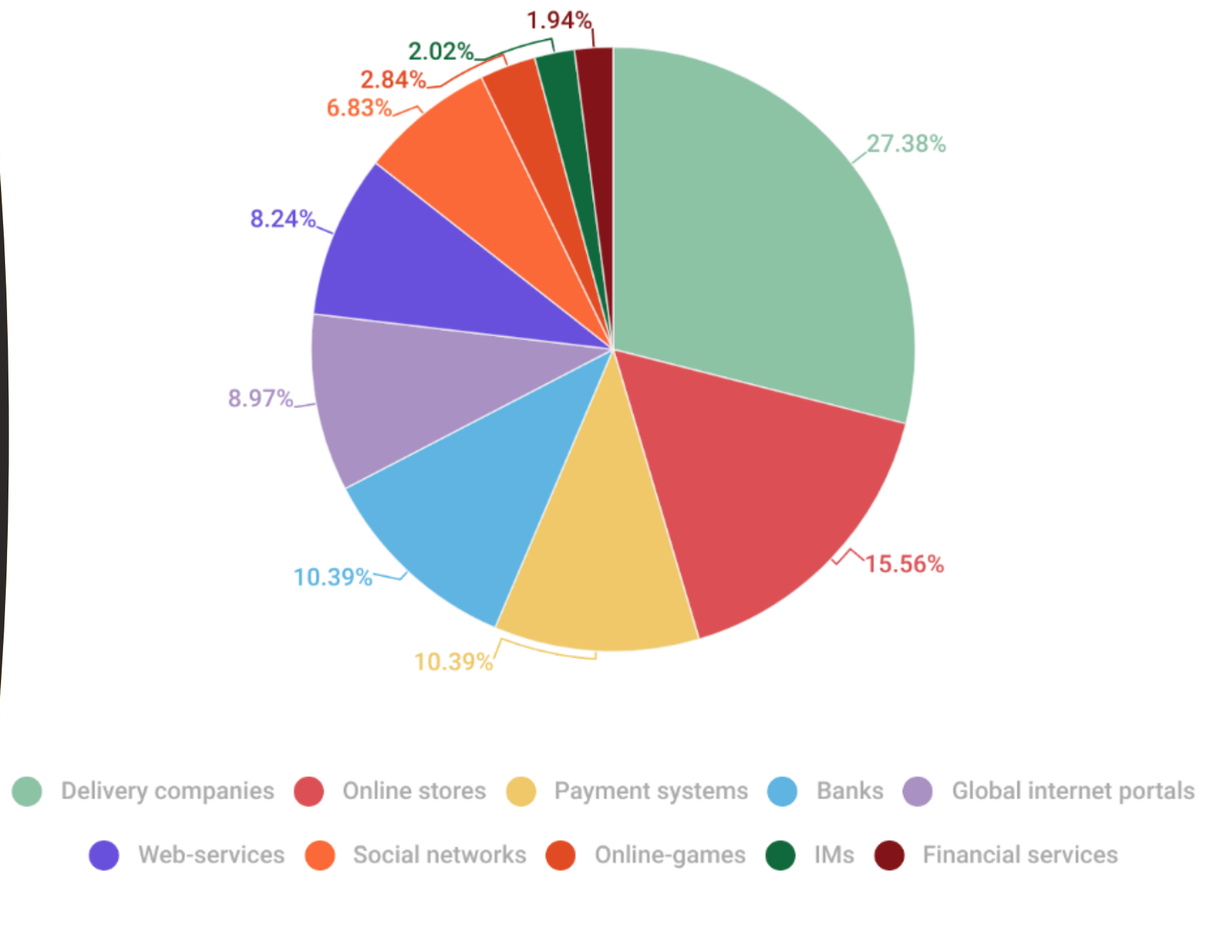
- **Email Phishing**: The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims.
- **Spear Phishing**: A particular user(organization or individual) is targeted. The attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data.
- **Whaling**: It is just like spear-phishing but the main target is the head of the company, like the CEO, CFO, etc. A pressurized email is sent to such executives so that they don't have much time to think, therefore falling prey to phishing.
- **Smishing**: The medium of phishing attack is SMS. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is then invited to enter their personal information like bank details, credit card information, user ID/ password, etc. Then using this information the attacker harms the victim.
- **Vishing**: Vishing is also known as voice phishing. The attacker calls the victim using modern caller ID spoofing to convince the victim that the call is from a trusted source. It is generally used to steal credit card numbers or confidential data from the victim.
- **Clone Phishing**: The attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

THE IMPACT OF PHISHING

IMPACT:

Phishing attacks can have severe consequences for both individuals and organizations:

- Financial Loss: Victims can lose money directly through fraudulent transactions.
- Identity Theft: Attackers can use stolen personal information to open accounts, make purchases, or commit other fraud.
- Data Breaches: Sensitive information from businesses can be compromised, leading to further attacks and loss of confidential data.
- Reputation Damage: Organizations that suffer phishing attacks may lose customer trust and suffer long-term reputational harm.



ANTI-PHISHING TOOLS

Anti-Phishing Tools

Well, it's essential to use Anti-Phishing tools to detect phishing attacks. Here are some of the most popular and effective anti-phishing tools available:

- **Anti-Phishing Domain Advisor (APDA)**: A browser extension that warns users when they visit a phishing website. It uses a database of known phishing sites and provides real-time protection against new threats.
- **PhishTank**: A community-driven website that collects and verifies reports of phishing attacks. Users can submit phishing reports and check the status of suspicious websites.
- **Webroot Anti-Phishing**: A browser extension that uses machine learning algorithms to identify and block phishing websites. It provides real-time protection and integrates with other security tools.
- **Malwarebytes Anti-Phishing**: A security tool that protects against phishing attacks by detecting and blocking suspicious websites. It uses a combination of machine learning and signature-based detection to provide real-time protection.
- **Kaspersky Anti-Phishing**: A browser extension that provides real-time protection against phishing attacks. It uses a database of known phishing sites and integrates with other security tools to provide comprehensive protection.

Note: These anti-phishing tools can provide an additional layer of protection against phishing attacks, but it is important to remember that they are not a complete solution. Users should also be cautious of suspicious emails and messages and practice safe browsing habits to minimize their risk of falling victim to phishing attacks.

HOW TO STAY PROTECTED AGAINST PHISHING?

- **Authorized Source:** Download software from authorized sources only where you have trust.
- **Confidentiality**: Never share your private details with unknown links and keep your data safe from hackers.
- **Check URL**: Always check the URL of websites to prevent any such attack. it will help you not get trapped in Phishing Attacks.
- **Avoid replying to suspicious things**: If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.
- **Phishing Detection Tool**: Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.
- **Try to avoid free wifi**: Avoid using free Wifi, it will lead to threats and Phishing.
- **Keep your system updated**: It's better to keep your system always updated to protect from different types of Phishing Attacks.
- **Keep the firewall of the system ON**: Keeping ON the firewalls helps you filter ambiguous and suspicious data and only authenticated data will reach you.

CONCLUSION

Therefore, phishing attacks are a serious problem that can steal your data. When it comes to your personal information, always confirm the person requesting for your data. If you are not sure whether the request is genuine or fraudulent, never share any personal information. Always stay alert to avoid such tricks and protect yourself from fraudsters.
Educating users on phishing is crucial for enhancing cybersecurity. By understanding what phishing is, how it works, and its potential impact, individuals can better protect themselves and their organizations from these malicious attacks.