PHISHING ATTACKS

SHUSHMA PRIYA VADLAMANU

TABLE OF CONTENTS

INTRODUCTION TO PHISHING

What is Phishing

Definition: Phishing is a type of cyber attack where attackers disguise themselves as trustworthy entities to steal sensitive information.

Types of Phishing Attacks

- Email Phishing: The most common form, where attackers send fraudulent emails to trick recipients into providing personal information.
- Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
- Whaling: Phishing attacks aimed at senior executives or high-profile targets.
- Smishing: Phishing attacks conducted via SMS text messages.
- Vishing: Phishing attacks conducted via voice calls.

RECOGNIZING PHISHING EMAILS

Email phishing attacks are fraudulent messages that appear to come from a legitimate source, typically through email, to steal sensitive data or install malware. The goal is to trick the recipient into revealing information like login credentials or credit card numbers, or to transfer money.

Characteristics of Phishing Emails:

- Unusual sender email address.
- Generic greetings (e.g., "Dear Customer").
- Urgent or threatening language.
- Suspicious links or attachments.
- Poor grammar and spelling.

Examples:

Phishing email attacks are a type of cyber attack that use email to trick people into sharing sensitive information. Here are some examples of phishing email attacks:

Spear phishing

- Uses specific information to send targeted emails to individuals or organizations to steal sensitive information. For example, whaling is a type of spear phishing that targets wealthy individuals, such as CEOs, with fake emails to get their login credentials.

Clone phishing

- An email that appears to be from a trusted sender is actually from a malicious actor. The email may include a link to a fake version of the sender's website.

Vishing

- An email that contains a virus or malware that automatically downloads onto a computer when the email is opened

RECOGNIZING PHISHING WEBSITES

How to Identify a Phishing Website:

- Check for HTTPS and padlock icon.
- Look for misspellings in the URL.
- Verify the website’s contact information and security certificates.
- Be cautious of pop-ups asking for personal information.

Example 1: Fake Bank Website
Legitimate Site:

- URL: https://www.bankofamerica.com
- Features: Secure HTTPS connection, proper security certificates, professional layout, and legitimate contact information.

Phishing Site:

- URL: http://www.bankofamerrica.com
- Features: Misspelled URL, HTTP connection (no HTTPS), absence of security certificates, poorly designed layout, and suspicious pop-ups asking for personal information.

Example 2: Fake Online Store
Legitimate Site:

- URL: https://www.amazon.com
- Features: Secure HTTPS connection, recognizable branding, professional design, and trusted payment methods.

Phishing Site:

- URL: http://www.amaz0n.com
- Features: Misspelled URL (using zero instead of "o"), HTTP connection, offers that are too good to be true, and requests for credit card information through pop-ups.

Example 3: Fake Email Provider
Legitimate Site:

- URL: https://mail.google.com
- Features: Secure HTTPS connection, recognizable Google branding, secure login process, and additional security features like two-factor authentication.

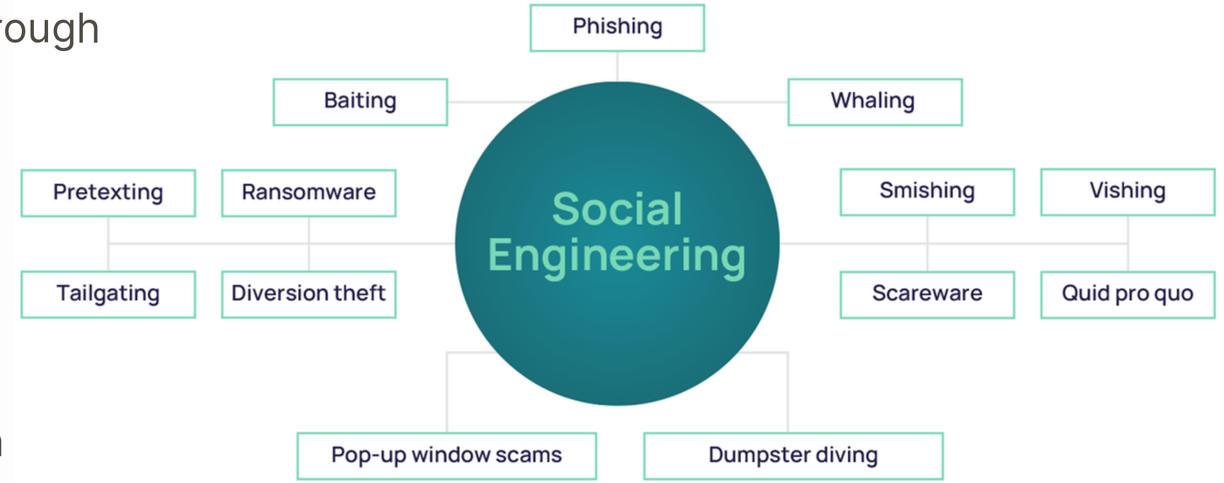
Phishing Site:

- URL: http://mail.g00gle.com
- Features: Misspelled URL (using zeros instead of "o"), HTTP connection, fake login page designed to steal credentials, and absence of additional security features.

UNDERSTANDING SOCIAL ENGINEERING TACTICS

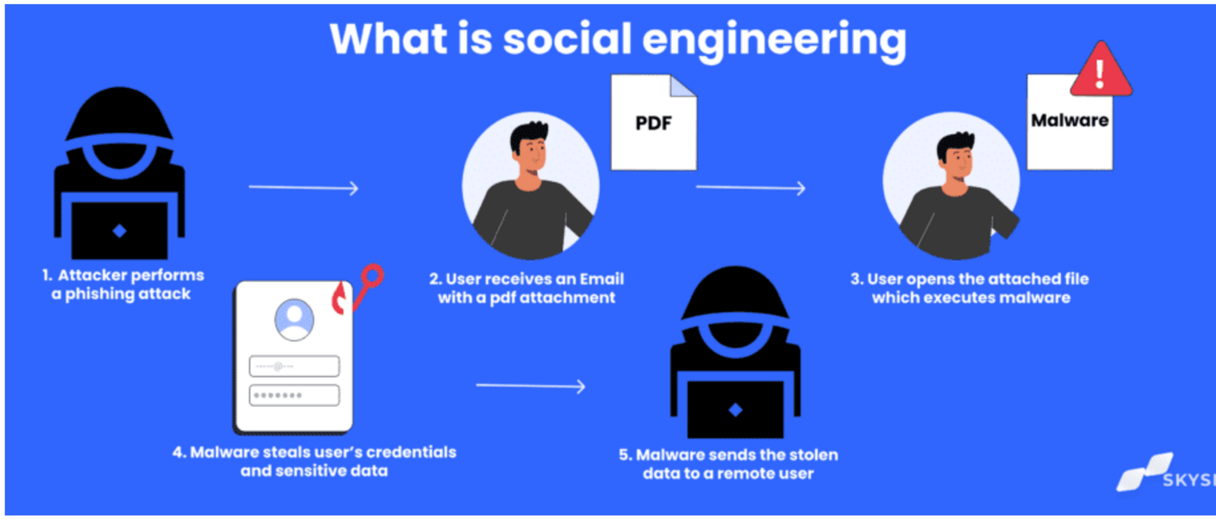
Definition of Social Engineering:

Manipulating people into divulging confidential information through psychological manipulation and deceit.



Common Techniques Used:

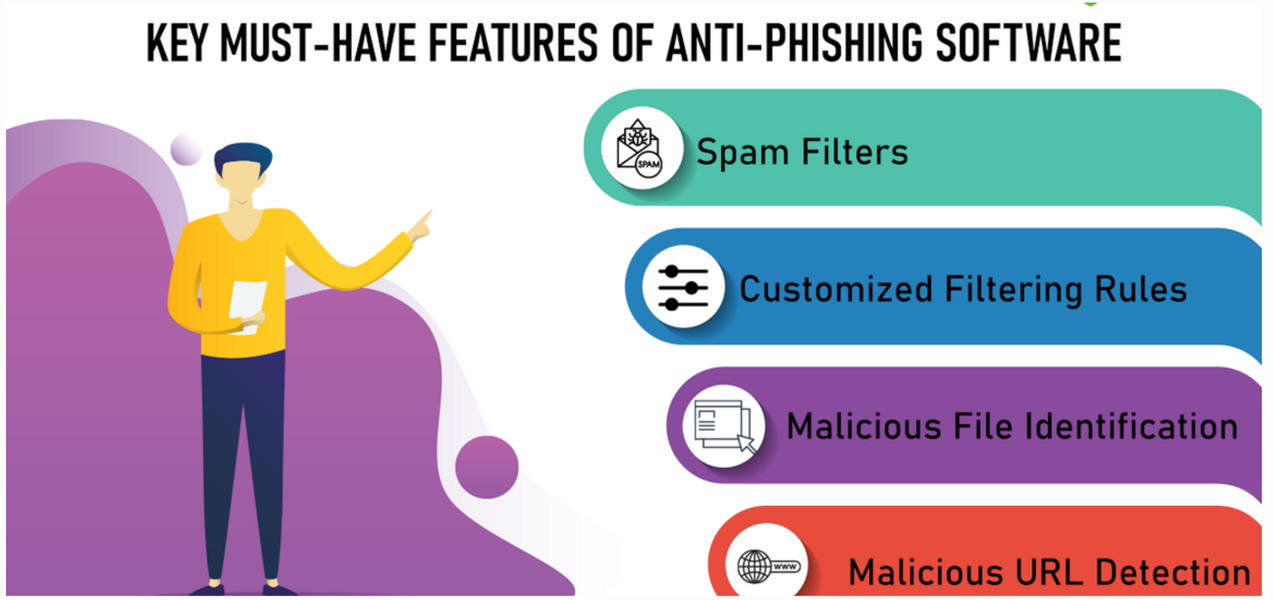
- Pretexting: Creating a fabricated scenario to obtain information. For example, pretending to be from IT support to ask for login credentials.
- Baiting: Offering something enticing to get information, such as free software or a prize that requires entering personal details.
- Tailgating: Gaining unauthorized access to a secure area by following someone who has legitimate access, often by pretending to be in a hurry or carrying heavy items.
- Quid Pro Quo: Offering a service or benefit in exchange for information, like pretending to be a researcher offering a free survey for personal data.



PREVENTIVE MEASURES

Best Practices for Email and Web Safety:

- Always verify the sender's email address: Ensure that the email is from a legitimate source before responding or clicking any links.
- Avoid clicking on links in unsolicited emails: Be cautious of emails from unknown senders, especially those with urgent requests or enticing offers.
- Use multi-factor authentication (MFA): Add an extra layer of security by requiring a second form of verification, such as a text message or authentication app.
- Keep your software and antivirus updated: Regular updates help protect against the latest security threats and vulnerabilities.
- Regularly back up your data: Ensure you have backups of important data to prevent loss in case of a security breach or malware attack.



Tools and Software for Protection:

- Use email filters: Set up filters to automatically detect and block spam and phishing emails.
- Install and update antivirus software: Protect your devices from malware and other security threats by using reliable antivirus software and keeping it up to date.
- Use security plugins for your web browser: Enhance your browser's security with plugins that block malicious websites and prevent tracking.

REPORTING PHISHING ATTEMPTS

Steps to Report Phishing Emails and Websites:

1. Use the report feature in your email client:
2. Most email clients have a built-in feature to report phishing emails. Use this to mark the email as phishing and alert the email provider.
3. Notify your IT department or security team:
4. Inform your organization's IT or security team immediately. They can take steps to protect the network and other employees.
5. Report phishing attempts to relevant authorities:
6. In India, you can report phishing attacks through the National Cyber Crime Reporting Portal (NCRP) at cybercrime.gov.in.
7. In the US, report phishing to the Federal Trade Commission (FTC) at reportfraud.ftc.gov.
8. Many other countries have similar organizations for reporting cybercrimes.

Organizational Reporting Procedures:

Explain your organization’s specific reporting process:

- Detail the steps employees should follow to report phishing attempts within your organization. This could include contacting the IT help desk, filling out a report form, or using a dedicated security email address.

Importance of Reporting:

Helps improve overall security and protects others:

- Reporting phishing attempts allows your organization to take proactive measures to protect against future attacks. It also helps security teams to identify and mitigate threats more effectively.

CONCLUSION

Recap of Key Points:

What Phishing Is: A form of cyberattack where attackers trick individuals into providing sensitive information by pretending to be legitimate entities.
How to Recognize It: Look for misspellings in URLs, lack of HTTPS, suspicious pop-ups, poor design, and unsolicited requests for personal information.
Preventive Measures: Verify email addresses, avoid clicking on unsolicited links, use multi-factor authentication, keep software and antivirus updated, and regularly back up data.
How to Report It: Use the report feature in your email client, notify your IT department, and report to relevant authorities like the NCRP,FTC.

Assessment:

Quiz:

Question 1: What is phishing?
Question 2: How can you recognize a phishing website?
Question 3: What steps should you take to report a phishing email?

Scenario-based Questions:

Scenario 1: You receive an email from your bank asking for your login details due to a "security issue." What steps should you take?

Scenario 2: You notice a website you frequently use has a URL with a misspelling and lacks a padlock icon. What should you do next?