Phishing Awareness

Protect Yourself from Phishing Attacks

Presented by:
Mohsina Rubaab

What is Phishing?

- Definition: Phishing is a type of cyber attack where attackers trick you into revealing sensitive information like passwords, credit card numbers, or personal details

- Importance: Phishing is one of the most common ways attackers breach accounts and steal data.

- Objective: Learn to identify, avoid, and report phishing attempts.

Types of Phishing Attacks

Email Phishing

Fake emails that look legitimate, designed to steal personal info or login credentials.

Spear Phishing

Targeted attacks on specific individuals using personalized information to appear credible.

Smishing

Phishing via SMS messages that trick users into clicking links or sharing sensitive info.

Vishing

Phishing over the phone where attackers impersonate trusted authorities to extract data

How to Recognize Phishing Emails

- Look for suspicious sender addresses (e.g., info@amaz0n.com instead of info@amazon.com).
- Generic greetings like “Dear Customer” instead of your name.
- Urgency or threats (e.g., “Your account will be closed if you don’t act now!”).
- Suspicious links or attachments – hover over links to verify the URL.
- Poor grammar or spelling mistakes.

Recognizing Fake Websites

Inspect the URL

Check the website address carefully, as phishing sites often mimic legitimate sites with slight variations or misspellings.

Verify Security Indicators

Look for HTTPS and the padlock icon, but remember that a secure connection alone doesn't guarantee the site is safe.

Assess Website Authenticity

Examine logos, design, and overall quality—any inconsistencies or unusual requests for personal/financial information are red flags.

Best Practices to Avoid Phishing

Never click on suspicious links or download unknown attachments.

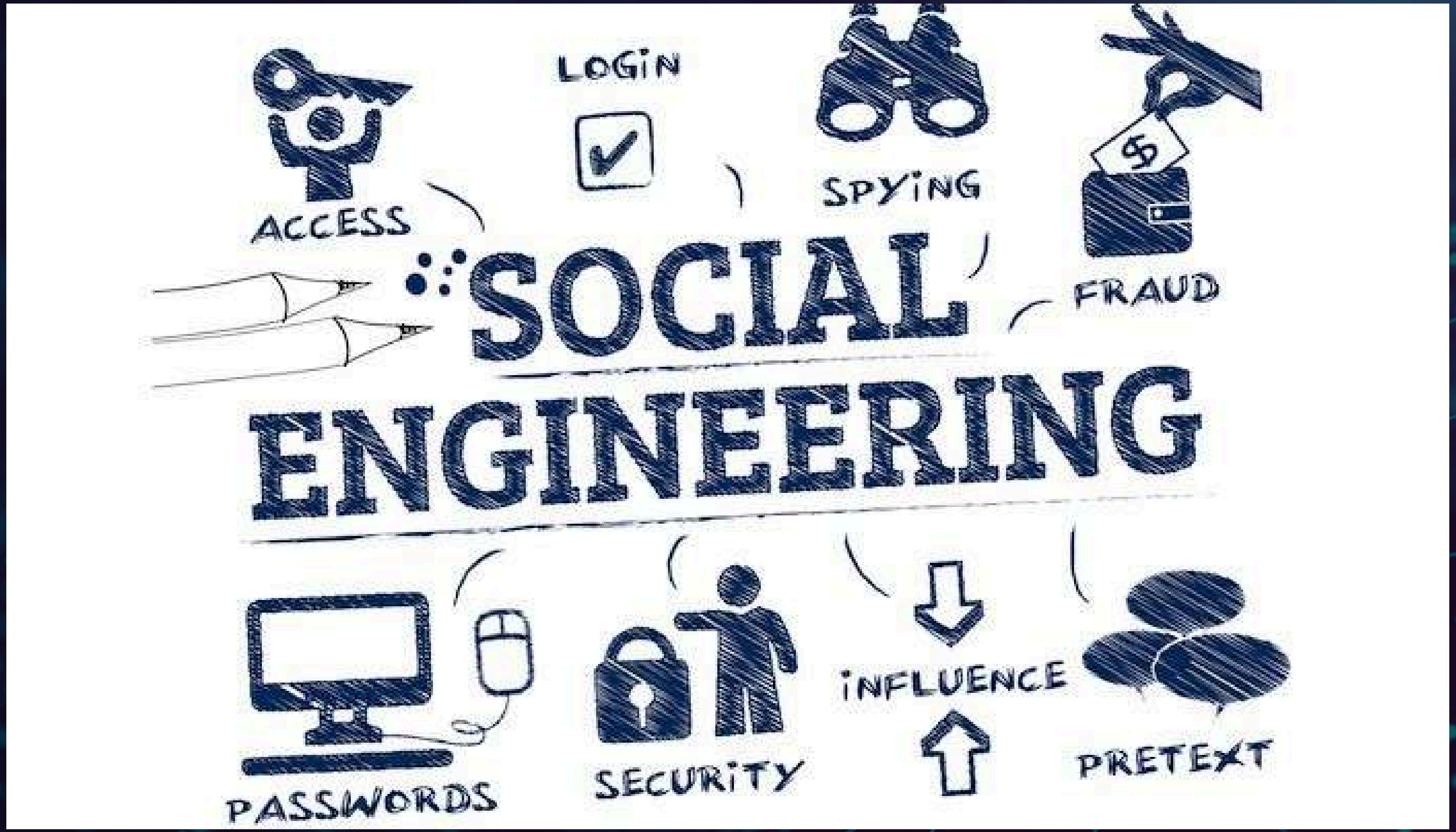
Use multi-factor authentication (MFA) whenever possible.

Verify requests for sensitive information via trusted channels.

Keep software and antivirus programs up to date.

Social Engineering Tactics

- Attackers exploit human psychology, not technical vulnerabilities.
- Common tactics include:
- Fear and urgency (“Immediate action required!”)
- Curiosity (“Click to see who sent you a gift!”)
- Authority impersonation (pretending to be your boss or IT support)
- Reciprocity (offering rewards or incentives)



Real-World Examples

1 Email from "IT Support" asking to reset your password – link leads to fake login page.

2 SMS claiming you won a prize – asks for personal info.

3 Phishing email with an invoice attachment – malware download

Interactive Quiz

You receive an email from your bank asking for your password. What should you do?

Click the link and enter the password

Verify via official bank website or phone number

Reply to the email

Submit

● Loading...

A website URL is www.amazon-secure.com. Should you trust it?

Yes

No

Submit

● Loading...

Summary

- Phishing is dangerous but avoidable.
- Always be cautious with emails, links, and requests for sensitive information.
- Use verification, MFA, and reporting to stay safe.
- Remember: If it seems suspicious, don't click it!

RESOURCES & REPORTING

- ANTI-PHISHING TOOL LINKS: PHISHTANK, APWG
- TIPS & GUIDES: COMPANY SECURITY POLICIES, CYBERSECURITY AWARENESS MATERIAL

THANK YOU!