Phishing Awareness Training

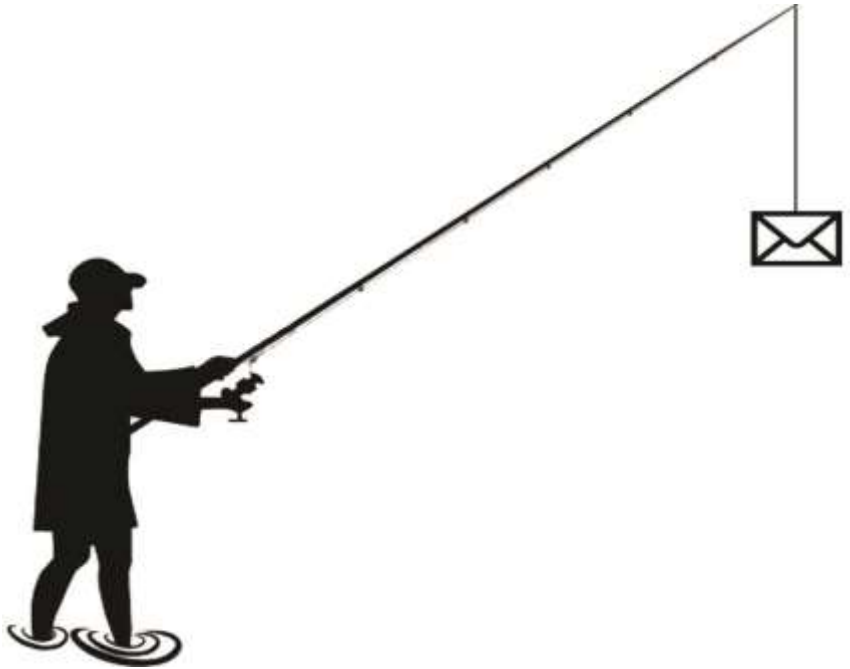
Presented by: Saif Ullah

Phishing Awareness Training

Introduction

- Protect Yourself from Cyber Threats

Phishing



What is Phishing?

What is Phishing?

- Phishing is a cyberattack that uses disguised emails, websites, or messages to trick you into revealing personal information, like passwords, credit card numbers, or account details.
- Goal of Phishing: To steal sensitive data or install malicious software.

Real Phishing Attack

Real Phishing Attack

- Story: In 2016, a phishing email led to a major breach of sensitive data at XYZ Corporation, causing financial loss and reputational damage.
- What Went Wrong?: An employee clicked a malicious link disguised as an internal message.
- Lesson Learned: Training and awareness could have prevented the breach.

Common Phishing Techniques

- Email Phishing: Fake emails from trusted sources asking you to click a link or download an attachment.
- Spear Phishing: Personalized emails targeting specific individuals or organizations.
- Smishing: Phishing via SMS or messaging apps.
- Vishing: Voice-based phishing attempts.
- Clone Phishing: Duplicating legitimate emails and changing the attachments or links.

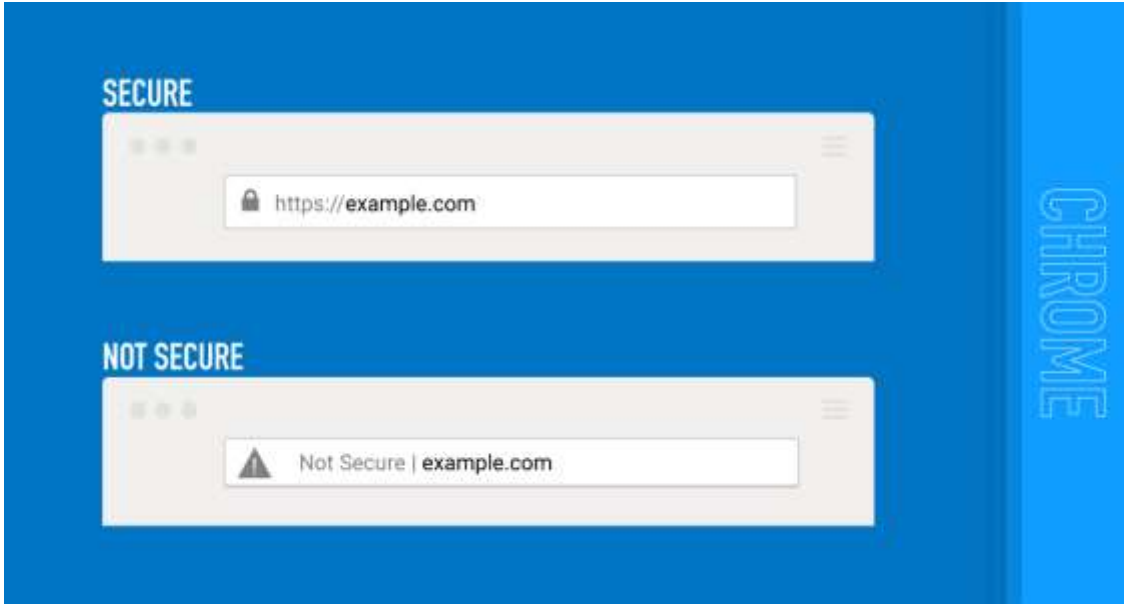
Recognizing Phishing Emails

- Unusual Sender Email: Slight variations in email addresses.
- Urgent or Threatening Language: "Act now!" or "Your account will be suspended!"
- Suspicious Links: Hover over links without clicking to check for unusual URLs.
- Unexpected Attachments: Never open attachments from unknown sources.
- Grammar and Spelling Errors: Poorly written messages often indicate phishing.

Phishing Websites

Lookalike Websites:

- Attackers create fake websites that look like real ones (e.g., fake bank websites).



How to Spot Them:

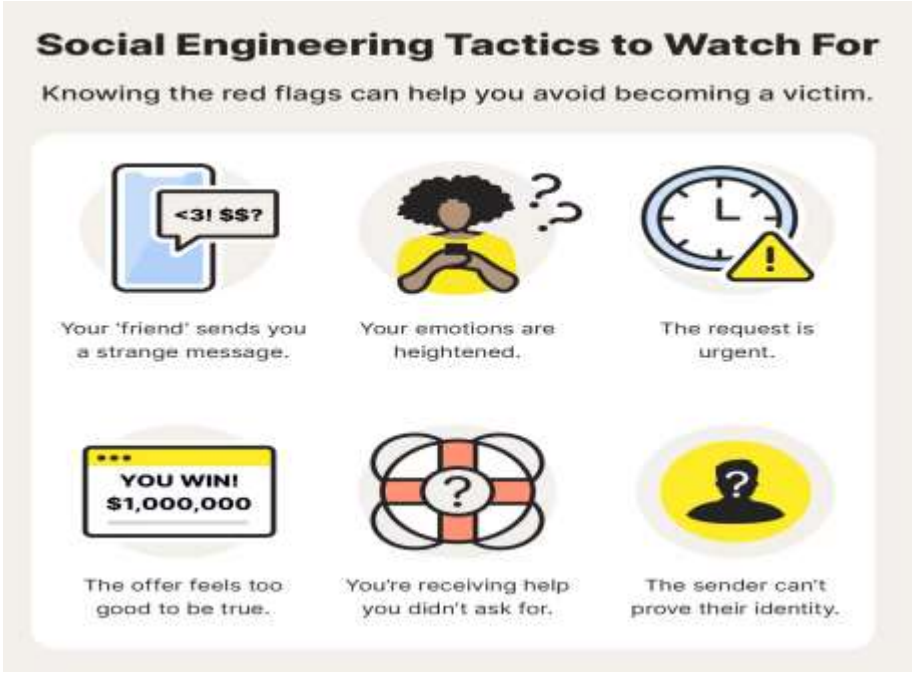
- Check for HTTPS: Secure sites have HTTPS in the URL.
- Look for Misspellings: Minor differences in domain names (e.g., g00gle.com).
- Unusual Pop-Ups: Legitimate sites rarely use excessive pop-ups asking for personal data.

Social Engineering Tactics

What is Social Engineering?

- Manipulating individuals into divulging confidential information.

Tactics:


Social Engineering Tactics to Watch For
Knowing the red flags can help you avoid becoming a victim.
<3! $$?
Your 'friend' sends you a strange message.
Your emotions are heightened.
The request is urgent.
YOU WIN! $1,000,000
The offer feels too good to be true.
You're receiving help you didn't ask for.
The sender can't prove their identity.

Tactics:

- Pretexting: Pretending to be someone you know (e.g., IT department or a boss).
- Baiting: Offering something tempting (e.g., a free download) to get you to share information.
- Tailgating: Physical intrusion by following someone into restricted areas.

What to Do if You Suspect Phishing

Steps to Take:

- Don’t click on links or download attachments.
- Report the email to your IT or cybersecurity team.
- Verify the request by contacting the sender directly through known channels.
- Use anti-phishing tools and keep software up to date.

Best Practices for Phishing Prevention

- Stay Alert: Always be cautious with unexpected emails or messages.
- Use Strong Passwords: Use unique and complex passwords for different accounts.
- Enable Two-Factor Authentication (2FA): Adds an extra layer of security.

Cont....

- Regularly Update Software: Security patches prevent vulnerabilities.
- Educate Others: Share what you know to create awareness.

Key Points:

- Phishing is a growing threat.
- Stay vigilant and educate yourself on recognizing scams.
- Always verify before clicking, sharing, or downloading.
- Report suspicious activity immediately.

Thank You!