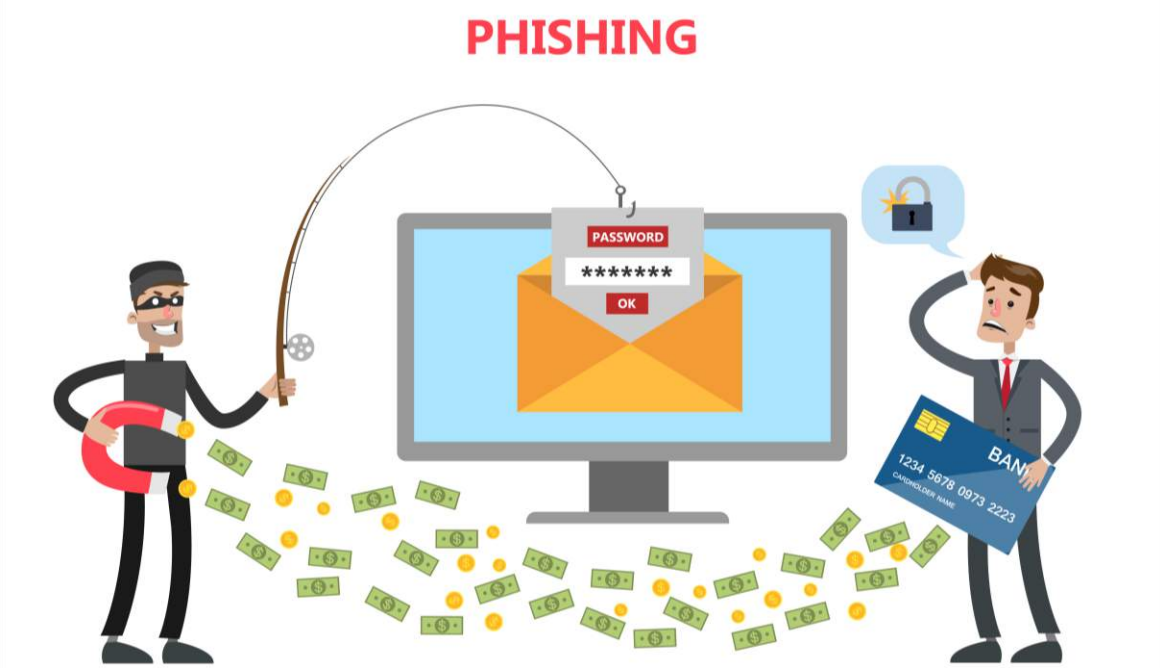
Defending against phishing attacks

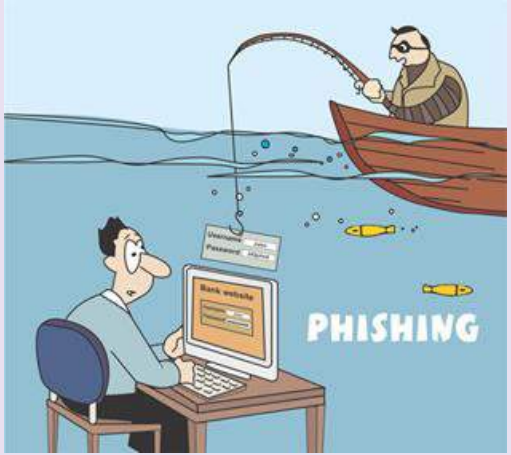
Introduction

In today's digital age, a single click can lead to disaster. Learn how to recognize and avoid phishing attacks to protect your personal information!



What is Phishing?

- When criminals pose as genuine sources (banks, credit cards, social media) to obtain personal information.
- The goal is to steal valuable data (such as credentials, financial information, and personal information) for illegal reasons.



Types of Phishing Attacks

- Email phishing
- Spear phishing
- Whaling (targeting executives)
- Vishing (voice phishing)
- Smishing (SMS/text phishing)

Common Tactics in Phishing

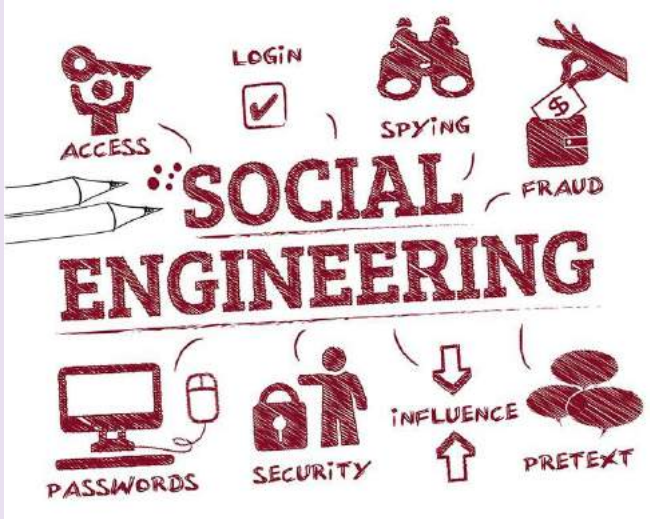
- **Spoofed Emails and Websites:** Phishers produce emails and webpages that look authentic, copying reputable institutions such as banks, social media platforms, and even your employer. Logos, fonts, and layouts may be carefully copied to trick you.
- **Social Engineering Techniques:** Cybercriminals utilize psychological manipulation to exploit human trust and emotion. They use a sense of urgency (e.g., "Account closure!") or an opportunity (e.g., "Free gift!") to get you to respond quickly.
- **Impersonation of Trusted Entities:** Phishers claim to be someone you know, such as a bank representative, a customer service agent, or even a friend. This false impression of authority can decrease your defenses, making you more vulnerable to their deceitful requests.

Recognizing Phishing Emails

- Email addresses from suspicious senders.
- Generic greetings or urgent language.
- Requests for confidential information or money
- Attachments or links that appear suspicious

Identifying Phishing Websites

- **Misspelled URLs and Strange Domains:** Examine the website address (URL) for typos, additional characters, or strange domain extensions (.com vs. something else).
- **No padlock & Missing HTTPS:** Secure websites use HTTPS and show a padlock in the address bar. Phishing sites may lack these security signs.
- **Unprofessional Design and Branding:** Phishing websites frequently have low-quality design, inconsistent logos, and grammatical problems. Be aware of anything that appears unprofessional.



Social Engineering Red Flags

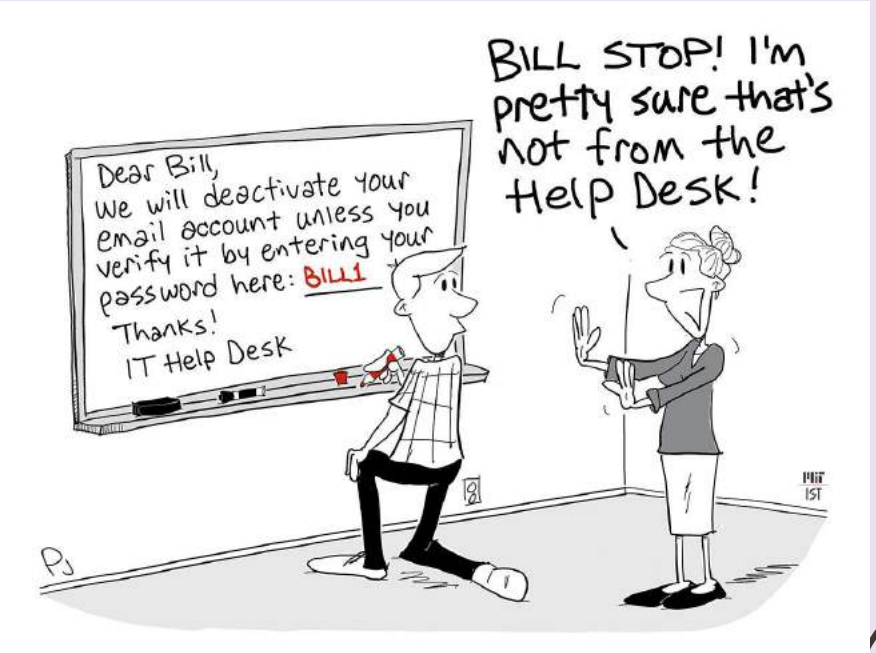
- **Psychological Manipulation:** Phishers use fear (account termination) or enthusiasm (free gift!) to coerce you into disclosing information.
- **Exploiting Familiarity or Authority:** To secure your assistance, they may imitate someone you trust, such as a colleague, bank representative, or customer service agent.
- **Targeting using Social Media Information:** Cybercriminals might use personal information from your social media profiles to create more convincing phishing efforts.

Techniques to Avoid Phishing Attacks

- Before responding, verify the sender's identity.
- Hover over links to check URLs before clicking.
- Type URLs directly into the browser.
- Enable two-factor authentication (2FA).
- Educate employees about phishing strategies.

Reporting Phishing Attempts.

- **Internal Reporting:** Notify your IT department or designated security personnel in a timely manner.
- **External Reporting:** Forward questionable communications to your email provider and consider reporting them to appropriate authorities (such as the FTC in the United States).



Real-World Examples and Prevention

Phishing assaults are not hypothetical threats; they are directed at real people and organizations. Here's a recent example:

Case Study: In 2020, intruders gained access to multiple Twitter accounts, including those of elected officials and celebrities. They accomplished this using a combination of social engineering and phishing techniques. Attackers targeted Twitter employees with spear phishing emails that appeared to come from respectable sources, such as IT support. These emails tricked employees into disclosing login information, allowing attackers to gain access to internal networks and compromise specific Twitter accounts.

Lessons learned: Phishing attacks can be quite sophisticated, targeting anyone regardless of position or technical skills.

Even major corporations with security systems in place may be vulnerable.

You're Phish-Proof Now!

Conclusion

- Phishing steals information from emails, messages, and phone calls; stay aware!
- Red flags include unexpected senders, haste, and fraudulent websites.
- Report phishing efforts to protect yourself and others.
- Stay informed - new tricks develop; remain watchful!
- Strong passwords, two-factor authentication, and regular updates - become a cybersecurity champion!

Thank you for your attention! ☺

Lisa Brezina, Elisabeth Hamal and David Mueller