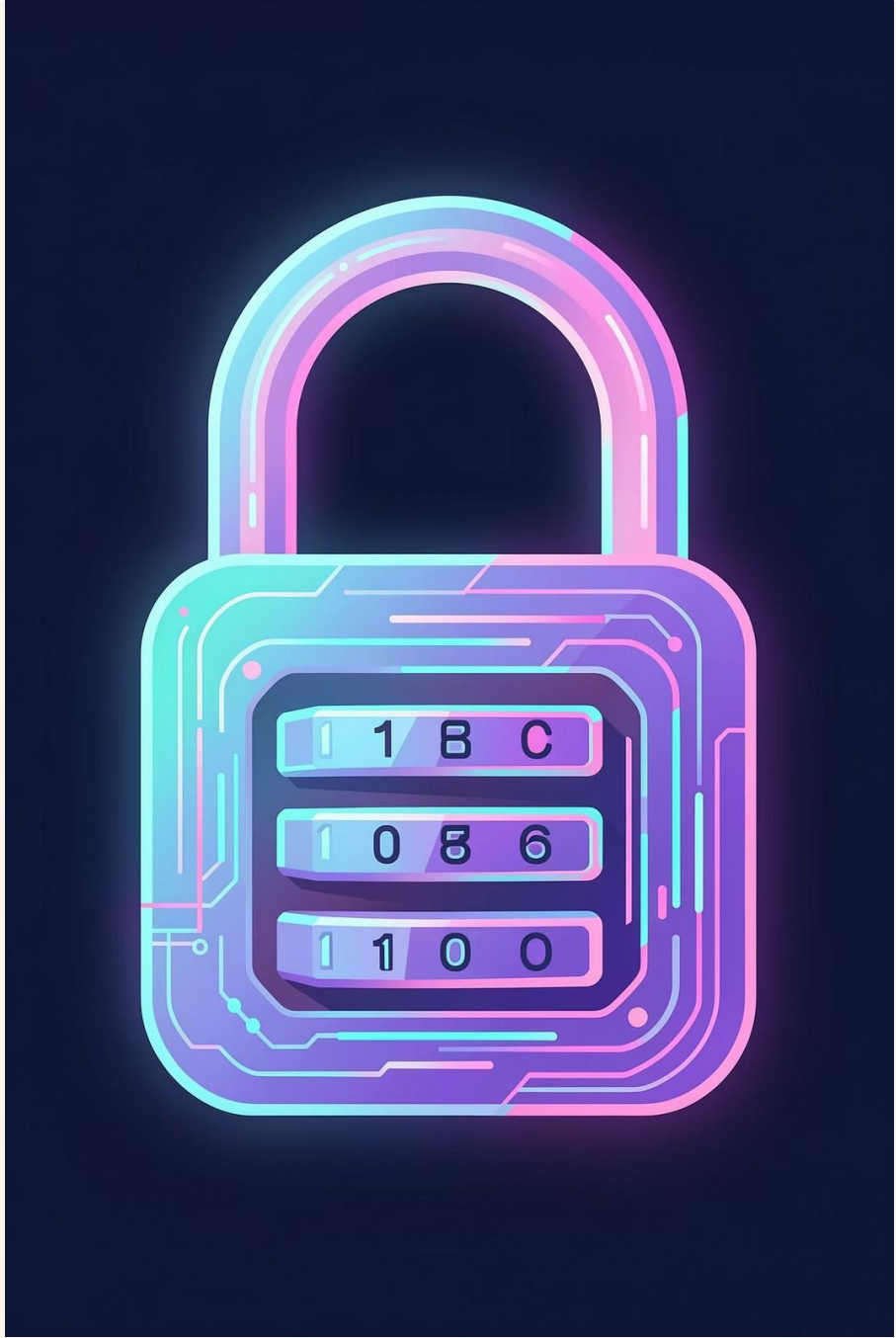
Phishing Awareness: Stay Safe Online

Cyber Security Internship – CodeAlpha

Prepared by: Yash Sawant

Domain: Cyber Security



UNDERSTANDING THE THREAT

What is Phishing?

Phishing is a deceptive tactic where cybercriminals impersonate trusted entities to trick individuals into divulging sensitive information. They aim to steal personal data such as passwords, bank details, and other confidential credentials.

These attacks typically occur through various digital communication channels, including emails, text messages, and social media, often designed to appear legitimate and trustworthy.

COMMON ATTACK VECTORS

Types of Phishing Attacks

Email Phishing

Deceptive emails impersonating banks, online retailers, or even acquaintances to solicit sensitive data.

SMS Phishing (Smishing)

Scams delivered via text messages, often containing malicious links or requests for personal information.

Social Media Phishing

Fake profiles or fraudulent messages on platforms like Instagram, Facebook, and X (formerly Twitter) designed to trick users.

Phone Phishing (Vishing)

Scammers make phone calls, posing as legitimate organisations or authorities, to persuade victims to reveal confidential details.

EMAIL RED FLAGS

Spotting Phishing Emails

Phishing emails often exhibit several tell-tale signs that can help you identify them:

- **Urgent or Threatening Language:** Messages demanding immediate action or threatening severe consequences if you don't respond.
- **Suspicious Sender Addresses:** Email addresses that don't quite match the legitimate organisation (e.g., "support@amz0n.com" instead of "support@amazon.com").
- **Grammar and Spelling Errors:** Professional organisations typically proofread their communications. Numerous mistakes are a clear warning sign.
- **Unsolicited Links or Attachments:** Be wary of unexpected links or files, even if they appear to come from a known sender.
- **Generic Greetings:** Phishing emails often use impersonal greetings like "Dear Customer" rather than addressing you by name.

WEBSITE VERIFICATION

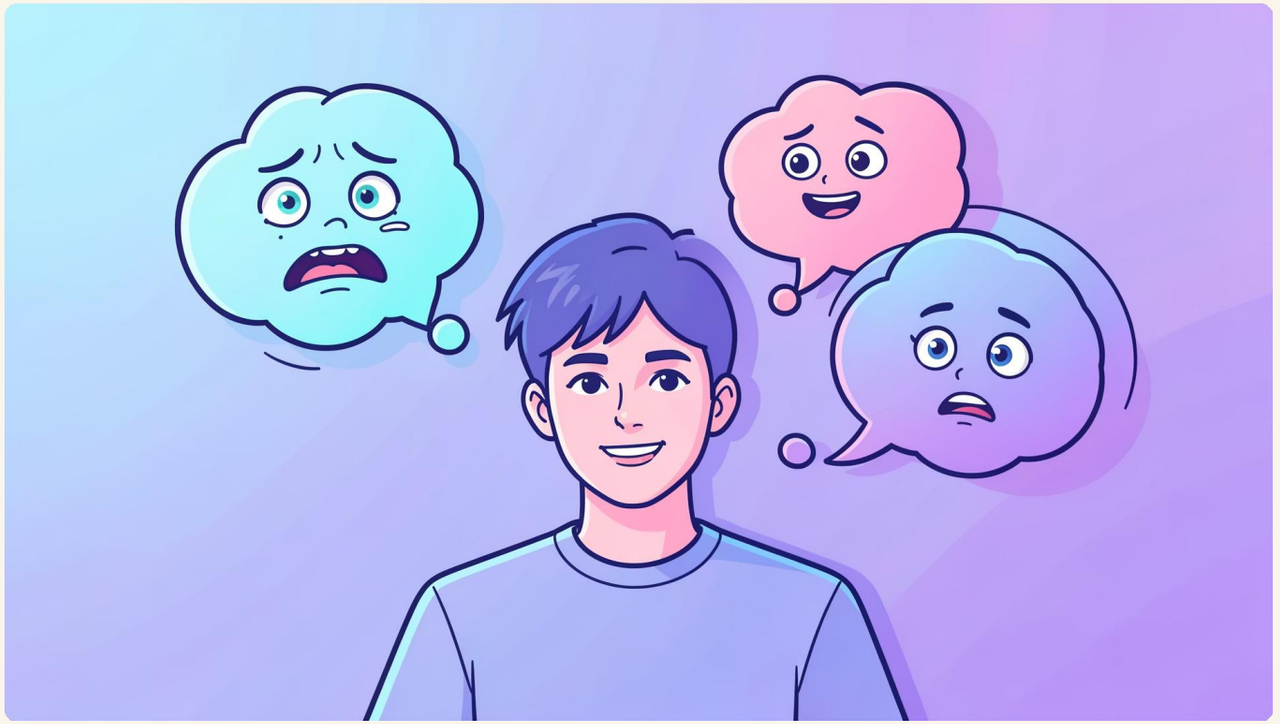
Identifying Fake Websites

Scammers often create convincing fake websites to harvest your credentials. Here9s how to spot them:

- **Slightly Altered URLs:** Look for subtle changes in the website address (e.g., "bankofamerica.net" instead of "bankofamerica.com").
- **Missing HTTPS or Padlock:** Always check for "https://" at the beginning of the URL and a padlock symbol in the address bar, indicating a secure connection.
- **Unexpected Pop-ups:** Legitimate sites rarely use intrusive pop-ups to ask for personal or payment details.
- **Always Double-Check:** Before entering any sensitive information, verify the website's authenticity by carefully inspecting the URL.

MANIPULATING TRUST

Social Engineering: The Human Element



Social engineering is a manipulation technique that exploits human psychology to trick individuals into performing actions or divulging confidential information.

- **Emotional Triggers:** Scammers often play on emotions like fear (e.g., "Your account is locked"), curiosity (e.g., "You have a new message"), or excitement (e.g., "You've won a prize!").
- **Creating Urgency:** Their goal is to rush you into making a decision without thinking, compelling you to click malicious links or share information quickly.
- **Think Before You Act:** Always take a moment to pause and critically evaluate any unexpected or high-pressure requests before reacting.

STAYING PROTECTED

Best Practices for Online Safety

1 Be Skeptical of Unsolicited Communications

Never click on suspicious links or download attachments from unknown senders, regardless of how convincing they appear.

2 Guard Your Personal Information

Refrain from sharing passwords or sensitive personal details online unless you are absolutely certain of the recipient's legitimacy.

3 Verify All Requests Directly

If you receive a suspicious request from a company, contact them directly using official phone numbers or websites, not the contact details provided in the suspicious message.

4 Strengthen Your Digital Defenses

Use strong, unique passwords for each account and enable multi-factor authentication (MFA) whenever possible. Regularly update your passwords.

5 Keep Software Updated

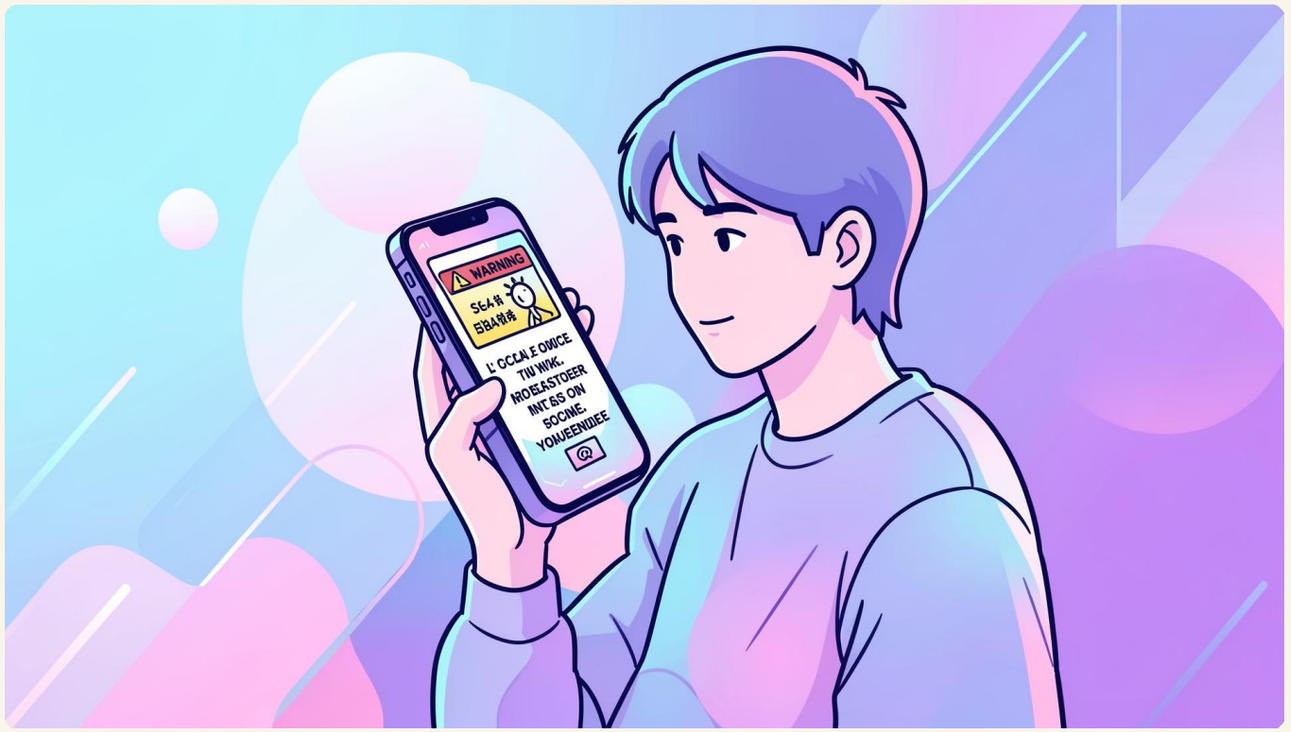
Ensure your operating system, web browsers, and antivirus software are always up-to-date to protect against known vulnerabilities.

REPORTING SUSPICIONS

What to Do If You Suspect Phishing

If you encounter what you believe to be a phishing attempt, it9s crucial to act responsibly to protect yourself and others:

- **Do Not Engage:** Avoid replying to the message or clicking on any embedded links or attachments.
- **Seek Trusted Advice:** Share the suspicious message with a trusted adult, IT support, or a cybersecurity professional for guidance.
- **Report the Incident:** Forward phishing emails to your email provider, school IT department, or relevant authorities.
- **Securely Delete:** Once reported, safely delete the suspicious message to prevent accidental interaction in the future.



INSTANT VERIFICATION

Quick Checklist to Spot Phishing

Urgency/Threat?

Is the message creating pressure or instilling fear?

Sender Suspicious?

Does the sender's email address look legitimate?

Errors Present?

Are there obvious spelling or grammar mistakes?

Link Strange?

Does the URL appear unfamiliar or inconsistent?

Info Requested?

Are you unexpectedly asked for personal details?

Conclusion: Stay Alert, Stay Safe

Phishing is a prevalent online threat, but with heightened awareness and caution, you possess the power to protect yourself. Remember these key principles:

- **Think Before You Click:** Always critically evaluate any unexpected communication before interacting with links or sharing information.
- **When in Doubt, Ask:** If you're unsure about a message's legitimacy, consult a trusted source or IT professional.

Your vigilance is the strongest defence against online scams. Stay safe!