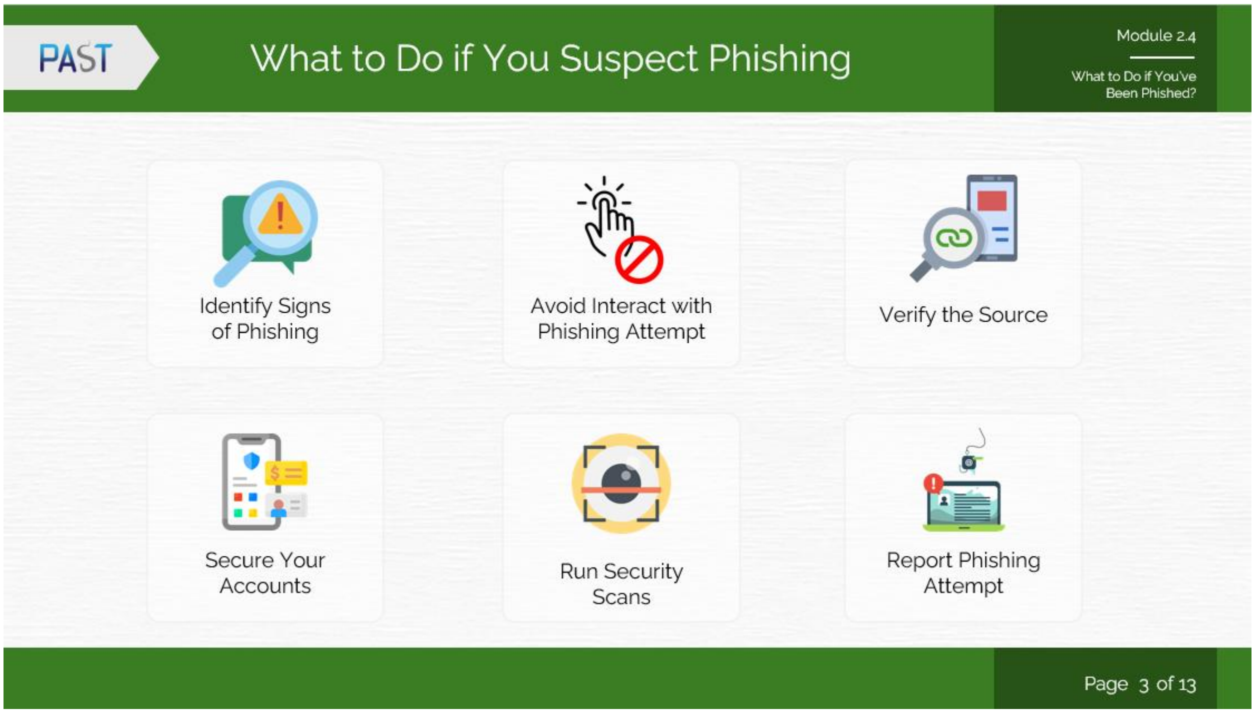
Phishing Assessment

Module 2.4: What can you do if you have been Phished?

Table of Contents

1. What to Do if You Suspect Phishing


PAST

What to Do if You Suspect Phishing

If you suspect a phishing attempt, taking the right steps immediately and follow below structured approach to handle the situation safely:

Identify Signs of Phishing: Before taking action, confirm if the message, email, or call, shows common phishing signs, such as Urgency & Threats, Unknown Senders or Fake Email Addresses, Unusual Links , Unexpected Attachments , Requests for Personal Information.

Avoid Interact with Phishing Attempt: Once you identify a potential phishing attempt, do not engage with it: Do Not Click Links , Do Not Call Numbers in the Message, and Do Not Reply.

Verify the Source: If the message appears legitimate but seems unusual, always verify its authenticity: Check the Email Domain, Manually Visit the Website and Call the Company Directly.

Secure Your Accounts: If you interacted with a phishing attempt, take immediate action to prevent damage: Change Passwords Immediately, Disable Unauthorized Sessions, Enable Account Alerts

Report Phishing Attempt: Report Phishing Emails to providers like Gmail and Outlook. Notify Banks and Companies if financial details were involved. Report to Government Authorities such as the police or cybersecurity agencies.

Run Security Scans: If you clicked a suspicious link or downloaded an attachment, check your system for malware: Run a Full System Scan, Clear Browser, Data Reset Your Device (if necessary).

2. Best Cybersecurity Tips

1. Use Strong, Unique Passwords

Create long, complex passwords (a mix of uppercase, lowercase, numbers, and symbols) that are different for every account. Avoid using easily guessable information like birthdays or common words.

Why: Weak or reused passwords are easily cracked, giving attackers access to multiple accounts if one is compromised.

2. Enable Authentication Methods

Activate Authentication Methods (2 factor authentication or Multi-factor authentication) on all important accounts, such as email, banking, and social media. This adds an extra layer of security by requiring not just a password but also a code sent to your phone or generated by an app.

Why: Even if your password is stolen, MFA ensures that attackers cannot access your account without the second factor.

3. Use Antivirus Software & Keep Software and Devices Updated

Install reputable antivirus software, and make sure it's kept up-to-date. Regularly run scans on your devices to detect threats.

Why: Antivirus software helps detect and remove malware that could otherwise steal your information or damage your systems.

Updates often include patches of known vulnerabilities that attackers could exploit.

4. Back Up Your Data Regularly

Use automated backup systems to regularly save copies of your data on external drives or cloud services.

Why: In case of ransomware attacks or system failures, backups ensure you can recover your data without paying a ransom or suffering permanent loss.

5. Use a VPN on Public Wi-Fi

Always use a Virtual Private Network (VPN) when connecting to public Wi-Fi networks to encrypt your internet traffic and prevent eavesdropping.

Why: Public Wi-Fi is notoriously insecure, and attackers can intercept unencrypted data on such networks.

6. Beware of Public USB Charging Ports and Devices

Avoid using public USB charging stations or plugging unknown USB devices into your computer, as they may contain malware.

Why: Attackers can install malware or steal data via compromised USB ports (a technique known as "juice jacking").

7. Limit Social Media Sharing

Be mindful of what you share online, especially personal details like your address, phone number, or vacation plans.

Why: Attackers can use publicly available information to craft convincing social engineering attacks or impersonate you.

8. Log Out of Accounts When Not in Use

Log out of accounts on shared devices or after finishing important transactions and avoid saving login credentials on public or untrusted devices.

Why: Staying logged in on shared or public devices increases the risk of unauthorized access.

9. Be Wary of Unsolicited Attachments or Links

Don't open attachments or click links from unfamiliar or unexpected sources, even if they seem urgent. Hover over links to check their actual destination.

Why: Phishing emails and malicious attachments are used to steal credentials or install malware.

Summary

Phishing remains one of the most prevalent cyber threats, but by recognizing the warning signs and following cybersecurity best practices, you can significantly reduce your risk. Always verify suspicious messages, secure your accounts, and stay vigilant against evolving threats. Cybersecurity is a shared responsibility—by staying informed and cautious, you can protect yourself and others from falling victim to phishing attacks.

- END -