PRACTICE CYBER HYGIENE

Use strong passwords. Think long, strong, unique. Length is more important than complexity. Change passwords frequently.

Enable multi-factor authentication. Add an extra layer of security by requiring more than one form of verification to access your accounts.

Practice safe browsing. Keep your web browser up-to-date. Stop visiting websites without HTTPS. Clear browser cookies. Block ads whenever possible.

Be smart on open Wi-Fi networks. Limit your use of public hotspots and instead use protected Wi-Fi from a trusted network operator or mobile wireless connection to reduce your risk of exposure.

Verify requests. If you receive an email or text requesting sensitive information, verify the request through a secondary communication channel (e.g., phone call to a known number).

Use the right tools. High-quality antivirus software, network firewall, password manager and encryption. Regularly perform software updates.

FSA
COMPLIANCE
COLLABORATIVE

Common Signs to Help Identify a Phishing Scam

- Unknown Email Address: The email comes from an unfamiliar address or domain. If the URL of the website doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site.
- Mismatched Display Name and Email Address: The display name might look legitimate, but the actual email address does not match the company's domain. Hover over links without clicking to see the URL. If it looks strange or does not match the expected domain, it's likely a phishing link.
- Unexpected Attachments or Links: The email contains unexpected attachments or links, often urging you to download or click. Be cautious of file extensions such as .exe, .zip, or .scr.
- Inconsistent or Strange Language: The email contains awkward phrasing, poor grammar, or spelling mistakes. Email can also create a sense of urgency or fear, urging immediate action. Phrases like "Your account will be suspended" or "Immediate action required" are common.
- Be Leary of Pop-Ups: they are often linked to malware. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups.
- Fake Logos: The logo and branding might be poorly copied or slightly off compared to the legitimate company's branding.
- Impersonal or Unprofessional Appearance: The email lacks proper branding, has low-quality images, or contains unusual formatting. Uses generic greetings like "Dear Customer" instead of addressing you by name.
- Beware of AI-generated Deep Fake Phishing: Artificial intelligence create speaking voices that impersonate real people. If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement or on the company's or government agency's website to verify the authenticity of the request.

How to Handle a Phishing Attack

- Disconnect Your Device from the internet. Either locate your Wi-Fi settings and disconnect from the network or simply unplug the internet cable from your device.
- Change Your Passwords. If you were redirected to a spoof website and asked to enter your credentials, change your password by visiting the real website directly, not through the phishing link. Additionally, if you have reused the password on other accounts, make sure to change those as well.
- Report the incident immediately. Inform your supervisor, compliance official/officer, privacy or security officer. Do this as soon as possible.
- Contact the company or organization. If you responded to a phishing email that appeared to be from a trusted source, contact the company or organization to alert them so that they can monitor any suspicious activity.
- Monitor your accounts. Closely monitor your financial and online accounts after a phishing scam. Regularly review your credit card and bank statements for unauthorized transactions, and consider enrolling in credit monitoring services for added security.

In 2023, FBI’s Internet Crime Complaint Center received 880,418 complaints with potential losses exceeding $12.5 billion from the American public, which is nearly a 10% increase in complaints and a 22% increase in losses compared to 2022. The most frequently reported crime was phishing schemes, where unsolicited emails, text messages, and phone calls impersonate legitimate companies to request personal, financial, or login credentials.

The full 2023 Internet Crime Report can be found here: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

FSA COMPLIANCE COLLABORATIVE