TIP SHEET

PHISHING ATTACKS

PHISHING

Phishing attacks collect your personal and financial information using email, text, or malicious websites to infect your digital devices with malware. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers or mobile phone and makes the user vulnerable to an attack. Think twice because cybersecurity is the collective responsibility of everyone.

Phishing emails or texts may appear to come from a trusted financial institution, e-commerce site, a government agency, or any other service, business, or individual. The email or text may ask for account numbers, passwords, or Social Security Numbers. When users respond or click on a link, attackers take the data to access users' accounts.

HOW CYBERCRIMINALS LURE YOU IN

> "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."

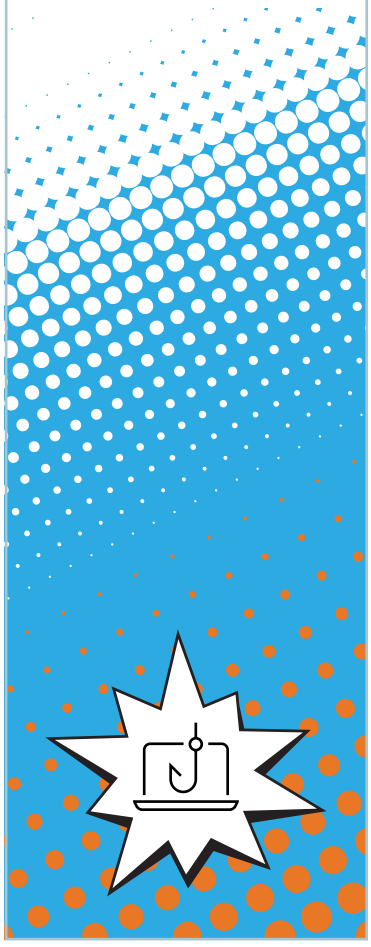
> "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

> "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

- **Play hard to get with strangers.** Links in emails, texts and online posts are often the way cybercriminals compromise your devices. If you are unsure who the message is from—even if the details appear accurate—do not respond, and do not click on any links or attachments—just delete it. Be cautious of generic greetings, as these are often phishing attempts. If you question the message, call the company directly.
- **Think before you act.** Be wary of messages that implore you to act immediately, causing you to fear your account is in jeopardy. If you receive a suspicious message that appears to be from someone you know, reach out to that person directly on a secure platform. If a message is from an organization, but still looks "phishy," reach out to the organization to verify the message.
- **Check hyperlinks.** Avoid clicking on hyperlinks in messages, and hover over links to verify authenticity. Ensure that webpage URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

- **Once you post on the internet it is there forever.** Keep personal information to yourself. If people have key details from your life like your job title, full name, birthdate and more, they can attempt a direct "spear-phishing" attack on you. Criminals can also use social engineering with these details to try to manipulate you into skipping setting up normal security protocols. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- **Be alert for suspicious emails.** If you receive an e-mail from a known vendor that seems suspicious, encouraging you to click on a link to your account, **do not click on the link or call the number in the email.** Instead, login directly to your account to verify if there are any issues with your account or call the company using the number listed on their website.

KNOW YOUR CYBER BASICS

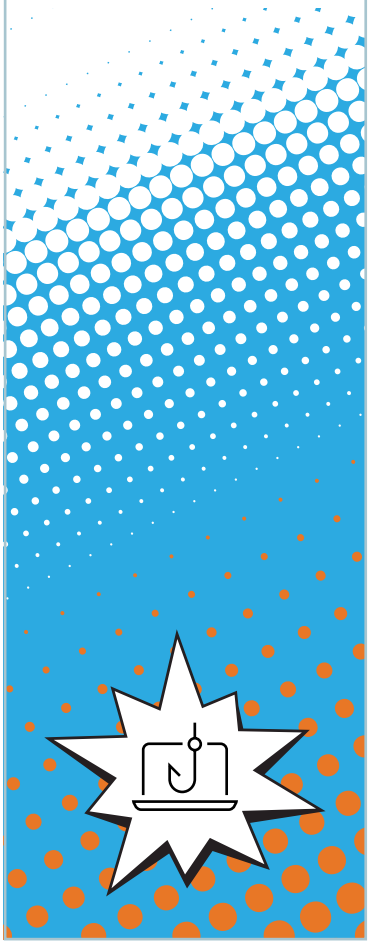
- **Enable multi-factor authentication (MFA).** Enable multi-factor authentication (MFA), meaning use two or more user verification methods to log in to your accounts or devices, to ensure that the only person who can access your account is you. Use it for email, banking, social media, and any other password-protected service. If MFA is an option, enable it on trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.
- **Shake up your password protocol.** Use the longest password or passphrase permissible. Use strong and unique passwords, which can prevent criminals from gaining access to accounts and protect you in the event of a breach. Use password managers to generate and remember different passwords for each account.
- **Use password managers.** There are password apps to generate and remember different passwords for each account.
- **Install and update antivirus software.** Make sure all your computers, Internet of Things devices, phones, and tablets are equipped with regularly updated antivirus software, email filters, and anti-spyware.

HOW TO REPORT

The Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.