TIP SHEET

CYBER SECURITY BASICS: IDENTITY THEFT & INTERNET SCAMS

CYBERSECURITY BASICS: IDENTITY THEFT AND INTERNET SCAMS

Today's technology allows us to connect around the world, to bank and shop online, and to control our devices from our smartphones. This added convenience brings with it an increased risk of identity theft and internet scams. We can greatly increase our cybersecurity online, at work, and at home by taking a few simple steps.

IDENTITY THEFT

Identity theft happens when someone steals your personal information to commit fraud. The identity thief may use your information to apply for credit, file taxes, or get medical services. These acts can damage your credit status and cost you time and money to restore your good name.

- **Don't reveal personally identifiable information** such as your bank account number, Social Security Number (SSN), or date of birth to unknown sources.
- **Practice safe web surfing** wherever you are by checking for the green lock or padlock icon in your browser bar—this signifies a secure connection.
- **Type website URLs directly into the address bar** instead of clicking on links or copying and pasting from the email.
- **Check with the known sender before clicking on any links.** All emails and messages should be considered suspicious, when in doubt.

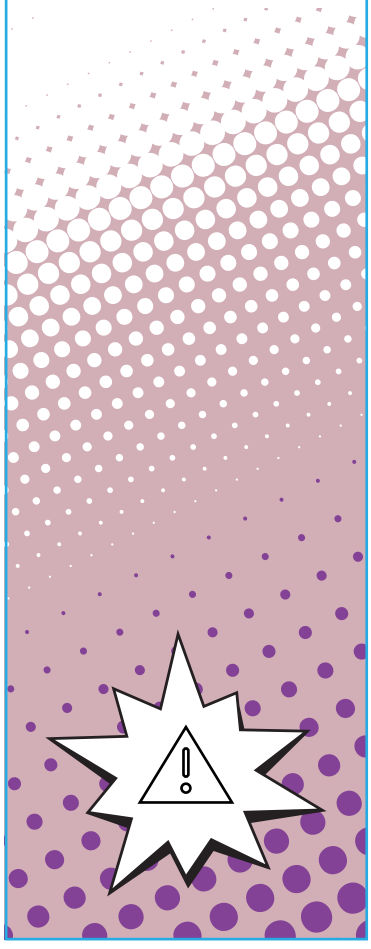
For additional resources to report and recover from identity theft contact the Federal Trade Commission's Identity Theft website: www.identitytheft.gov/#/

COMMON INTERNET SCAMS

- Imposter scams, such as phishing and spoofing, occur when you receive an email or call from a person claiming to be a government official, family member, or friend requesting personal or financial information. For example, an imposter may contact you from the Social Security Administration informing you that your SSN has been suspended, in hopes you will reveal your SSN or pay to have it reactivated.
- Donation scams take the form of emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email involving recent world events, such as COVID-19, or geo-political events. Be wary of social media pleas, texts, or calls.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Spoofing and Phishing - FBI
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

TIP SHEET

CYBER SECURITY BASICS: IDENTITY THEFT & INTERNET SCAMS

KNOW YOUR CYBER BASICS

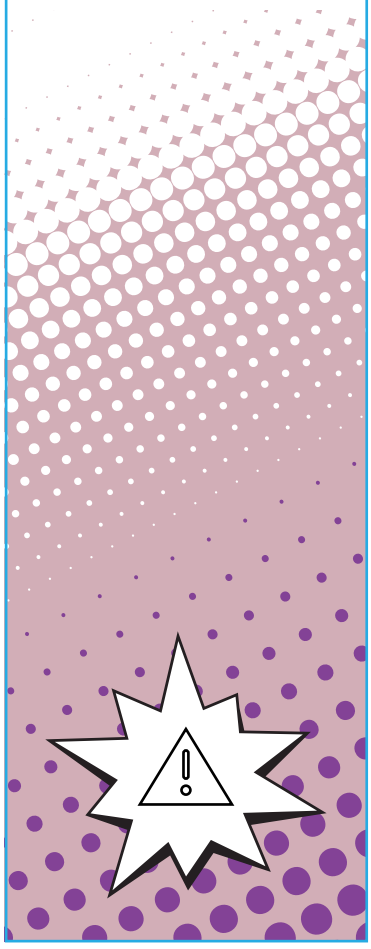
- **Enable multi-factor authentication (MFA).** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other password-protected service. If MFA is an option, enable it by using a trusted mobile device, 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.** You should consider using the longest password or passphrase permissible. Use long, random and unique passwords for different sites to prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different passwords for each of your accounts.
- **Stay up to date.** Keep your software updated with the latest version available. Maintain your security settings to keep your information safe by turning on automatic updates so you do not have to think about it, and set your security software to run regular scans.

REPORTING A CYBERCRIME

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. Crime reports will aid investigations and acting immediately can help you recover lost funds or data.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Spoofing and Phishing - FBI
- 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.