TIP SHEET

CYBER SECURITY BASICS: PASSWORDS & PASSWORD MANAGEMENT

CYBERSECURITY BASICS FOR PASSWORDS AND PASSWORD MANAGEMENT

Creating long, random and unique password is a critical step to protecting yourself online. Using long passwords is one of the easiest ways to defend yourself from cybercrime. The most secure way to store all your unique passwords is by using a password manager. With just one password, a computer can create and save passwords for every account that you have—protecting your online information, including credit card numbers and their three-digit codes, answers to security questions, and more.

STRONGER PASSWORDS INCREASE SECURITY

- **Use a long passphrase with 12 or more characters.** Use the longest password or passphrase permissible. For example, you can use a password manager or passphrase such as a news headline or even the title of the last book you read.
- **Don't make passwords easy to guess.** Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.
- **Keep your passwords on the down low.** Do not tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or by phone. Every time you share or reuse a password, it chips away at your security by opening more ways with which it could be misused or stolen.
- **Use unique passwords.** Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protects you in the event of a breach.

KNOW YOUR CYBER BASICS

- **Strengthen your login protection.** Use 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-required service. Enable MFA 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.
- **Fortify your online accounts** by enabling the strongest authentication tools available, such as biometrics (biological measurements—or physical characteristics—that can be used to identify individuals, such as fingerprint mapping, facial recognition, and retinal scans), and/or security keys. Your usernames and passwords are not enough to protect key accounts like email, banking, and social media.

FOLLOW-ON RESOURCES

- CISA's Multi-Factor Authentication Website
- Multi-Factor Authentication Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime