BE CYBER SMART

#CyberMonth

CYBERSECURITY AWARENESS
DO YOUR PART. #BECYBERSMART

CREATING A PASSWORD

Creating a strong password is a critical step to protecting yourself online. Using long, complex passwords is one of the easiest ways to defend yourself from cybercrime. No one is immune to cyber risk, but #BeCyberSmart and you can minimize your chances of an incident.

SIMPLE TIPS

- **Use a long passphrase.** According to National Institute of Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.
- **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.
- **Avoid using common words.** Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L."
- **Get creative.** Use phonetic replacements, such as "PH" instead of "F". Or make deliberate, but obvious misspellings, such as "enjin" instead of "engine."
- **Keep your passwords on the down-low.** Don't tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. 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.
- **Unique account, unique password.** Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. It's important to mix things up—find easy-to remember ways to customize your standard password for different sites.
- **Double 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 service that requires logging in. 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. Read the Multi-Factor Authentication How-to-Guide for more information.
- **Utilize a password manager to remember passwords.** 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.

CONTACT THE CISA CYBERSECURITY AWARENESS MONTH TEAM

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please email our team at CyberAwareness@cisa.dhs.gov or visit www.cisa.gov/cybersecurity-awareness-month or staysafeonline.org/cybersecurity-awareness-month/ to learn more.