U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow ARCYBER:

Passwords and Securing Accounts

Passwords are like keys to your house. You should do everything you can to protect your house and prevent those who wish you ill from gaining access.

HOW DO I CREATE A GOOD PASSWORD?

- Remember the phrase "long and strong." Good passwords have a minimum of 12 characters and a mix of upper and lowercase letters, numbers, and symbols. Avoid using consecutive characters such as "1234" or recurring characters such as "zzzz".
- Avoid words that can be found in a dictionary or the name of a person, character, product, or organization. It's okay to make passwords unique to your life, but not something that is easily guessed.
- Make sure that every password is significantly different from your other passwords.
- Better yet, say the experts at the National Institute of Standards and Technology (NIST), is to create a passphrase that uses a few normal words or phrases that have a unique association to you; words that are connected in your mind, but not the same in others' minds. These are much easier to remember, but harder to guess (as long as your words aren't also a grouping that is easily guessed, such as the names of your children or colors of the rainbow). Better examples might be words that come to mind when you think of your house, such as "bluecornerfamilymaple", or your hobbies, such as "travelboatrelaxsunny".

HOW DO I ENSURE MY PASSWORD PROTECTION STAYS SAFE?

- Never share your passwords with others, not even friends and family members, and never send a password by email, text message, or other forms of communication that may not be secure.
- Get a password manager program to help you remember your passwords. A good manager will encrypt and automatically update stored passwords, and require multi-factor authentication for access.
- If you write passwords down, store them in a safe place away from your computer. Instead of the actual password, consider writing a hint that will remind you of the password.
- Security experts used to advise that you change your passwords several times a year. Now they say it's not such a good idea, because many users change their passwords in predictable patterns, and frequent changes make passwords harder to remember. Today NIST recommends changing passwords once a year or immediately if there is a data breach, threat, or you suspect they have been compromised.
- Screen passwords (or one you'd like to use) against lists of commonly used, weak or breached passwords to see if they have been compromised by a data breach or hacking. Some browsers and websites offer this service.
- If you're asked to create answers to security questions, provide an unrelated answer. For example, if you are asked "Where did you go to school?", you might answer, "Fourteen." Just be sure that you can remember them.

- Don't let criminals trick you into revealing your passwords. Treat all unexpected requests for your information with caution, even if they appear to come from trusted sources. If you receive an email or phone call that appears to be from a store or your bank, that tries to convince you to share your password or other information, it could be a phishing scam.

ARE PASSWORDS THE ONLY FORM OF PROTECTION FOR MY ACCOUNT(S)?

Typing a username and password isn't the only way to identify yourself. Many web services add to their security features with with two-factor or multi-factor authentication that asks for additional forms of authentication to verify your identity, such as:

- Biometrics such as voice ID, facial recognition, iris recognition, and finger scanning.
- A one-time security code, usually sent via phone call or text.
- A security key or token; a small device (most often used via a USB port or in conjunction with a smartphone) that is used when logging in.

It's a good idea to enable multi-factor authentication any time it's available. In some cases, two-step and multi-factor authentication services may be available, but are not required. Ask your financial institution and other online services if they offer these methods or additional ways to verify your identity.

The National Cyber Security Alliane also offers authentication tips and a guide on how to turn on strong authentication for several popular online services at: https://stopthinkconnect.org/campaigns/lock-down-your-login

SOURCES: National Cyber Security Alliance, National Institute of Standards and Technology, Microsoft