U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil |

Passwords and Securing Accounts

Your data is a precious commodity. Hackers and thieves who steal it can steal your personal information, your money and maybe even your identity. Good passwords and authentication practices are often your first line of defense in preventing unauthorized access and data theft.

HOW DO I CREATE A GOOD PASSWORD?

- Focus on length, no complexity. Recent studies have shown that password length is more important than password complexity. Password recommendations from the Massachusetts Institute of Technology showed that an 8-character password with special characters can be broken in less than an hour, while a 12-character simple phrase can withstand the same attack for more than 200 years. Security experts say a password between 12 and 16 characters allows for strong security without being overly burdensome.
- Complex passwords that use special characters, numbers and upper- and lower-case letters are also less secure because users often choose easy-to-remember or predictable words or patterns. Less complex passwords can be longer and still be more easily remembered. But make sure you use significantly different passwords for each account.
- The experts at the National Institute of Standards and Technology (NIST) say a good practice 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 they're not a grouping that is easily guessed, such as the names of your children or colors of the rainbow). An example 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.
- Be cautious with "knowledge-based" authentication questions such as first car or father's middle name, as the answers to many of these can be found on social media. If 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.
- Check to see if your password (or one you'd like to use) has been compromised by a data breach or hacking. Some browsers and websites offer this service.
- 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 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 message.
- 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 multifactor 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.

NIST 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