Using an easy-to-guess password is like locking the door but leaving the key in the lock. Strengthen your password with three simple tips from the United States Cybersecurity & Infrastructure Agency (US CISA):

1) Make them long, at least 16 characters is recommended by US CISA.

2) Make them random. You can do this by using a random string of mixed-case letters, numbers, and symbols. Example: J8dqa3@#XMo0Rs!? Another option Is to create a memorable phrase of 4-7 words. This is called a passphrase. Example: Syr@cusew1ntersarec0ld!

3) Make them unique. Use a different strong password for each account. Do not use the same password for more than one account!

When making a password, avoid the following:

- Do not use your network username as your password.
- Don't use easily guessed passwords, such as "password" or "user."
- Do not choose passwords based on information that may not be as confidential as you think, such as your birth date, Social Security number, phone number, or names of family members or pets.
- Don't use a consecutive string of numbers such as "1234."
- Do not use consecutive letter sequences found on the keyboard, such as 'asdfghjkl.'

Password Managers

A password manager is a software program to prevent password fatigue by automatically, generating, auto filling, and storing strong passwords. Password managers typically require a user to create and remember a single password to unlock to access the stored passwords.

There are many password managers available, with some offering both free and paid versions. Typically, the free versions have more limited features, and often, though not always, they restrict the number of devices you can use to access your saved passwords. Here are just a few examples of popular password managers. Remember, every password manager needs to be set up before it can be used. Every password manager out there has its strengths and weaknesses.

LastPass Offers both free and paid versions. The paid version offers password storage and syncing across multiple devices, the free version limits this feature to one device.

Bitwarden Free for unlimited devices, a paid version with additional features is available.

Proton Pass Free for unlimited devices, a paid version with additional features is available.

1Password No free version available. Only offers a paid for version.

NordPass Offers both free and paid versions. Made by the developers of NordVPN.

Chrome Password Manager Free with a Google Account. This is an integrated password manager for users of Google Chrome, syncing passwords across devices when signed in with a Google account. It’s a very seamless experience for Chrome users, especially since it auto-fills passwords and securely stores them in your Google account. However, it’s somewhat limited compared to full-featured password managers.

Samsung Pass Free on Samsung Products with a Samsung Account. Samsung Pass is designed for Samsung users, and it securely stores passwords, payment information, and even biometric data like fingerprints or iris scans for added security. It’s great for people using Samsung smartphones or tablets, as it integrates well with Samsung's ecosystem.

iCloud Keychain Free for any user with an Apple device and an iCloud account. iCloud Keychain works seamlessly for users within the Apple ecosystem, securely storing passwords, credit card details, and even Wi-Fi network information across all Apple devices (iPhone, iPad, MacBook, etc.). It's a great tool for Apple users, as it integrates directly with Safari and automatically fills in passwords when needed. However, it’s primarily geared toward Apple products and doesn’t have the cross-platform compatibility that some other password managers offer.