CYBERSECURITY AWARENESS MONTH

Make Strong Passwords to Boost Security

Managing passwords can be a challenge. Most of us don't have just one or two passwords, but dozens when you include work and personal accounts.

Keeping them updated and secure just adds to the challenge, but it doesn't need to be hard. By making a few simple practices password habits, we can help improve security and make our passwords easier to manage.

How Long is Long Enough?

The longer your password or passphrase the harder to crack. Most experts recommend password length should be at least 11 or 12 characters—longer is better. Even adding just one character to your password can boost its security exponentially. To see what kind of boost you can get by adding extra characters, check out How Secure is My Password?

Don't Skimp on the Characters

A typical computer keyboard has 94 characters. Use as many as you can, including upper- and lower-case letters, numbers and special characters.

Passwords Versus Passphrase

Cybersecurity experts debate whether it's better to use a password or passphrase. But a passphrase is just a kind of password that uses a series of words instead of a series of random characters, so does it really matter what they call it? What's important is that whatever you use—passphrase or password— it's long enough.

What about Password Managers?

A password manager is a great option. It can create hard-to-crack passwords, and then remember them for you. To access your password manager vault, you just need to remember one master password, not dozens. There are plenty of free password managers available for download. Click here to see the ones recommended by *CNET*.

Are your Passwords Secure Enough?

There are a number of free tools you can use to check up on your passwords. Websites like https://haveibeenpwned.com/, https://breachalarm.com/, and https://passwords.google.com/ check your info against a list of hacked records. If your name comes up, you need to change your password ASAP.