Cybersecurity Awareness Month – *Making passwords secure*

Passwords are everywhere - email, social media profiles, bank web sites, work documents, and smartphones are all protected by passwords. To keep information safe, the rules sound simple: passwords need to be long, different for every site, easy to remember, hard to guess and never written down. What can you do to help secure passwords?

1. Make the password long

Complexity is good, but length is best:
Time it takes to crack a password:

- ssnd#2011 – 1 day 20 hours
- ssndcppassword – 730 years 6 months

So how can you build a good passphrase that is easy to remember? One way is to build a short sentence using common grammatical components like: [**person/animal/thing] + [action] + [place/time/thing]**. Using that as a formula along with our password criteria, here are some examples of memorable and strong passphrases: "Birdsjumpon2trees!" or "Crayons&color4theworld."

2. Use different passwords for different accounts

Do you have the same password for most of your accounts? Well, it may be time to change things up! Having different passwords means that in the event of a security breach, you're more protected — the hacker may be able to access one system, but not all of them. If your password is the same on multiple sites, and someone gets access to one of them, it won't take long for them to find out that the password works in other places as well. This can be especially troublesome if those websites house your personal information, such as your bank account PINs and access numbers, your Social Security number and other sensitive material. The more different passwords you have, the harder it will be to hack all or many of your accounts.

3. Use a password manager

For those who need to keep track of a high volume of passwords and find yourself storing a long list of passwords in an Excel spreadsheet, paper notebook, etc. now is a good time to give a service like LastPass a try. The online password service works in a way that all passwords stored in it are encrypted. You create a master password and then store all your other passwords in your account, so it allows you to just remember the one master password.

If you still have the need to write down your passwords, it is important that they are kept in a safe space or locked away. If an intruder were to get access to that post-it note on your monitor or notebook left out in the open, they have access to all your passwords.

Please continue to follow along this month at our IT Resource Center where we will cover a variety of topics to help keep us safe in our digital lives!