
# OCTOBER 2022

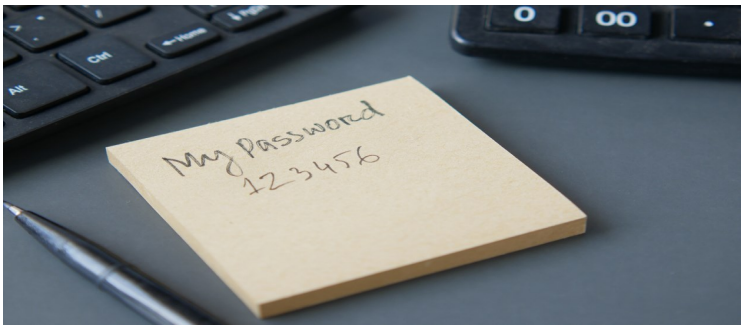
CYBERSECURITY AWARENESS MONTH 2022

October is Cybersecurity Awareness Month! It's that time of the year when we call attention to what we should be doing to keep ourselves safe online. In reality, though, we need to pay attention every single day of the year! Still, this document lists a number of things you should be doing to keep your Internet interactions safe and secure.

**STRONG PASSWORDS:** I can't emphasize enough the importance of using strong passwords. Yes, major computing companies like Microsoft, Apple and Google are working towards the elimination of passwords. However, for the moment, we still need them. Besides using strong passwords, you should not: use the same password everywhere; store passwords on your computer in a file; and, you should not save your passwords in a browser—regardless

**PASSWORD MANAGER:** If you have a number of passwords, you should use a password manager. These types of software store your passwords in an encrypted format and are not as easily hacked as those passwords stored in a browser. When using a password manager, make sure that your Master Password is the strongest password you use since it protects all your other passwords. Before you purchase one of these programs, investigate their history of

**TWO-FACTOR AUTHENTICATION:** Passwords alone are not good enough. For any account that allows you to do so, you should enable two-factor authentication. This process takes you a step further towards better security. Usually, there are three types of two-factor authentication: send a code to an email, send a code to a phone via SMS, and/or send a code to an authentication app. The last option is the most secure and the one I highly recommend.




**THINK BEFORE YOU CLICK:** There are three basic methods scammers use to trick you and compromise your computer or bank accounts or credit cards or identity. These are: 1) they try to panic you; 2) they try to appeal to your willingness to help others; 3) they attempt to tap into your dreams. Regardless of what method a scammer uses, you can prevent being scammed simply by thinking before you click (or tap or call).

**UPDATE SOFTWARE:** I've heard this reason for years, "My friend updated their computer and it crashed so I'm not updating mine." Hackers and scammers absolutely love computer users who think this way! Yes, it's true that, on occasion, a computing device update will cause an issue with that particular piece of equipment. However, the positive reasons for updating far outweigh the risks. Updates almost always fix security issues. If you want to help keep hackers out of your devices and accounts, be sure you update!

**USE AND KEEP CURRENT ANTI-VIRUS/ANTI-MALWARE SOFTWARE:** In the earlier days of computing, viruses—especially on Windows machines—were all the rage. However, in today's world, malware is the most common software used to compromise computing systems. You need to have good anti-malware on your devices. Yes, Mac users, that includes you! If you're an Android user, it's extremely important that you have anti-malware.