June 2020 – Technology Security Tip

Lock down your Log-in with MFA

Passwords are the keys to most devices and almost everything you do online. Unfortunately, even the best passwords can get hacked, stolen, or unintentionally shared. But fortunately, there is an easy way to add another layer of protection in addition to your username and password to make your log-in more secure. This is called multi-factor authentication, or MFA.

MFA, sometimes referred to as two-factor or two-step authentication, is a security enhancement that requires you to present an additional piece of information beyond your username and password when logging into an account. This additional information is usually in the form of:

- something you have (like an app on your phone, a token, or smart card)
- something you are (like your fingerprint or facial/speech recognition)

While two-factor authentication may seem like more work at first, it will make your accounts and personal information substantially more secure. Use MFA whenever possible, especially for your most sensitive accounts, like your email, bank accounts, health records, and social media. You can find a list of websites that offer MFA, along with step-by-step instructions for turning it on here.

Courtesy of www.ucop.edu