CYBERSECURITY BASICS FOR MULTI-FACTOR AUTHENTICATION

Have you noticed how security breaches, stolen data, and identity theft are consistently front-page news these days? Perhaps you, or someone you know, are a victim of cybercriminals who stole personal information, banking credentials, or more. As these incidents become more prevalent, you should consider using multi-factor authentication (MFA), also called strong authentication, or two-factor authentication.

This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code. By applying these principles of verification to more of your personal accounts, such as email, social media, and more, you can better secure your information and identity online.

MFA is defined as a security process that requires more than one method of authentication from independent sources to verify the user's identity. In other words, a person wishing to use the system is given access only after providing two or more pieces of information which uniquely identifies that person.

HOW AND WHEN MFA SHOULD BE USED

There are three categories of credentials: something you either know, have, or are. Here are some examples in each category:

- Something You Know: Password/passphrase, pin number.
- Something You Have: Security token or software application, verification text, call, email, or smart card.
- Something You Are: Fingerprint, facial recognition, voice recognition.

Your credentials must come from at least two different categories for you to gain access. One of the most common methods is to login using your username and password. Then a unique one-time code will be generated and sent to your phone or email, which you would then enter within the allotted amount of time. This unique code is the second factor. MFA should be used to add an additional layer of security around sites containing sensitive information, or whenever enhanced security is desirable. MFA makes it more difficult for unauthorized people to log in as the account holder. According to the National Institute of Standards and Technology (NIST), MFA should be used whenever possible, especially when it comes to your most sensitive data—like your primary email, financial accounts, and health records. Some organizations will require you to use MFA; with others, it is optional. If you have the option to enable it, you should take the initiative to do so to protect your data and your identity.

KNOW YOUR CYBER BASICS

To learn how to activate MFA on your accounts, visit the Lock Down Your Login Multi-Factor Authentication | CISA page, which gives instructions on how to apply this stronger form of security to many common websites and software products. If any of your accounts are not listed on that resource site, look at your account settings or user profile and check whether MFA is an available option. If you see it there, consider implementing it right away! Usernames and passwords are no longer sufficient to protect accounts with sensitive information. By using multi-factor authentication, you can protect these accounts and reduce the risk of online fraud and identity theft. Consider also activating this feature on your social media accounts!