Cyber Security Awareness Month

"Secure Our World"

Multi-factor Authentication (MFA)

What is MFA?

Multi-factor authentication, or MFA, is a security measure that requires anyone logging into an account or app to complete a two-step process to prove their identity.
Most MFA authentication methodology is based on one of three types of additional information:

- Things you know (knowledge), such as a password or PIN
- Things you have (possession), such as a badge or smartphone
- Things you are (inherence), such as a biometric like fingerprints or voice recognition

Why is it important?

MFA makes it twice as hard for criminals to hack an online account. When it's available, always turn it on; it's easy to do and greatly increases your security.

How does it work?

The first step is to create a password or passphrase. The second step is to provide an extra way of proving that you're you, like entering a PIN code or texting/emailing a code to your mobile device, or accessing an authenticator app.
Example:

- Step 1: Username and password are entered
- Step 2: One-time PIN from phone app entered

What type of accounts offer MFA?

Any online location that stores your personal information (especially financial information), or any account that can be compromised and used to trick or defraud someone else should be protected with MFA.

www.globallearningsystems.com