Frequently Asked Questions Regarding Multi-Factor Authentication

What is multi-factor authentication (MFA)?
Chances are you've used multi-factor authentication without realizing it. If you've logged onto your bank account and been asked to verify your identity through a text message or call with a generated code — that's multi-factor authentication. It's a software-based tool that's used to confirm that you are who you say you are using an additional authentication factor:

- Knowledge (what you know — a password or PIN)
- Possession (what you have — a mobile device or key fob)
- Inheritance (what you possess — a fingerprint, voice or face)

What is two-factor authentication (2FA)?
Two-factor authentication or 2FA is a subset of MFA that requires the user to present two pieces of evidence before gaining access to files or websites and is considered MFA. The first piece of evidence might be your user name and password and the second could be a security code sent to your email. Most companies require employees to use two-factor authentication to protect the company's network and customer data. The MIIA cyber application calls for MFA and 2FA satisfies that requirement.

Why do I need two-factor authentication?
You could be at risk of having your password stolen if you:

- Use the same password on more than one site, share it with your coworker, write it on a sticky note or use one that's easy to guess
- Download software from the internet – which could unwittingly result in malware being delivered to your device and provide a hacker with access to your municipalities' files on the network
- Click on links in an email message – which could be a phishing attack where an attacker sends a fraudulent email posing as a legitimate business to try to get your credentials or to place malware (malicious attachments or links) on your computer or network

2FA provides another level of security helping to keep hackers out (even if they have your password). Anyone who accesses files remotely should use 2FA.

What could happen if someone steals my password?
If someone steals your password and you don't use 2FA, you're inviting the intruder into your company network where they could introduce malware, access systems, steal data and launch a ransomware attack. The hacker could gain access to confidential financial documents, HR or credit card information tied to the residents who pay their city or town bills on the site, which could be devastating to the municipality and its many users.

Am I protected from this if I have antivirus software installed on my device?
Although antivirus software, such as Norton, helps to prevent, detect and eliminate malware and viruses, it doesn't protect you from having your credentials stolen. Using 2FA helps mitigate credential theft.

What do I need to do to enable 2FA?
You should work with your IT provider to enable 2FA within your municipality. There are many 2FA providers and there's minimal cost to implement these tools. Google Authenticator is the baseline because nearly all

sites that support 2FA support Google's app too. It's a software-based authenticator that implements two-step verification services and it's platform-agnostic so you don't need to be a Google user to use it. Please see the contract user guide for cybersecurity for additional information on state-approved providers.

Won't this be more work for me/my users?
The added security of 2FA outweighs the few seconds it will take for your users to authenticate themselves. Most people are already familiar with how the process works. It can be set up based on the user's preference (phone call, text or authenticator app) and provides peace of mind to the user and required cybersecurity for your organization.

Why does 2FA work?
2FA works so well because it's simple. You just need something you know (your password) and something you own (your computer, tablet or mobile phone). The goal is to add an extra layer of security to your online accounts with little disruption to your users.

Who should I contact if I have additional questions?
Please call the CyberNET Support Line at 877-574-6406. They're available to answer your MFA questions.

Download this advisory as a printable document

April 28, 2022

MIIA Risk Management
Work Safe. Be Safe.