TOIRMA Update

By Jim Donelan TOIRMA Executive Director

Multifactor Authentication (MFA) – Protect Your Information

We read about it every day. Electronic devices or systems being hacked and compromised. Whether it's your computer, tablet, or smartphone your information is being sought after for nefarious purposes. Within the past few years, my credit card information has been compromised a half a dozen times. That's the bad news. The good news is that there is a simple process to better help in securing the access points to your personal information/files. Multifactor Authentication (MFA). The following questions and answered have been developed to provide a better understanding of MFA.

Question 1: What is multifactor authentication (MFA)?
Answer: According to TOIRMA's cyber partner, Berkley Cyber Risk Solutions, MFA is "a best practice for security, but now it is effectively a prerequisite, minimal practice for digital security."

Question 2: How does MFA work?
Answer: MFA is a second form of authentication that verifies a user's identity before granting them access. This applies to PCs, Macs, tablets, and mobile devices.

Question 3: Why is MFA important?
Answer: Under certain circumstances, hackers can easily compromise your passwords, and once this happens your information is accessed. A breach can create havoc and be very costly to you and your township. MFA helps protect your information by utilizing an additional layer of security.

Question 4: What are the types of MFA available?
Answer: There are three types of MFA.

- Knowledge Based Authentication: Something you know, such as a password, answer to a question, or personal identification number (PIN).

- Possession Based Authentication: Something you have, such as mobile authentication (smartphone with an app or text message), or a security token (USB key).

- Inherence Factor Authentication: Something you are, such as a fingerprint, retina scan, or facial recognition.

Question 5: Which of the three types of MFA described in question 4 provide the best security?
Answer: Possession Based and Inherence Factor Authentication are the strongest. A common example of Possession Based Authentication is a one-time code sent to your mobile device. An example of Inherence Factor Authentication would be the facial recognition feature on an iPhone.

Question 6: What is the cost of MFA?
Answer: A number of MFA methods are included (and sometimes mandatory) with applications or services. An example of a low-cost way of better securing your devices that our staff uses is Microsoft's Authenticator application. This application is downloaded to your mobile device and is available at no cost to existing customers. Whatever method you are seeking, we encourage you to consult with your IT advisor about MFA and implementation in your townships.

Question 7: Are there MFA resources are available to TOIRMA Members?
Answer: Yes. TOIRMA has developed new MFA *Risk Reminders* that are available in the "Members Only" section of the TOIRMA website, toirma.org.

In addition, members have access to online cyber resources and trainings through eriskhub.com/berkleycyberrisk. These tools are designed to better equip townships in reducing cyber liabilities and exposures and are available on the "Members Only" section of the website. To obtain your access code, contact Carla Hilligoss at chilligoss@ccmsi.com, (217) 444-2111.

Thank you for your attention to these matters.

As always, if you have any additional questions, please feel free to contact me toll-free at (888) 562-7861 or by email at jdonelan@toirma.org.

Think Safe . . . Drive Safe . . . Work Safe