TOIRMA Update

By Jim Donelan TOIRMA Executive Director

Cyber Liability – Multifactor Authentication (MFA)

Have you ever said or heard: "It can't happen to me." or "Does this really apply to me?" I remember these types of questions coming to mind regarding identity theft. I mean I really, I thought, "I'm careful and who would want to have my information." That line of thinking was just fine for a while until my credit cards were breached, not once, but six times. Cyber liability is no different.

As a township official you may be thinking as I once did regarding identity theft as it relates to cyber liability and your township. However, if you have a smartphone, tablet, personal computer, or laptop, you need to be prepared. The days of using "password123" or the same password for all of your online accounts or applications is over. It only takes one breach to impact you on multiple fronts.

What is multifactor authentication (MFA)?

According to Berkley Cyber Risk Solutions, multifactor authentication (MFA) is "a best practice for security, but now it is effectively a prerequisite, minimal practice for digital security." This helps protect online accounts by using the strongest authentication tools available, such as biometrics or a unique one-time code that is sent to your phone or mobile device.

This is a low-cost way of better securing your devices. Microsoft, as an example, has an MFA authenticator application available at no cost to existing customers. Please ask your IT advisor about MFA and implementation in your systems.

Is it important to update applications?

Yes. Whether is it's your device's operating system or applications such as Office 365 it is critical to keep all updated with the latest version. Companies constantly update applications to address the latest security concerns, and if you are not up-to-date you are more vulnerable to attacks or breaches.

What is Phishing

Phishing emails look like they came from a person or organization you trust, but in reality they're sent by hackers to get you to click on or open something that gives them access to your computer.

Be mindful of phishing attacks. Phishing emails look legitimate, and appear to be from a reliable company, organization, or even other townships officials or employees. Phishing emails often have the following characteristics:

- Ask you for your username and password, either by replying to the email or clicking on a link that takes you to a site where you're asked to input the information;
- Look like they come from your human resource or information technology (IT) personnel; and
- Have grammatical errors.

What Resources are Available to TOIRMA Members?

TOIRMA members may access online cyber resources and trainings, through eriskhub.com/berkleycyberrisk. These internet-based tools are designed to better equip townships in reducing cyber liabilities and exposures. To obtain access to eRiskHub, please visit the "Members Only" section of the TOIRMA website, toirma.org, or contact Carla Hilligoss at chilligoss@ccmsi.com, (217) 444-2111 to obtain your access code.

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

TOIRMA

toirma.org