TOIRMA

toirma.org

TOWNSHIP OFFICIALS OF ILLINOIS RISK MANAGEMENT ASSOCIATION

RISK REMINDER

MFA WHICH TYPE TO USE

Remember, any form of multi-factor authentication (MFA) is better than no MFA.

Here are the most popular forms of MFA (in order of strength) from weakest to strongest:

- **Text Message (SMS) or Email**: When you login to an account, the service will send a code to your phone or email account, which you then use to login. Note that the SMS/mail is the weakest form of MFA, and you should only use it if none of the other options are available.
- **Authenticator App:** An authenticator app is one that generates MFA login codes on your smartphone. When prompted for your MFA code, you launch the app and type in the displayed number. These codes often expire every 30 or 60 seconds.
- **Push Notification**: Instead of using a numeric code, the service “pushes” a request to your phone to ask if it should let you in. You will see a pop-up and can approve the login request or deny it if you did not initiate the authentication request.
- **FIDO Authentication**: FIDO stands for "Fast Identity Online" and is the gold standard of multi-factor authentication. The FIDO protocol is built into all major browsers and phones. It can use secure biometric authenticators like facial recognition, a fingerprint, or voice recognition.

Any MFA will enhance your cyber protection and will reduce your risk.
Only FIDO authentication is phishing resistant.

TOIRMA recommends consulting your IT Department with any questions.

For more information, contact your Loss Control Consultant at (888) 562-7861

CLAIM REPORTING HOTLINE (844) 562-2720 | Available 24/7