TOWNSHIP OFFICIALS OF ILLINOIS RISK MANAGEMENT ASSOCIATION

RISK REMINDER

toirma.org

CYBER SAFETY BEST PRACTICES

1) THINK BEFORE YOU CLICK

If you receive an enticing offer via email or text, don't be so quick to click on the link. Instead, go directly to the company's website to verify it is legitimate. If you're unsure who the email is from, or if the email looks "phishy," do not respond and do not click on any links or open any attachments found in that email. They may be infected with malware.

2) WHEN IN DOUBT, THROW IT OUT

Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Links in email, tweets, texts, posts, social media messages and online advertising are the easiest way for cyber criminals to get your sensitive information.

3) LOCK DOWN YOUR LOGIN

Create long and unique passphrases or passwords for all accounts and use multifactor authentication (MFA) wherever possible. MFA will help protect your online accounts by utilizing the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

4) SHARE WITH CARE

Think before posting about yourself and others online. Consider what information a post reveals, who might see it, and how it might affect you and/or others.

5) BE CAUTIOUS OF PUBLIC NETWORKS AND WIFI HOTSPOTS

Public wireless networks and hotspots are not secure. Limit what you do on public WiFi and avoid logging in to key accounts like email and bank accounts. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.