SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING FEBRUARY 13, 2023

Submitted by Arnold H. Shifrin

Some Ways To Protect Yourself On The Internet

- Be very skeptical of emails you receive from individuals you don't know. Internet imposters are not who they claim to be and are responsible for the majority of online scams.
- Don't click on links or open attachments in unsolicited emails or text messages if you don't know the sender. You may unknowingly be directed to bogus websites.
- Use strong passwords and 2-factor authentication (2-FA) to access your accounts and keep your online data safe.
- Look for a "lock" icon and "https" preceding the URL in the browser address bar before providing your personal information. These generally signify the site is secure and encrypted.
- Check the URL for misspellings and wrong domains. Examples: ***arnazon.com*** (look closely; the first three letters of the address are "a, r, n" NOT "a, m, a."), ***betsbuy.com, walmrt.com,*** and **neimanmarcs*.com***.
  - Examples of legitimate domain names: ***.com***, ***.org***, ***.net***, ***.edu***, and ***.gov***.
  - Examples of domains reputed to circulate malicious content: ***.xyz***, ***.icu***, ***.ru***, ***.cn***, and ***.tk***.
- If you receive an email from the IRS, your bank, a credit card company, the local police department, a utility company, or Medicare threatening you with arrest or a monetary fine if you fail to provide or confirm your personal information, delete the message. It's from a scammer. Do not provide the requested information, click on links, or open attachments in the message.
- If you wish to confirm the validity of a message, contact the sender at a website or telephone number you know is correct, not one that was given to you by someone else. A sender's legitimate telephone number can be obtained from their website or a receipt.
- If you receive a message that you are the winner of a lottery or some other drawing and all you have to do to collect your winnings is to pay a small shipping and handling fee, you are dealing with a scammer. Did you enter such a drawing? If you never entered a contest, you couldn't be a winner.
- If you're in a public Wi-Fi environment such as Starbuck's, a library, or an airport, do not conduct online business (e.g., pay bills, access bank accounts, make purchases). These settings are generally not secure and scammers located near you may be able to access your personal information.
- If you are using a public computer in a library, school, or government facility, make sure you completely log out when you're finished.
- Before making charitable contributions, verify that the organizations are registered with the IL Attorney General's office and that their registrations are current.
- Scammers often try to rush their victims into making hasty decisions. Don't let tight deadlines or threats of harm or arrest cause you to panic and act without first verifying the facts.
- If you purchase something online and are told to pay with a gift card, prepaid debit card, or by wire transfer, you're dealing with a scammer. No legitimate business will require you to pay this way.
- Keep current with updates for your computer. Microsoft, Adobe, and other companies release software patches for their products on "Patch Tuesday," the second Tuesday of each month.
- Do not save your passwords in a file on your computer or on a piece of paper you keep in your pocket or purse. Instead, use an encrypted software program (e.g., LastPass®) to manage your passwords.
- Regularly back up your data to an external hard drive and/or the cloud. If your system is breached (e.g., virus, malware, ransomware), a comprehensive backup will help you restore any lost data.

[Sources: Various]