MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING MAY 8, 2023
Prepared by Arnold H. Shifrin

HOW TO PROTECT YOURSELF FROM SCAMMERS

1. Do not click on links or open attachments in unsolicited emails.
2. If you do not recognize the telephone number on your Caller ID, let the call go into voice mail. You can then pick up the message at your convenience.
3. If you answer the phone and realize it's a scam call and then hang up, your telephone number is sold to other scammers as a number that someone will answer when it's called.
4. If you answer the phone and the caller says: "Can you hear me?" do not say "Yes." Scammers record your response as a confirmation that you agreed to make a purchase. Answer with anything but "Yes."
5. The IRS, Medicare, Social Security, ComEd, Nicor Gas will not call you to say you owe money. They will not call you to confirm or update your account information. Contact from these agencies will be via U.S. Mail.
6. If someone comes to your door and tries to lure you outside on the pretense of tree branches that need trimming, a fence that must be moved, or the need to check your water meter, do not open the door. Keep the door locked and call the local police. This is an attempt to distract you so other criminals can enter your house and steal money and jewelry while you're in the yard.
7. If you wish to contact a business, contact them at a number or website you know is correct, not at a number or website given to you by someone else.
8. Do not access your bank account, make an online purchase, or conduct other business in a public Wi-Fi environment (e.g., library, airport, or Starbucks). Others who are nearby may be able to access your personal information.
9. If you receive a telephone call allegedly from a grandchild in need of money because they were in an accident while attending a friend's wedding out of state, it is a scam. Hang up the phone. Call your grandchild or his / her parents to confirm the child is OK.
10. If you make an online purchase and are told that payment must be made with a debit card, prepaid gift card, or by wire transfer, you are dealing with a scammer. No legitimate business will insist that payment has to be made in this manner.
11. If you receive a call or email that you won a lottery or sweepstakes contest and all you have to do is pay a small handling fee to collect your winnings, you are dealing with a scammer. Try to recall if you ever entered such a contest. You could not possibly be a winner if you were never an entrant.
12. File your income tax return as early in the year as possible. This prevents a fraudster who has stolen your identity from filing a return in your name and receiving a refund to which you are entitled. Tax fraud scams should be reported to the FTC (*identitytheft.gov*).
13. Under Illinois law, charitable organizations are required to register each year with the Attorney General's office. Before donating to a charity, verify it is registered and that its registration is current.
14. Do not "play games" with scammers and deliberately try to keep them on the line by feigning interest in what they are selling. Though you may think you're "getting even," what's actually happening is that your telephone number is categorized as one that will be answered by a live person and is sold to other scammers. The result is that you will start receiving more calls from scammers than you had been receiving previously.
15. When conducting business online, be sure the URL address in the address bar of your browser is preceded by a "padlock" icon before entering your personal information. This signifies the site is secure and that your personal and financial information are encrypted.
16. If you are the victim of a scam, notify the Illinois Attorney General's Senior Fraud Helpline (1-800-243-5377) and your local police department.