SCAM REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING MAY 12, 2025

Prepared by Arnold H. Shifrin, RPh

How to Avoid Being a Scam Victim

1. Do not answer calls from unknown numbers; let those calls go to voicemail. You can retrieve a voice mail message and return the call at another time if you wish. If you don’t answer the call, your number will not be sold to criminals on the “dark web” as a “live” number.
2. Your caller ID can be spoofed, so do not trust it to verify who is calling.
3. If you answer a call and it seems suspicious, hang up. You are not being rude by doing so. Your safety comes first.
4. Do not click on links or open attachments in unsolicited emails.
5. Do not share personal and financial information with unsolicited callers.
6. Look for “https” in the address bar of a website before submitting personal and financial information. This signifies the site is secure and the transmitted data is encrypted.
7. If you receive a threatening call about an unpaid bill or late taxes, hang up. To confirm whether you owe a balance, contact the caller using contact information from the payee’s website or a previous statement or receipt. Do not use information given to you by someone else.
8. Pay for purchases with a check or credit card, as these offer some fraud protection if you are scammed. Do not pay with cash, gift card, prepaid debit card, wire transfer, or cryptocurrency.
9. Register your telephone number with the national Do Not Call Registry (1-888-382-1222) to stop receiving telemarketing calls. Your registration never expires and does not have to be renewed.
10. Determine if your phone carrier offers call-blocking tools or apps to stop unwanted calls.
11. Do not press any buttons on your phone to stop receiving Robocalls. If you do, your number is sold to criminals on the “dark web” as a “live” number and you will receive even more calls.
12. Before investing in cryptocurrency, talk with a trusted and knowledgeable financial advisor. Be sure to become familiar with crypto technology and terminology.
13. Be skeptical of demands for mandatory payments with cryptocurrency, as these are likely scams.
14. Enable two-factor authentication (2FA) to access your online accounts; this adds another layer of protection to the accounts.
15. Shred all paperwork that contains your personal information before discarding.
16. Regularly check to make sure your computer’s software is current (e.g., Windows, Google).
17. Do not conduct online financial transactions on public networks such as those found in libraries, coffee shops, and airports. These environments do not provide secure connections and your personal information may be vulnerable to theft.
18. Be alert for communications with spelling and grammatical errors. These often originate from scammers in other countries.
19. Do not allow strangers to enter your residence for any reason (ruse burglaries). If you are asked to step out of your house to view something in your yard, lock your door before leaving.
20. Do not grant remote access to your computer for repairs unless you initiated the contact and trust the individual.
21. If you are a victim of a scam, report it to the following agencies:
    a. Federal Trade Commission (reportfraud.ftc.gov),
    b. Illinois Attorney General Senior Citizens Consumer Fraud Hotline (tel: 1-800-243-5377 or email: seniorhelpline@ilag.gov),
    c. FBI’s Internet Crime Complaint Center - for online scams (www.ic3.gov), and
    d. your local police department.

[Sources: Varied]