**SCAM REPORT**

**MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING JULY 14, 2025**

Prepared by Arnold H. Shifrin, RPh

## Refund Phishing Scams

In refund phishing scams, fraudsters pretend to be representatives from well-known companies or government agencies to convince victims they are owed a refund. They use fake communications designed to look legitimate to trick victims into providing sensitive personal information.

**How it works:** Victims receive calls, emails, or text messages stating they are eligible for refunds due to overpayments for goods, services, or taxes. They are told their personal information is needed to process the refund and instructed to act quickly before the offer expires. Instead of issuing a refund, the scammers steal sensitive information, such as Social Security numbers (SSNs), bank account details, or credit card information.

Victims are often asked to click links or open attachments in emails or text messages to process a refund. These lead to fake websites designed to extract personal information or install malware.

### How to protect yourself

- Do not respond to suspicious refund messages, including those in which you are told to act quickly before the offer expires.
- Do not open attachments or click links in unsolicited messages.
- If you believe a refund message is legitimate, contact the sender for verification. Use trusted contact information, not information provided in the message.
- Look for messages with poor grammar and spelling errors, as these are signs of scams originating in other countries.
- Be wary of generic greetings such as "Dear Customer" instead of your actual name.
- Do not be fooled by AI-generated voices that are used to make telephone scams sound convincing.
- Never grant remote access to your device to anyone claiming they need it to process a refund.
- Be cautious of spoofed calls. Your caller ID may have been manipulated to confirm the caller's identity.
- When offered, enable multi-factor authentication (MFA) for your online financial accounts to add an extra layer of protection.
- Use strong, unique passwords for your online financial accounts. Consider using a password manager.
- Be sure your device is protected with reliable antivirus and anti-malware software.
- Keep the operating system and web browser on your device up-to-date
- Regularly monitor your financial accounts for suspicious activity.
- Be wary of scam recovery offers. Scam victims are often exploited a second time by fraudsters who offer to recoup their losses in exchange for personal information or an upfront fee.

### Notify the following agencies if you are a victim:

- Illinois Attorney General Senior Citizens Consumer Fraud Helpline: 1-800-243-5377 or seniorhelpline@ilag.gov.
- Federal Trade Commission (FTC): www.identitytheft.gov. Victims who report identity theft to the FTC receive a personalized recovery plan from the agency.
- Internet Crime Complaint Center (IC3), an agency run by the FBI: www.ic3.gov.
- If you are the victim of a phishing scam related to tax matters, notify the IRS: phishing@irs.gov.
- Your bank or financial institution.
- Your local law enforcement agency.

*[Sources: IRS, FBI, FTC]*

# NOTICE

## Distracted Driver Ticket Scam

Recently, Milton Township became aware of a scheme to use the Milton Township logo and name on traffic Tickets. These Tickets are not issued by the State of Illinois, the DuPage County Sherriff's Office, or any local City/Village law enforcement Agencies. If you have received a Ticket for "Distracted Driving", please call the Township Office, at (630) 668-1616; or take this matter directly to the DuPage County States Attorney's Office, at (630) 407-8000.

Milton Township will continue to work closely with local law enforcement authorities to investigate and take appropriate steps regarding this matter.