SCAM REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING JANUARY 13, 2025

Prepared by Arnold H. Shifrin, RPh

ComEd Impersonator Scam

Background: In February 2024, ComEd implemented an upgraded billing system in which new account numbers were assigned to all residential and business customers. Scammers have exploited the change to target unsuspecting ComEd customers.

How the scam works: You receive an unsolicited call from someone impersonating a ComEd employee. Though "ComEd" appears on your caller ID, the call is fraudulent. The caller claims no payments have been posted to your account since the system upgrade and demands immediate payment to prevent disconnection of service. When you question how service could be terminated without prior notice, the agent tells you ComEd sent you four notices that you must have ignored.

The agent directs you to a ComEd website to make the payment. Upon visiting the website, you are prompted to make payment with a prepaid card, wire transfer, or cryptocurrency. You may be asked for your Social Security Number, bank account details, or other sensitive information. The scammer creates a sense of urgency and tries to pressure you to act swiftly before you can consult with relatives or friends.

Once the scammer obtains the payment information, the money is lost and cannot be recovered. If you provided personal and banking information, the scammer will steal your identity and money from your accounts.

How to protect yourself:

- If you receive a call demanding immediate payment or threatening service disconnection, hang up the phone.
- Contact ComEd Customer Service at 1-800-334-7661 (1-800-EDISON1) or visit *comed.com* > *My Account* to verify the status of your account. Do not use contact information provided by the caller or anyone else.
- Do not share personal information with unsolicited callers. Legitimate ComEd employees will not ask for your personal or financial information.
- ComEd will not ask for payment by cash, prepaid cards, wire transfers, or cryptocurrency. If you are requested to make payment by these methods, you are dealing with a scammer.

Notify the following agencies if you are a victim:

- ComEd Customer Service (1-800-334-7681 or *comed.com* > *Stay Alert* > *Report a scam*).
- Illinois Attorney General's Senior Citizens Consumer Fraud Helpline (1-800-243-5377 or *illinoisattorneygeneral.gov/consumer-protection*).
- Federal Trade Commission (*reportfraud.ftc.gov*).
- Your local law enforcement agency.

[Sources: ComEd, Nextdoor]

BBB Tip: Top resolutions for a fraud-free new year

BBB recommends adding a few precautionary steps to the New Year's resolution list and the weight loss and financial goals to help make the upcoming days and months fraud-free.

- **I resolve to be cautious with email.** Be wary of unsolicited emails from a person or a company. Remember, scammers can make emails look like they are from a legitimate business, government agency, or reputable organization (even BBB!). Never click on links or open attachments in unsolicited emails.
- **I resolve never to send money to strangers.** If you haven't met a person face-to-face, don't send them money. This is especially true if the person asks you to transfer funds using a pre-paid debit card or CashApp. Money sent to strangers in this way is untraceable, and once it is sent, there's no getting it back. Scammers will try to trick you into panicking – so before making a move, think the situation through. Don't fall for it!
- **I resolve to do research before making online payments and purchases.** Research the retailer before entering payment information when shopping online, or if asked to pay online, research the retailer before entering payment information. Ask: Is this a person or business I know and trust? Do they have a working customer service number? Where is the company physically located? Would I be making payments through a secure server (https://....com)? Have I checked to see if others have complained?
- **I resolve to use my best judgment when sharing my personal information.** Sharing sensitive personal information with scammers opens the door to identity theft. Never share financial information, birthdate, address, Social Security/Social Insurance number, or Medicare number with an unsolicited caller.
- **I resolve to create strong, unique passwords for each account.** Using strong, varied passwords across accounts makes it harder for fraudsters to access multiple accounts if one is compromised.
- **I resolve to enable two-factor authentication.** Adding this layer of security to accounts, especially those involving finances or personal data, greatly reduces the risk of unauthorized access.
- **I resolve to be social media smart.** Use privacy settings on social media and only connect with people you know. Be careful about including personal information in your profile, and never reveal your address and other sensitive information – even in a "fun" quiz. Scammers may use this information to make themselves pass as friends or relatives and earn your trust. Also, be careful when buying products you see on social media. BBB Scam Tracker has received thousands of complaints about misleading Facebook and Instagram ads.
- **I resolve to regularly check my financial statements.** Committing to review bank and credit card statements can help catch unauthorized transactions early.
- **I resolve to educate myself about the latest scams.** Staying informed on emerging scams helps you recognize and avoid new fraud tactics.

[Courtesy of the Better Business Bureau]