SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING SEPTEMBER 12, 2022
Submitted by Arnold H. Shifrin

WINDOWS 10 RANSOM SCAM

How it works: You receive an email message with the subject line "Install Latest Microsoft Windows 10 Update Now." You're instructed to click on a link in the message to install the update. If you follow the sender's instructions and click on the link, ransomware is installed on your system. Your files are encrypted and locked, and you cannot retrieve the data until a demanded ransom is paid.

If you refuse to pay the ransom, you will be denied access to your files. The perpetrators use the personal and financial information captured from your system to steal your identity and remove money from your accounts. The stolen information is sold to other criminals, exposing you to further losses.

Facts to keep in mind

- By default, the setting for automatic Windows updates is enabled on all systems. You do not have to manually install updates unless the setting has been disabled.
- It is advisable to periodically verify that the Windows version installed on your system is current even if the default setting for automatic updates has not been disabled. To do this, go to the Windows Update utility as follows: *Start* > *Settings* > *Update & Security* > *Check for updates*. If updates are available, you'll be able to download and install them. You will also see a history of previous updates to your system.
- If you prefer, you can download Windows updates directly from the Microsoft website at *https://www.catalog.update.microsoft.com/Home.aspx*. You can verify this site is legitimate by the "padlock" symbol that precedes the URL in the address bar at the top of the screen. The padlock signifies the connection is secure and encrypted.
- Do not install Windows updates from links or attachments in emails. These messages are sent by scammers and should be immediately deleted. Never click any links or open attachments in unsolicited emails regardless of who the sender claims to be.
- If you receive an unsolicited telephone call from someone claiming to represent Microsoft who offers to help you with a Windows update, hang up the phone. You are dealing with a scammer. Legitimate Microsoft agents never initiate contact with customers and offer to assist with Windows updates or provide other technical support.
- Do not give out your personal or financial information to callers claiming to be from Microsoft. Legitimate Microsoft agents will never ask for this information.
- Do not click on internet "pop-up" ads that suddenly appear on your screen and offer assistance with Windows updates. These ads are furtive attempts by scammers to install ransomware or other types of malware on your system in an attempt to steal your personal information.
- Be sure to make regular system backups. Even if you pay the ransom, there is no guarantee you'll be able to recover all your data. System backups may help you recover some or all of any lost information.

What to do if you're a victim of this scam

- Report fraudulent communications you receive about Windows updates to Microsoft at *https://support.microsoft.com/reportascam*.
- If you lost money or had your identity stolen in this scam, report the incident to the following agencies:
    - Federal Trade Commission at *identitytheft.gov* or 1-877-438-4338;
    - Internet Crime Complaint Center (IC3) at *https://www.ic3.gov/Home/*FileComplaint;
    - Illinois Attorney General's Senior Fraud Helpline at 1-800-243-5377; and
    - Your local police department.

[Source: Microsoft Corporation]