SCAM REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING DECEMBER 11, 2023

Submitted by Arnold H. Shifrin

Quishing Scam

Definitions

- Phishing: a scam in which the perpetrator poses as a legitimate business or reputable person to acquire an individual's personal and financial information.
- Quishing: a phishing scam that uses QR codes. Quishing is also known as QR code phishing.
- Example of a QR code (QR code stands for Quick Response code):

Background: Quishing is a relatively new practice but is a larger threat since the use of QR codes has become widespread. QR codes evolved during the pandemic and are used for touchless transactions. These include reading digital restaurant menus, submitting job applications, checking in at entertainment and athletic venues, paying automobile parking meter charges, and receiving discounts and special offers from retail merchants.

How the scam works: Criminals create fake QR codes that look legitimate. The fake codes are embedded in emails, text messages, social media posts, flyers, and posters. When you scan one of these codes with your device, you are redirected to a scammer's website and asked for your personal and financial information to complete what you think is a legitimate transaction. If you provide the requested information, your identity will be stolen and money removed from your account. While visiting the scammer's website, malware or ransomware will be downloaded onto your device, threatening your system's security.

How to protect yourself

- Do not scan QR codes from unknown sources. If you inadvertently do so, do not click any links on the site to which you are taken.
- Be sure there are no visible signs of damage or tampering before scanning a QR code.
- After scanning a QR code, be sure the destination URL in your browser's address bar is one you expect. You are dealing with a scammer if there are grammar and spelling errors or odd characters and symbols.
- Be cautious if you receive emails containing a QR code you are asked to scan. Look for signs intended to make a fake website to which you are directed appear legitimate. If in doubt, contact the company or organization from which the message is supposed to originate.
- Do not scan a QR code that promises a reward, free merchandise, or a discount if you make a purchase. These are underhanded attempts to obtain your personal and financial information.
- Be sure your device's operating system and browser software are current.
- When offered, enable two-factor authentication (2FA) for your financial accounts. This provides an extra layer of protection against unauthorized access.
- When scanning a QR code for a business transaction, be sure the website to which you are directed is encrypted and secure before providing your personal and financial information. The website is considered safe if a "padlock" icon appears to the left of the URL in your browser's address bar.
- If you are a victim of this scam, report it to the following agencies:
  - FBI's Internet Crime Complaint Center (*www.ic3.gov*),
  - Better Business Bureau (*www.bbb.org*),
  - Illinois Attorney General Senior Citizens Consumer Fraud hotline (1-800-243-5377),
  - business or organization the QR code claims to represent, and
  - your local police department.

[Source: U.S. Dept. HHS (HC3)]