SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING APRIL 11, 2022

Submitted by Arnold H. Shifrin

QR Code Scams

Background: The QR (Quick Response) code has become very popular during the pandemic as a touchless means of reading restaurant menus, receiving discounts at retail stores, and making mobile bill payments. We're familiar with the barcode which is one-dimensional and contains information horizontally. The QR code is a two-dimensional barcode that includes a substantial amount of information horizontally and vertically. It enables a user to access the information quickly. Following is a sample QR code:

Sample QR Code

How it works: Though it's convenient and rapid, scanning a QR code can expose one to scams and malware. Scammers have created QR codes that are designed to trick unsuspecting victims into divulging their personal and financial information. When these bogus QR codes are scanned with a smartphone or Android device, victims are taken to fraudulent websites that are designed to obtain their sensitive information or redirect monetary payments from their intended destinations.

Some QR codes are embedded with malware. When these codes are scanned, criminals gain access to a victim's cell phone or device and, in turn, their personal and financial information.

How to protect yourself

- When you scan a QR code, read the complete address of the website to which you're taken. Make sure there are no spelling errors or unusual characters and that the site matches what you expected.
- Be cautious if you're requested to provide personal or financial information on a site you navigated to from a QR code. Does it seem reasonable that your personal information is necessary for what you're trying to accomplish? Before you enter the information, look for a padlock icon and "*https:*" in the address bar to confirm that the site is secure.
- Make sure there are no visible signs of tampering before you scan a QR code. For example, stickers have been placed over QR codes on parking meters causing a customer's payment and personal information to be redirected to a scammer's site.
- Avoid making payments through sites you navigated to from QR codes plastered on your vehicle's windshield, handed to you by strangers, or found in public locations such as airports or bus stops.
- To make a purchase using a QR code: 1) open the payment app on your phone, 2) scan the QR code of the item, and 3) confirm the details to process the payment. CAUTION: Be sure the payment app was downloaded from your phone's app store and not from some other source.
- If you receive an email from a company stating that a payment you recently made failed to post and that you must complete the payment through a QR code, delete the email. You are dealing with a scammer. To confirm the status of a payment, contact the company at a telephone number you know is legitimate.
- If you receive an email message containing a QR code that you're asked to scan, be very cautious. You may be dealing with a scammer. A legitimate sender would not ask you to connect to another website by scanning a QR code with your phone or other device if you're already online.
- If you're a victim of a QR code scam, file a report with your local police department and the FBI's Internet Crime Complaint Center (IC3) at *www.ic3.gov.*

[Resources: ABC News, McAfee, Trend Micro]