SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING MARCH 8, 2021 (VIRTUAL)
Submitted by Arnold H. Shifrin

"Catfishing" Scams

A catfish is someone who creates a false identity on internet dating and social media websites and uses lies, exaggerations, and flirtatious remarks to establish relationships with strangers. Catfish will often spend many months "grooming" their victims in order to gain their trust and confidence. Once this is accomplished, catfish tell their victims they've suffered a recent financial setback and need money to cover medical or legal expenses. They may claim they're stranded in a foreign country and don't have the funds necessary to return home. Victims are told the money will be paid back once the scammers recover from their financial predicament.

"Romance" scams are the most common type of catfish scam. These scams largely target elderly women who are lonely and looking for affection and companionship. Elderly women are often financially stable and are excellent prey for catfish.

Catfish also commit identity theft, extortion, and residential robbery with the personal information they obtain from their victims. These criminals operate from many countries throughout the world, which makes it difficult for U.S. law enforcement officials to apprehend them. *[Resource: McAfee]*

COVID-19 Vaccination Record Card Warning

The COVID-19 Vaccination Record Card that one receives after being vaccinated should not be posted on social media sites (e.g., Facebook, Twitter, LinkedIn). Law enforcement agencies report that individuals who posted replicas of their cards on these sites have had their identities stolen. Fraudsters were able to capture personally identifiable information contained on the cards and use it for illicit purposes. *[Resource: FTC]*

"Netflix" Scam

The coronavirus pandemic has caused people to spend more time than usual at home. Many have found that subscription-based streaming services are excellent sources of entertainment while they're confined. A scam has recently surfaced in which victims receive calls, emails, or text messages offering services such as Netflix or Hulu at no cost for the first year and at significantly reduced rates thereafter. Though these offers are enticing, they are covert attempts to obtain a victim's personal and financial information. Criminals use the information to steal a victim's identity, or they may sell it to other scammers. Needless to say, victims never receive the streaming services to which they subscribed.

If you receive such a call, you can confirm the legitimacy of the offer by contacting the service provider directly at a number or website you know is correct, not one furnished by someone else.

[Resource: Scambusters]