SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING SEPTEMBER 13, 2021

Submitted by Arnold H. Shifrin

Online Food Ordering Scam

During the COVID-19 pandemic, ordering food from restaurants for delivery or carryout has been very common for many families. Scammers, however, have taken advantage of this practice to steal money and personal information from unsuspecting consumers.

How it works: You search the internet for a neighborhood restaurant that offers online ordering and provides delivery service to your residence. You find one with a suitable menu and delivery schedule. You click on the link, place your order, and enter your payment information. You patiently wait for the delivery, but the order never arrives. You call the restaurant and are told there is no record that you placed an order.

Instead of arranging for your order to be delivered, you may have opted to pick it up in person. You arrive at the restaurant at the designated time and are told there is no record of your order. You produce the "confirmation" that you printed from the website after placing the order, but you're told that it's a counterfeit document and was not sent by the restaurant.

Here's what happened: The website on which you placed the food order is a fake and is operated by fraudsters. You were the victim of a scam that is commonly referred to as "phishing" and were tricked into revealing your personal information. The scammers use that information to steal your identity and make fraudulent purchases that are charged to your account. Your personal information is then sold to other criminals.

How to protect yourself:

- Call the restaurant before you place your first order and verify that they have online ordering. This will help establish the credibility of the restaurant's website.
- Order only from websites that you know and trust. Verify the URL in the address bar before placing your order.
- Before entering your payment information, verify that the restaurant's website contains a "padlock" or "https://" preceding the URL. The "padlock" image and the letter "s" in "https" confirm that the website is secure.
- If you're satisfied that the site is secure, you should pay with a credit card. Credit card companies will usually assist their customers if disputes arise over fraudulent charges.
- Do not pay with a debit or gift card or send money by wire transfer. If you do, the money is gone and cannot be recovered. Warning: If a business insists that payment must be made with a debit card, gift card, or by wire transfer, you are dealing with a scammer.
- If you are a victim of this scam and paid with a credit card, contact your bank immediately to cancel the card and request a replacement. Consider putting a fraud alert on your credit reports at one of the three national credit reporting agencies (Trans-Union, Experian, or Equifax). Note: When you request a fraud alert at one credit bureau, it is automatically added at the other two bureaus.
- If you are a victim of this scam, file a report with your local police department.

[Source: BBB]