Common Online Shopping Scams

With the holiday season upon us, and more and more shopping happening online, it's important to recognize scams before you fall victim. Aside from fake websites, there are other ways that fraudsters take advantage of individuals completing their holiday shopping online. To ensure safe online shopping this holiday season, follow these few safety tips:

- ***Do not connect to public Wi-Fi to make purchases.*** Public Wi-Fi is not a secure connection and can easily be manipulated by fraudsters to capture your data as you enter it over that Wi-Fi connection. Anyone could be monitoring your data. In addition, we suggest that you do not enter any of your financial applications while connected to public Wi-Fi.
- ***When completing your purchase, use a payment device that has built in fraud protection,*** like a credit card that has fraud monitoring, or PayPal which does not share your personal banking information with the seller. Consider purchasing a prepaid debit card for risky or unverifiable websites.
- ***Do not respond to or click on links in emails that come from merchants which state delayed shipping, cancellation of the purchase, or that there is a general issue with your order.*** Fraudsters send out fake emails in mass hoping that just a few individuals open and click on the links inside. They assume that most people have purchased something online and may be waiting on communications from the seller. Instead, go directly to the website or app for the merchant you are expecting products from and check your account for communications and delivery status there.
- ***Avoid making purchases from social media, especially if the deal seems too good to be true.*** These ads can lead to those fake websites that were discussed in the "Fake Shopping Sites" article.
- ***If you are making a purchase from Craigslist, eBay, or Facebook Marketplace, use caution!*** Never send payment in the form of a gift card. No reputable merchant will demand you pay with store, Apple, or Visa Gift cards. If you must meet in person, pay in cash when you receive the product, and bring a second person with you, just in case.
- ***If donating this holiday season use extra caution when choosing your charity.*** Visit the secure website directly to be sure the charity is legitimate. Do not donate using any pop-

up ads, or social media ads. Fraudsters exploit the goodwill of the holiday season by creating fake organizations, with names or logos very similar to ones that are real.

- ***Plan to have someone home when your packages arrive.*** Porch Pirates follow delivery vehicles and steal products from your front door.

If you believe that you have been a victim of a holiday online shopping scam, close down the payment device used *immediately*. Safeguard your accounts by changing passwords and doing virus and malware scans. You should also file a complaint with the FBI's **Internet Crime Complaint Center** and dispute any transactions that may be involved in the scam. Consider placing a freeze on your credit or placing alerts in services like Credit Karma, which notify you when your credit is run.