‘Tis the Season… For Fraud

Keeping an eye on your online shopping cart? Well, fraudsters are too. The holidays typically introduce fraud involving e-skimming, fake charities, porch pirates, false shipping notifications & payment fraud, and other scams. Between parties, gift giving, and travel – you can easily get distracted and let your guard down. Be sure to educate yourself on the latest scams and trends.

Details

Black Friday, Cyber Monday and last minute holiday shopping oh my! This time of the year typically brings frequent online and in-store purchases. Whether its through a mobile app, on a website, or in-person, remind yourself to be aware and diligent about who you are purchasing goods and services from.

Some of the latest scams include:

- **E-skimming**: Scammers exploit weak links on an e-commerce platform. In many cases, you can be re-directed to a malicious domain where the skimming code can capture your information from the checkout page. The skimming code would capture your information in real-time and send it to a remote server where the data is collected by the criminals behind the scene. Your credit card data would either be sold or used to make fraudulent purchases from that point going forward.

• **Social media scams**: A newer version of online shopping scams involves the use of social media platforms to set up fake, online stores. By using social media to advertise the fake website; they'll take your payment, but you will never see the goods.

• **Porch pirates**: Year-round, but especially near the holidays, criminals steal packages from the doorstep/porch of unsuspecting homes, apartments, businesses, etc.

• **Shipment update scams**: Fraudsters send a fake email notifying you of a delivery failure or the request for updated shipping information. The email may look like it's coming from the original sender, but it contains a link with malware.

• **Donation and fake charities**: People love giving back this time of year and scammers know this. Similar to online scams, donation scams often try to replicate a charity website convincing you to donate money – which goes right to the criminal.

Risk Reduction Tips

Member Tips

• Sign up for transaction alerts to monitor for unauthorized transactions.

• Pay attention to emails, links, and websites. Think before you click!

• Avoid entering card information on web forms (could be malware installed); instead, use your stored payment information when possible such as Amazon pay or PayPal.

• Ensure home computers, laptops, and mobile devices are protected with antivirus, anti-spyware, and a firewall.

• Use well-known websites for online purchasing.

• Go directly to the website rather than through social media website advertisements.

• Be cautious for skimming or shimming devices when using ATMs or gas pumps. For gas pumps, try to use the pump closest to the entrance door as they are less likely to be a target for skimmers.

• Review and monitor your accounts daily and report any discrepancies immediately.