Holiday Scams

As you are putting together lists of gifts and purchases for the upcoming holidays, it can be easy to let your guard down. Here are some of the latest fraud and scams targeting shoppers during this holiday season.

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

Social Media Scams: Online shopping scams often involve the use of social media platforms to set up fake, online stores. By using social media to advertise the fake website; fraudsters take the member's payment, but your member will never see the goods.

Porch Pirates: Especially near the holidays, criminals steal packages from the doorstep / porch of unsuspecting homes, apartments, businesses, etc.

Buy Online / Curbside Pick-up: One of the newest avenues for 'friendly-fraud', where a member may state they didn't receive an item and want a refund. Curbside pick-up is also another option for fraudsters to intercept your purchase.

Shipment Update Scams: Fraudsters send a fake email notifying you of a delivery failure or the request for updated shipping information. The email looks 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. Donation scams often try to replicate a charity website convincing you to donate money – which goes right to the criminal.

Gift Card Scams: Purchase gift cards only from trusted sources.

Member Tips:

- Sign up for transaction alerts to monitor for unauthorized transactions.
- Pay attention to emails, links, and websites. Think before you click!
- Don't open attachments with special offers. It's a classic scam. The offer should be in the email and you should be able to see it right away.
- Avoid entering card information on web forms (could be malware installed). 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.