Holiday Shopping Scam Awareness

The Holiday Shopping season is here. Scammers are ready, are you? Black Friday and Cyber Monday sales offer huge bargains, but thieves also come out of the woodwork to capitalize on shopping events like this. Before you dive in to all the deals this year, take some extra precautions to avoid getting duped and learn which scams to watch out for.

The Fake Order Scam
Scammers know it can be hard to keep track of all your online orders for the holidays and will send fake order confirmations via email or text. These seemingly legit confirmations often contain malware or phishing links that the scammers use to steal your identity. The best strategy is to track your orders directly from the seller's website or app.

The Phony Tracking Number Scam
Similar to the fake order scam, fraudsters send fake package tracking notifications as an email/ text attachment or link. Actual retailers will never send tracking numbers via an attachment. Scammers use these tactics to infect your device with malware or direct you to phishing sites. As always, visit the seller's site to get accurate tracking information for your order.

The Bogus Website Scam
Scammers are skilled at creating fake email addresses and URLs that resemble those of legitimate companies. These phishing emails often lead to scam sites that capture your login credentials and payment information. Avoid clicking on email links; it's safer to type the URL manually and search for deals.

The Hot Deal Scam
Scarcity is a prime tool for scammers. Criminals create fake websites offering popular items that are generally hard to find. These scams can result in you paying for a product you'll never receive and the scammer possessing your payment details. The Better Business Bureau provides useful reviews to help verify the legitimacy of a product or seller.

The Fake Charity Scam
During the holiday season, there's a surge in charitable donations, and scammers know this trend. They set up bogus charities and employ high-pressure tactics to get you to donate. Be wary of organizations that accept payment only through gift cards, wire transfers, or cryptocurrency. The U.S. Federal Trade Commission (FTC) offers resources to ensure your donations reach legitimate charities.

The False Discount Scam
In this scam, fraudsters lure victims with advertisements offering significant discounts on popular products. These advertisements usually contain a link redirecting you to a fraudulent website where your personal and financial information gets stolen. Always cross-check the offered prices with those on the manufacturer's or well-known retailer's websites. Also, check if the seller provides complete contact information. A lack of information or a recently registered website should raise a red flag.

The Social Media Gift Exchange Scam
During the holiday season, a gift exchange scam often resurfaces on social media. The concept is simple: you buy a gift worth a certain amount, typically$10, and supposedly receive several gifts in return. However, the only person who benefits is the scammer who initiated the scheme. This type of scam is not only deceptive but also illegal. If you encounter such a scheme on social media, report it immediately.

The Fraudulent Gift Card Scam
Scammers love gift cards! They use emails or text messages to trick you into thinking you've received a gift card from a friend or family member. These messages often contain links that, when clicked, install malware on your device or steal your personal information. Always verify the source before clicking on any links. And remember, if a deal sounds too good to be true, it probably is.

The Non-existent E-tailer Scam
Beware of new e-commerce sites offering popular items at massive discounts. Scammers often create fake e-commerce sites that vanish after collecting money from their victims. Always research the seller's reputation before making a purchase. If you can't find any reviews or feedback about the seller, it's better to avoid the risk.

The Smishing Scam
Smishing is a scam where fraudsters send text messages posing as reputable companies to trick individuals into revealing personal information. During the holiday season, these messages often link to a supposed deal or gift. However, the link usually leads to a fraudulent website designed to steal your data. Treat unsolicited text messages with caution, and never click on suspicious links.