UNITED STATES SECRET SERVICE

Tips for Avoiding Scams 2024 Holiday Season

The holiday season is one of the most profitable periods for cyber criminals. The United States Secret Service Global Investigative Operations Center and its field-based Cyber Fraud Task Forces have observed certain trends that scammers will enlist to perpetrate their crimes. The list below contains information about common threats that can help the public remain vigilant during the holiday season and beyond.

Buy Gift Cards for Gifts, Not for Payments

Gift cards are convenient for shoppers, but they are also a scammer's favorite way to steal your money. If someone contacts you and demands that you pay them with a gift card, for any reason, don't let them. Funds stolen from gift cards cannot be recovered.

Charity Scams

Scammers may use the recent hurricanes and the holiday season as opportunities to steal funds from donors. If someone contacts you to ask for a charitable donation, research the charity. Make sure your donation goes where you want it to, not into the hands of a scammer.

False Advertisements

Social media platforms generate personalized advertisements for each individual user. However, scammers often use these ads to create "lookalike stores" to sell counterfeit products or perpetuate other scams. If it is too good to be true, it may likely be a scam. For example, scammers target senior citizens with false ads for medicines and equipment that can be covered by Medicare. Don't click on online adds because they may be phishing scams. Verify the legitimacy of an online retailer by reading reviews about the seller.

Scam Delivery Messages

Online purchases come with package tracking notifications. But beware, scammers may send phishing texts or emails about a deal or problem with "your" package. These fraudulent messages may have misspellings and awkward grammar. Before clicking on these messages, check to make sure that the package tracking notification numbers match the information from your purchase.

Voucher Scams

Scammers may call individuals and purport to be conducting travel research for a chance to win a holiday travel package voucher. The scammers then notify the individual that they won the voucher and instruct them to pick it up at a specific location. The scammers then pressure the victim into purchasing a timeshare or paying fees to redeem the voucher. Do not provide any personal information or accept anything offered, especially in response to a phone call.

Tips for Avoiding Scams

- **Guard Your Personal Information:** Do not offer your personal information unless you have confirmed that a request is legitimate. Scammers engineer methods to entice you to share your personal and financial information.
- **Slow Down:** Scammers create a false sense of urgency to get you to act quickly. If you are asked to act quickly, or there is an emergency, it may be a scam.
- **Use Caution When Shopping Online:** Verify that the website you are using is legitimate and safe before you use your card to pay.
- **Use Strong Passwords:** Use different usernames and passwords for all financial accounts and online shopping portals. Choose passwords that are not easy to guess, most legitimate sites and apps require passwords that contain symbols, letters, and numbers.
- **Verify Before Donating:** Before making a charitable contribution, research the charity using these organizations: BBB Wise Giving Alliance, Candid, Charity Navigator, and Charity Watch. Donate directly to a verified charity rather than through someone that claims to be an intermediary. Be cautious of organizations with names that are similar to reputable charities.

What to Do If You Are a Victim

Report fraud schemes to your local law enforcement agency, the Federal Trade Commission at **https://reportfraud.ftc.gov**, and the Internet Crime Complaint Center at **https://www.ic3.gov/**. The United States Secret Service works closely with local and federal law enforcement agencies.