Illinois Is No. 6 At Most-Risk State: Study Projects Online Shopping Scams Will Surge This Holiday Season

November 17 2021 11:51 AM

A new study projects online shopping scams will surge this holiday season as consumers set to spend a record $207 billion online.

Fake websites, Instagram giveaways, and Secret Santa contents are the common scams consumer need to avoid right now.

SocialCatfish.com today released a study on Online Shopping Scams to Avoid This Holiday Season using data from the FTC and the FBI's IC3 through 2020.

Illinois is the No. 6 most at-risk state, having lost $150 million to fraudsters last year, when a record $4.2 billion was stolen nationally.

Online shopping has also been the No. 1 most common scam reported to the FTC in Illinois relating to the pandemic, which has led to the scam surge with more people operating online.

Here are 5 Online Shopping Scams to Avoid This Holiday Season:

1. **MISSING PACKAGE SCAM:** Capitalizing on inevitable supply chain delays, scammers pretend to be FedEx and send an email with a link to track your package. When clicked on, these malicious links steal your personal and financial information. They also may text, leave voicemails, or place a "missed delivery" tag on your front door.

How to Avoid: Never click a link or call back a number from an unexpected delivery notice. Always contact the company directly using a verified number or website.

2. **SOCIAL MEDIA SECRET SANTA:** A pyramid scheme called "Secret Sister" is circulating on Facebook. Scammers recruit "sisters" with the promise that if they buy a $10 gift for another member, they will receive 36 gifts in return. A version of this scam includes exchanging bottles of wine.

How to Avoid: Do not respond to communication from "Secret Sister" or do an exchange "for the good of the sisterhood."

3. **FAKE RETAILERS AND WEBSITES:** Look out for fake websites that advertise enormous sales on popular gift ideas that are out of stock everywhere else due to supply chain issues. Fake sites have a domain name with an extraneous letter or number, grammatical errors, and limited contact information.

How to Avoid: Research the company and read customer reviews before purchasing. Google their name with the word "scam" to see if anything comes up.

4. **HOLIDAY CHARITY GIFT SCAM:** In addition to traditional gifting, people may donate to charity on someone's behalf. This increased during COVID-19 and

ramps up every year during the season of giving. Scammers pose as a fake charity to solicit fraudulent donations. Often, they pick a name that sounds close to a well-known charity.

How to Avoid:Search the charity on a public database such as BBB Wise Giving Alliance and Charity Navigator.

5. **FAKE INSTAGRAM GIVEAWAYS:** Around the holidays, brands and influencers offer free product giveaways. Scammers are using a technique called "like-farming," where they ask you to like or comment on their post for a chance to win a holiday prize. They include malicious links and steal your personal information.

How to Avoid: Look for the blue checkmark which social media platforms use to verify a real page from copycats. Watch for typos and accounts with limited content.