HO, HO, HO, HOLIDAY SCAMS!

News Release from **FBI - Oregon**
Posted on FlashAlert: December 1st, 2021 12:59 PM

If you're doing online shopping this holiday season, be on the lookout for scammers trying to steal a deal, too!

During the 2020 holiday shopping season, the FBI Internet Crime Complaint Center (**IC3.gov**) received more than 17,000 complaints regarding the non-delivery of goods, resulting in losses of more than $53 million. The FBI anticipates this number could increase during the 2021 holiday season due to rumors of merchandise shortages and the ongoing pandemic.

"Oftentimes when we talk about cyber-crimes, we are referring to massive intrusions into financial institutions or ransomware attacks against large providers. Smaller cyber scams run by individuals or groups can be just as frustrating and difficult for families this time of year when all you want to do is provide the perfect gift for your family. The best thing you can do to be a savvy shopper is to know what scams are out there and take some basic precautions," says Kieran L. Ramsey, Special Agent in Charge of the FBI in Oregon.

Here's a look at some of the more common scams:

Online Shopping Scams:

Scammers often offer too-good-to-be-true deals via phishing e-mails, through social media posts, or through ads. Perhaps you were trying to buy tickets to the next big concert or sporting event and found just what you were looking for – at a good deal – in an online marketplace? Those tickets could end up being bogus.

Or, perhaps, you think you just scored a hard-to-find item like a new gaming system? Or a designer bag at an extremely low price? If you actually get a delivery, which is unlikely, the box may not contain the item you ordered in the condition you thought it would arrive.

In the meantime, if you clicked on a link to access the deal, you likely gave the fraudster access to download malware onto your device, and you gave him personal financial information and debit/credit card details.

Social Media Shopping Scams:

Consumers should beware of posts on social media sites that appear to offer special deals, vouchers, or gift cards. Some may appear as holiday promotions or contests. Others may appear to be from known friends who have shared the link. Often, these

scams lead consumers to participate in an online survey that is designed to steal personal information.

If you click an ad through a social media platform, do your due diligence to check the legitimacy of the website before providing credit card or personal information.

Gift Card Scams:

Gift cards are popular and a great time saver, but you need to watch for sellers who say they can get you cards below-market value. Also, be wary of buying any card in a store if it looks like the security PIN on the back has been uncovered and recovered. Your best bet is to buy digital gift cards directly from the merchant online.

Another twist on this scam involves a person who receives a request to purchase gift cards in bulk. Here's how it works: the victim receives a spoofed e-mail, a phone call, or a text from a person who they believe is in authority (such as an executive at the company). The fraudster tells the victim to purchase multiple gift cards as gifts. The victim does so and then pass the card numbers and PINs to the "executive" who cashes out the value.

Charity Scams:

Charity fraud rises during the holiday season when people want to make end-of-year tax deductible gifts or just wish to contribute to a good cause. These seasonal scams can be more difficult to stop because of their widespread reach, limited duration and, when done online, minimal oversight.

Bad actors target victims through cold calls, email campaigns, crowdfunding platforms, or fake social media accounts and websites. Fraudsters make it easy for victims to give money and to feel like they're making a difference. The scammer will divert some or all the funds for personal use, and those most in need will never see the donations.

Tips to Avoid Being Victimized:

- Pay for items using a credit card dedicated for online purchases, checking the card statement frequently, and never saving payment information in online accounts.
- Never make purchases using public Wi-Fi.
- Beware of vendors that require payment with a gift card, wire transfer, cash, or cryptocurrency.
- Research the seller to ensure legitimacy. Check reviews and do online searches for the name of the vendor and the words "scam" or "fraud."
- Check the contact details listed on the website to ensure the vendor is real and reachable by phone or email.
- Confirm return and refund policies.

- Be wary of online retailers who use a free email service instead of a company email address.
- Don’t judge a company by its website. Flashy websites can be set up and taken down quickly.
- Do not click on links or provide personal or financial information to an unsolicited email or social media post.
- Secure credit card accounts, even rewards accounts, with strong passwords or passphrases. Change passwords or passphrases regularly.
- Make charitable contributions directly, rather than through an intermediary, and pay via credit card or check. Avoid cash donations, if possible.
- Only purchase gift cards directly from a trusted merchant.
- Make sure anti-virus/malware software is up to date and block pop-up windows.

What to Do if You Are a Victim:

If you are a victim of an online scam, the FBI recommends taking the following actions:

- Report the activity to the Internet Crime Complaint Center at **IC3.gov**, regardless of dollar loss. Provide all relevant information in the complaint.
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.

For additional information and consumer alerts, and to report scams to the FBI, visit **IC3.gov**.