OFFICE OF THE SHERIFF
Sheriff Curtis L. Landers
225 W. Olive Street
Newport, Oregon 97365
(541) 265-4277
Fax (541) 265-4926

TIP OF THE WEEK

Date: 12/2/21 **FOR IMMEDIATE RELEASE**

Contact: Sheriff Curtis Landers
541-265-0654
lcsheriff@co.lincoln.or.us

HOLIDAY SHOPPING SCAMS!

Doing your shopping online? Always be extra cautious before entering any information, but especially around this time of year. We are re-posting this very educational information published by the FBI-Oregon:

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.

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 them 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.

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**.

For more information and tips, visit our web site at www.lincolncountysheriff.net and Like us on Facebook at Lincoln County Sheriff's Office – Oregon.