NH CONSUMER INSIGHT

December 2024

PHONE: (603) 271-3641

EMAIL: DOJ-CPB@doj.nh.gov

FILE COMPLAINTS ONLINE HERE: https://www.doj.nh.gov/consumer/complaints/index.htm

HOLIDAY SHOPPING: MAKE SURE SCAMMERS ONLY GET COAL IN THEIR STOCKINGS THIS YEAR

As we enter the busy holiday season, it is important to remain vigilant of potential scams. It is an extremely busy time but taking a few extra minutes to carefully review transactions or make plans for holiday packages, can save you from becoming a victim of a predatory scam. The following tips are intended to assist consumers in identifying common risks during the holiday shopping season and how consumers can best protect themselves from being victimized by scammers.

If you have questions or concerns about a holiday scam or purchase, call the Consumer Protection Hotline for help at (603) 271-3641 or email DOJ-CPB@doj.nh.gov.
You may also file a Consumer Complaint with the Consumer Protection and Antitrust Bureau by following the instructions here: https://www.doj.nh.gov/consumer/complaints/index.htm.

HOLIDAY SHOPPING SCAMS

It's no secret that shopping ramps up during the holidays, but scams do too. Be careful about how and where you share information and beware of fraudulent retailers and organizations.

Here are some holiday shopping scams to be aware of:

- **Fake shopping websites.** Some websites are intentionally created to mimic trusted retailers, with familiar logos and a URL that's easily mistaken for the real thing. A simple slip of the keyboard takes you to a scammer's website instead of the shop you intended to visit.
- **Knockoff products.** Some copycats do deliver merchandise — shoddy knockoffs worth less than even the "discount" price advertised as a once-in-a-lifetime deal on some famous designer item. Often, you won't receive a product at all.

- **Card declined scams.** This is a new scam criminals have cooked up. You order something, put in your card information and you're told that your card has been declined. If you put in information from another card to pay for the purchase, you'll find that both cards have been charged.

Here are some ways you can protect yourself:

- **Protect your personal info.** It's easy to hit the "Buy" button from anywhere when you're on your phone or on your laptop. But be sure you're not sharing personal or credit card information over public Wi-Fi. Wait until you're on a secure network to make a purchase.
- **There may appear to be deals galore over the holidays,** and many of them are on social media – but not all of them are legitimate. Carefully read reviews, look for security credentials on websites, and research unfamiliar retailers before you take advantage of a discount. If an online deal seems too good to be true, be suspicious and eliminate the possibility that the merchant is a scammer before committing to a purchase.
- **Try to pay by credit card and keep receipts** so you can try to get refunds if there's an issue. There are often better fraud protections with credit cards compared to debit cards.
- **Keep an eye out for common scams** in your area with the BBB **Scam Tracker**.
- **For examples of additional scams that target senior citizens,** visit the **AARP Fraud Watch Network**.

GIFT CARD SCAMS

Gift cards are a quick and popular item to purchase during the holiday season. As a result, scammers are busy trying to get access to those funds. There are two prominent gift card scams you should be aware of this holiday season. First, scammers will try to contact you to buy gift cards for them to pay off some debt or loan. It often starts with a call, text, email, or social media message. Scammers will say almost anything to get you to buy gift cards for retailers like Google Play, Apple, or Amazon. Once you purchase the cards, scammers will try to get you to provide the card number and PIN codes so they can utilize those funds. Here are some common tactics scammers use in this type of gift card scams:

1. Scammers will say it's urgent. They will create the impression that unless you pay them right away or something terrible will happen. They don't want you to have time to think about what they're saying or talk to someone you trust. Slow down. Don't pay. It's a scam.

2. Scammers will tell you which gift card to buy (and where). They might say to put money on an eBay, Google Play, Target, or Apple gift card. They might send you to a specific store — often Walmart, Target, CVS, or Walgreens. Sometimes they'll tell you to buy cards at several stores, so cashiers won't get suspicious. The scammer

also might stay on the phone with you while you go to the store and load money onto the card. If this happens to you, hang up. It's a scam.

3. Scammers will ask you for the gift card number and PIN. The card number and PIN on the back of the card let the scammer access the money you loaded onto the card — even if you still have possession of the physical card. Slow down. Don't give them those numbers or send them a photo of the card. It's a scam.

If you bought a gift card and gave someone the numbers, that's a scam. Use your gift card and store receipt for these next steps to try to prevent your funds from being stolen:

- Report the scam to the gift card company right away. No matter how long ago the scam happened, report it.
- Ask for your money back. Some companies are helping stop gift card scams and might give your money back. It is always worth asking.

The second type of gift card scam involves someone stealing the value of the gift card before you are able to use it. Scammers can either steal the value from cards sitting in unattended store racks or use malicious software to find and drain the value you've loaded on a card. In order to protect yourself, try to avoid buying a gift card off a rack and buy directly from a store counter. This will help ensure the gift card is protected and has not been tampered with.

HOLIDAY MAIL SCAMS

As we buy and mail gifts over the holidays, the high volume of mail and packages provides many avenues for scammers. Holiday deliveries can be easy targets for thieves and con artists.

- **When you're expecting a lot of packages over the holidays,** shippers will often provide updates on the status of orders. Knowing this, scammers will send phishing emails and texts pretending to be from companies like FedEx and UPS to lure you to phony webpages and get us to share personal information. Look closely at delivery notifications, texts, and email updates before you click on links or input information. And remember, UPS and FedEx won't ask for personal information via email.
- **All of those packages stacking up outside your door can be tempting for thieves.** Porch poachers might steal packages from your doorstep. Consider tracking your package so you'll know when they have arrived. You can also set up a different delivery address with a neighbor who is home during the day. Try to be aware of when packages may be delivered to make sure they won't sit unattended for too long. If there is an alternative and less visible spot for your packages, try notifying the delivery drivers to reduce the temptation for those pesky porch poachers.

- **If you're traveling for the holidays,** consider having your mail held for you at the post office. Allowing holiday cards to build up in your mailbox creates a considerable risk of theft. By making arrangements to collect all cards and letters once when you return, you can give yourself peace of mind that all of your holiday mail will be safe and waiting for you.

HOLIDAY CHARITABLE GIVING

The holiday season is often a time when individuals choose to make financial donations to charitable non-profits. Similarly, charities use this time of year to reach out directly to citizens for monetary donations as part of end-of-year campaigns. The New Hampshire Charitable Trusts Unit (CTU) offers the following tips to consider when making a financial contribution to a charitable organization:

- **Protect yourself from giving money to fake charities.** Fraudulent charities may impersonate well known charities by asking for donations on the charity's behalf but keeping the money for themselves or by establishing a professional looking website for a non-existent charity. Charities, both in-state and out-of-state, must register and file annual reports with CTU. Citizens can confirm if a charity is registered and in good standing on CTU's website: https://mm.nh.gov/files/uploads/doj/remote-docs/registered-charities.pdf.
- **Know if your donation will be tax-deductible.** If you would like to deduct your charitable donation on your federal taxes, you should confirm that you are donating to an organization designated by the Internal Revenue Service to accept tax-deductible donations. The IRS has an online tool to confirm the charity is a qualifying organization: Search for tax exempt organizations | Internal Revenue Service. Be sure to ask for letter from the charity confirming the amount of your tax-deductible donation for tax filing purposes.
- **Ask how much of your donation will go to the charity.** If a charity uses a paid solicitor to help it fundraise, both the charity and solicitor must file documentation with CTU stating how much of the proceeds the charity actually receives. Before making a donation, you can ask how much the charity will receive, and they should be able to tell you.

If you have questions or concerns related to a charity's status, please contact the New Hampshire Department of Justice Charitable Trusts Unit at (603) 271-3591 or charitabletrustsunit@doj.nh.gov. CTU has a number of resources available to the public related to charitable giving at: Donors/Public | New Hampshire Department of Justice