Champlain National Bank

Holiday Season Scams

Cybercrime intensifies during the holiday season so awareness and caution are key to keeping your information safe. The following examples are scams from last year that are already beginning this year.

Black Friday Deals: Fraudsters take advantage of Black Friday and Cyber Monday, which are the busiest online shopping days of the year. Watch out for the too-good-to-be-true coupons, especially those that offer free electronics like iPads and iPhones.

Postal Deliveries: Be wary of emails announcing you have received a package from FedEx, UPS or the USPS that ask for your personal information. Do not automatically provide it: think before you click!

Refunds: Most refund scams seem to be from Amazon, a hotel, or a retail chain store. The email claims there was an error with a transaction and directs you to "click for a refund". Clicking installs malware on your device.

Grinch eCard Greeting: You receive an email with an attachment that looks like an eCard. Opening the attachment may result in infecting your device.

Fake Gift Card Enticement: Cyber thieves promote a fake gift card on social media, which is simply a way to get your information. They in turn sell your information to other cyber criminals who use it for identity theft. As an example, a recent Facebook post offered a free $1,000 Best Buy Gift Card to the first 20,000 people who signed up for a Best Buy fan page, which ended up being a scam.

Copied Websites: Fraudsters build copies of well-known retail websites and then send you an email promoting great deals from this retailer. These websites only exist for a few days and the money they collect, which can be substantial, usually goes abroad. Once you discover you've been had, your credit card company will usually refund your money, but you will still need to get a new debit or credit card as your number will now be compromised.

Charity Tricksters: The holidays are traditionally a time for giving. Fraudsters are well aware of this, and use copy-cat websites to defer your well-intentioned gift from the intended recipient to a fraudulent website. Be wary of any site that asks you for a contribution by taking steps to ensure it is legitimate.

Twitter Scam: If you tweet about a gift you are trying to find and you get a message from another tweeter offering to sell you one, stop and think before you act. There are many sophisticated scams that use Twitter. If you do not know the person sending you a message, proceed with caution and never pay up front!

Search Term Traps: Fraudsters find out what items are in high demand each year for the holidays, and build websites that claim to have the desired items. They then work to get their website well ranked on search engine results, so that people will be more apt to click on a link to their website. Many times, these sites contain malware that infects your device. Make sure your web-browser is always updated with the latest anti-virus software and will warn you if the site is unsafe.

Evil Wi-Fi Twins: Cyber criminals put out Wi-Fi signals in public places such as coffee shops and shopping malls as a way to steal your credit card number. If you use a fraudulent Wi-Fi while using your credit card, the hacker now sits in the middle of your transaction and steals your credit card data while you shop online. Think twice before shopping online using a Wi-Fi connection in a public place.

Free Star Wars Movie Tickets: There are currently phishing attacks trying to trick people into winning movie tickets to the new Star Wars movie. The hook is that someone must click on "take the survey" or "watch the official trailer" in order to win two tickets for opening night. When you click on the link, you could be downloading malware or a virus on your computer or device.

EMV Chip Card Scam: The Federal Trade Commission (FTC) is warning consumers of a new scam related to the US conversion to EMV chip cards designed to make credit card use more secure. Many card issuers have issued, or are in the process of issuing new credit and debit cards to their clients. The new cards use EMV chip technology to reduce the chances of fraudsters stealing card information to create counterfeit cards. The FTC has warned that scammers are emailing people, posting as a card issuer who needs their personal information in order to send out a new EMV chip card. They ask people to provide personal information or to click on a link in order to continue the process**.** Don't respond to this type of email and don't click on any links in this sort of email. There is no reason a card issuer would contact you by email, or by phone to confirm personal information before sending you a card with a chip.