Shopping Online Securely

The holiday season is nearing. Many of us will be looking to buy the perfect gifts and shop online. Unfortunately, cyber criminals will be active as well, creating fake shopping websites and other online shopping scams to steal your information or money.

Holiday Scams

Fake Online Stores

Criminals create fake online stores that mimic the look of real sites or use the names of well-known stores or brands.

When you search for the best online deals, you may find yourself at one of these fake sites. By purchasing from such websites, you can end up with counterfeit or stolen items, or your purchases might never be delivered.

Scammers on Legitimate Websites

Large online stores often offer products sold by different individuals or companies that might have fraudulent intentions.

Everybody loves a great deal. But shocking offers, unbelievable discounts and unreal rates may signal that the offer isn't quite what it seems.

Advertisements

Fraudsters recognize that consumers spend a lot of time on social media and will post ads for free trials, or discounted merchandise.

They may also use the names and photos of well-known individuals or companies to fake endorsements of their products.

Text Messages

Cyber attackers use SMS/text messages to try to trick you into taking action you should not take.

For example, gift card scams can work this way. A cyber attacker will send you an urgent email pretending to be a friend, then ask for your cell phone number. Then they can send repeated text messages, pressuring you to purchase gift cards. Once purchased, the attackers have you scratch off the code on the back of the cards and message a picture of the codes back to them.

Phishing

When attackers create an email that attempts to trick you into taking an action, such as opening an infected email attachment, clicking on a malicious link, or giving up sensitive information.

For example, you are notified your package was delayed, even though you never ordered a package.

Vishing

Scammers may call you impersonating a financial institution.

For example, an automated voicemail informs you that your credit card has been cancelled, and you must call a number back to reactivate it.

Fraud Prevention Tips

Use a Secure Site

- Avoid making purchases and banking transactions unless you are certain that you are on a secure site/connection (i.e., https://)
- Be suspicious if a website domain name is different. For example, you may be used to shopping at Amazon, whose website address is www.amazon.com, but end up at a fake website that looks similar but has the website address www.aamazon.com.
- Regularly update your browser, and other software to increase your resistance to common malware, phishing, and other common attacks.
- Avoid online shopping when connected to unsecured Wi-Fi connections (like at an airport or coffee shop).
- If you think you've entered your password on a fraudulent site, go to the authentic site and change your password immediately.

Secure Your Account

- Protect your online accounts by using a unique, strong password for each of your accounts.
- Add an extra layer of security to protect your sensitive online accounts. The adoption of 2FA (also known as multifactor authentication) is a tool that makes stealing your credentials significantly more difficult than just using a password alone.
- Be cautious of any link or attachment provided in an e-mail.
- If you believe a phone call is an attack, simply hang up. Never trust Caller ID. Bad guys will often spoof the caller number so it looks like it is coming from a legitimate organization.

Third Party Service Providers

- If you receive a suspicious or fraudulent correspondence claiming to be from Amazon or another service provider, report it immediately.
- Be sure that you understand the seller's warranty and return policies before you make your purchase.
- If you believe you have been scammed on an online ad/marketplace site, be sure to report the seller/post.
- Be suspicious of ads or promotions on search engines or social media that are significantly lower than those you see at the established online stores. If a deal sounds too good to be true, it may be a scam.

Monitor Your Transactions

- Regularly review your credit card statements to identify suspicious charges. If you find any suspicious activity, call your credit card company right away and report it.
- Sign up for alerts. Make sure your bank accounts are configured to alert you whenever a transaction is made, especially for large purchases or money transfers.
- If you entered your payment information on a website or replied to a potentially fraudulent email, contact your financial institution immediately.

If You Become a Victim - Notify

- Inform the local police
- Canadian Anti-Fraud Centre 1-888-495-8501
- Crime Stoppers at 1-800-222-TIPS
- The Competition Bureau at 1-800-348-5358
- Contact your credit reporting agencies TransUnion and Equifax.