Communications Security Establishment | Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

HOW TO SHOP ONLINE SAFELY

DECEMBER 2020

ITSAP.00.071

Online shopping is convenient; you can purchase items through your mobile device and get next-day delivery to your front door. However, you should be aware of the threats associated with online shopping. These threats pose many risks to not only your personal information, but your organization's assets (e.g. email address, shipping address, phone number, credit card). Whether shopping online for personal reasons or using your organization's accounts to make company purchases, protective practices for shopping online will help you and your organization keep sensitive information and assets private. This document covers the different ways you can keep your organization and yourself safe while shopping online.

WHAT ARE THE POSSIBLE THREATS?

Online shopping puts you and your organization at risk for identity theft, hacking, and financial loss. Some ways in which threat actors can steal sensitive information and hack accounts include the following examples:

- Fake e-commerce sites that collect your information after you've followed through with a fake purchase
- Fraudulent payment processing sites (i.e. third-party financial arrangement) that collect your money for fake transactions
- Websites that are not encrypted, leaving your information open to anyone
- Websites that are not secure and don't have reputable sellers (e.g. individual sellers or private citizens)

> As stores and retailers increase their online presence, threat actors are finding more ways to steal information and commit fraud.

WHAT ARE THE WARNING SIGNS?

You should look out for the following warning signs when deciding whether a website is trustworthy or not:

- The site looks poorly designed and unprofessional.
- The links and the back button are broken or disabled.
- The website displays no contact information (e.g. phone number, email, address).
- The return policies or privacy policies are either unclear or not stated.
- Your credit card credentials are being requested for reasons other than your purchase.
- The item prices are incredibly low (i.e. unbelievable deals).
- The shipping, duties, and extra charges seem abnormal.

HOW CAN I PROTECT MYSELF?

There are ways that you can protect yourself and your organization when you are shopping online, such as the following practices:

RESEARCH THE RETAILER

- Read the website's privacy policies, return policies, and other information.

BROWSE SAFELY

- Use websites that start with HTTPS, as they use encryption policies to protect your information.
- Use websites that display a green lock (i.e. encrypts website traffic) in the address bar.
- Be cautious when browsing on your mobile phone because URLs are shortened (i.e. tricking you into visiting malicious websites).

PROTECT YOUR ACCOUNTS

- Create a unique and strong passphrase for online accounts.
- Use two-factor authentication..
- Check your credit card statements frequently.
- Use a safe form of payment (e.g. credit cards) from major financial institutions that guarantee reimbursement for fraudulent transactions.
- Use a virtual credit card number or a separate card with a low spending limit if you are unfamiliar with the website (i.e. banks offer temporary cards with set amounts to limit the damage that can take place on your real card).

TAKE ADDITIONAL PRECAUTIONS

- Limit the amount of personal information you use on the website (e.g. do not give your social insurance number).
- Back up, update, and patch devices.
- Use a secure Wi-Fi network (i.e. with a strong passphrase).
- Watch out for email scams (e.g. do not click links in emails for special deals).

Implementing these practices can help protect you when shopping online.

While they may reduce your risks, they do not erase them completely.

WHAT DO I DO IF I'VE BEEN SCAMMED?

Cyber threats can be difficult to spot. You may not even know that you've been tricked until it is too late. If you are the victim of a scam or a potential compromise, you should take the following actions to report and mitigate the incident:

1. Report the incident to your security department, technical support, or senior management.
2. Contact your credit card company.
3. Reset your account credentials for related accounts, such as your email or social media accounts.
4. Report the incident to the Canadian Anti-Fraud Centre at 1-888-495-8501 or online at **antifraudcentre.ca**

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**