Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

How to shop online safely

November 2023

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, like email and shipping addresses, phone numbers, and credit card numbers. Whether shopping for personal reasons or 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 yourself and your organization 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, such as a 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, like individual sellers or private citizens

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 deactivated
- The website displays no contact information
- 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 or there are deals that seem too good to be true
- The shipping, duties, and extra charges seem abnormal

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

AWARENESS SERIES

Cat. No. D97-1/00-071-2023E-PDF
ISBN 978-0-660-68380-5

How can I protect myself?

Here are ways that you can protect yourself and your organization when you are shopping online.

Implementing these practices can help protect you when shopping online.

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

Research the retailer

- Read the website's privacy policies, return policies, and other information.
- When shopping on a social network site, like Facebook or Instagram, investigate the individual or vendor to see if they are verified by the platform and read reviews from other buyers.

Browse safely

- Use websites that start with HTTPS, as they use encryption policies to protect your information
- Use websites that display a green lock in the address bar as the site encrypts website traffic. An open or missing padlock means the website's data is not secure.
- Be cautious when browsing on your mobile phone because they display shortened URLs. This can trick you into visiting malicious websites.

Protect your accounts

- Create a unique and strong passphrase for each online account and avoid using the same one for multiple accounts.
- Use multi-factor authentication (MFA).
- Check your credit card statements frequently.
- Use a safe form of payment, such as 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're unfamiliar with the website. 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. For example, do not give your social insurance number.
- Check out as a guest to avoid the website saving your information. If creating an account and saving payment details, use multi-factor authentication and a passphrase to protect your information.
- Back up, update, and patch devices frequently.
- Use a secure Wi-Fi network with a strong passphrase. Use cellular data or log into a virtual private network if you are using a public network.
- Watch out for email scams. Avoid clicking links in emails for special deals.

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 online to the Canadian Anti-Fraud Centre or call 1-888-495-8501.

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**