# Online Shopping Safety Tips

Every day, Canadians go online to research about products and make purchases from online merchants located in all parts of the world. The Internet allows consumers to comparison shop for the best deals and locate products that might otherwise be difficult to find in their neighbourhood.

The level of convenience provided by online shopping, also provides cybercriminals with opportunities to steal your money and personal information. Although there are legitimate concerns when it comes to shopping online, there are also steps to be taken to protect yourself.

## Before Purchasing

- **Comparison shop** - Use comparison sites or a search engine to look for the best deals. Be wary of deals that sound too good to be true. If an online merchant's prices seem unusually low compared to others, look for signs this could be on a fraudulent site. Are there any typos on the site? Does the company ask for unnecessary information such as your Social Insurance Number or date of birth?
- **Do background checks on the e-merchant** - Make sure the online merchant has a physical address and phone number listed. If suspicious about the site, call the company's phone number to see if a representative is available. Look for information like as how long the company has been in business, customer service policies, and whether they offer warranties, repairs, or returns.
- **Read customer reviews** - If there are multiple complaints about the company, proceed with caution.
- **Understand shipping policies** - Look into shipping and handling fees, including duty and brokerage fees, to ensure they seem reasonable. Understand the various shipping options and how they will affect the total cost of your purchase. Be aware of the time it will take for delivery and the merchant's shipping policy. If you are buying from a foreign merchant, ensure they ship internationally.
- **Understand return and exchange policies** - Shopping online does not allow the consumer to physically see, touch or try on the merchandise. It is important to check out the merchant's return and exchange policies. Is there a time limit or other restrictions on returns? Are there restocking charges for items returned. Will the merchant provide a full refund the charges or a store credit? If the merchant only offers store credits, are there any time restrictions on using the credit?
- **Review the company's privacy policy** - Review how the merchant uses personal information gathered. Check to make sure that it will not be shared with third parties. Many online check-out pages will indicate fields that are required to complete the transaction - consumers should only disclose information necessary to complete the purchase. Information such as Social Insurance Number or date of birth should not be disclosed.

## When Making Purchases

- **Never click on links from spam emails** - It can be dangerous to purchase from sites attached to a link in an email from someone you do not know. Do not click on pop-up ads, as they may redirect you to a malicious site.
- **Check the web address to make sure the site is legitimate** - Little things such as misspellings, requests for excessive personal information, and low-resolution logos and photos may be warning signs the site is a fake.
- **Check that the site is secure** - Look for a security features on the site, such as a lock symbol on the page or web addresses that start with http**s**://
- **Use a payment method with buyer protections** - In many cases, credit card companies limit one's liability for online purchases in cases of fraud. Some credit card companies even offer extended warranties on purchases. Online payment systems, such as PayPal, do not share full credit card numbers with sellers in order to give consumers extra protections. Do not send cash or allow an online merchant to access your bank account.
- **Do not use a public computer to shop online** - Computers save or "cache" information to speed up one's Internet experience. If using a public computer, information such as browsing history and login information may be accessible to strangers who subsequently use the computer.
- **Only use a secure connection** - Unsecured wireless networks can allow hackers to access payment and personal information as the network is not protected

## After the Purchase

- **Keep a paper trail** - Keep a copy of the order number and receipt, and note which credit card was used for the purchase. Review the credit card statement, to make sure the charge placed on the card is correct and there are no extra fees or charges.
- **Inspect the purchase upon receipt** - Make sure that the product received is correct and is not damaged. If a return or exchange is needed, do it quickly so not to exceed any return restrictions.