CANADIAN ANTI-FRAUD CENTRE BULLETIN

Check Twice, Pay Once: Starting New Habits to Avoid Merchandise Fraud

2025-10-20

FRAUD: RECOGNIZE, REJECT, REPORT

October is Cyber Security Awareness Month, and this year's theme is ***Get Cyber Safe – for future you***. Cyber threats are constantly evolving, and so are tactics fraudsters use to exploit Canadians. The Canadian Anti- Fraud Centre (CAFC) would like to remind Canadians that cyber security isn't only about protecting your devices; it's also about protecting yourself from fraud. By learning how criminals operate and taking simple steps today, you can build strong cyber habits that will safeguard your money, your identity, and your future.

Fraudsters are constantly looking for ways to take advantage of our everyday spending habits, specifically when it comes to online shopping. In today's fast-paced world, it`s easy to click "buy now" without double-checking the source. Taking a few extra seconds to pause and verify can save you from losing money and personal information.

How the fraud works

Criminals use a variety of tactics to trick Canadians into sending money for merchandise that doesn't exist:

Marketplace Frauds: Fraudsters often exploit online marketplaces and classified ad sites to trick Canadians out of money or their items. These frauds can take several forms:

- Overpayment Frauds: A fraudster poses as a buyer and sends a payment that exceeds the agreed price. They then ask the seller to refund the difference. Later, the original payment bounces or is reversed, leaving the seller without the product and the refunded money.

- Fake Payment Confirmation: Criminals may send fake payment notifications via email or text message to convince sellers that funds were sent when no money was actually transferred.

- Non-delivery frauds: Fraudsters pose as sellers, collect payment for an item, but never ship the product.

Deceptive Marketing Practices: Websites and advertising of counterfeit goods are often made to mimic legitimate sites and will use tactics such as "Today Only" or "Limited Time Offer" to justify the drastic discounts. Traffic to these websites is generated by paid advertisements often displayed on various sites – including social media (Facebook, Instagram et al). Beware, counterfeit products are typically poor in quality and can pose serious health and safety risks. To reduce the risk, the CAFC advises Canadians to destroy the product or return it to the seller.

Warning signs

- Be cautious of blowout sales or greatly reduced prices (e.g. 80%).
- Notice text with spelling errors or references to the product as “the item”.
- Beware of overseas buyers who want to buy without seeing the product first.
- Beware of overpayments for items you are selling.
- Sellers with social media profiles which have been recently created.

How to protect yourself

- Know the market value of the product you are looking for.
- Locate and verify the sellers contact information (address, phone number, email) before you buy.
- Look for customer reviews and ratings from third-party sources.
- Use a payment method with fraud protection (e.g. pay by credit card)
- Whenever possible, pick-up items and provide the payment in person.
- Review all email information to make sure they are coming from a legitimate source.
- Visit the CAFC websites to learn more about buying or selling goods and services online.

Remember! Small, consistent steps create lasting protection. Just like locking your front door becomes second nature, taking a moment to research the buyer or seller should become part of your digital routine.

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the Canadian Anti-Fraud Centre’s online reporting system or by phone at 1-888-495-8501. If not a victim, you should still report the incident to the CAFC.