

Internet Scams

Internet scams come in many forms of deception and trickery, looking to take advantage of people when they, or situations around them, are vulnerable. Internet fraudsters may make websites and products appear legitimate, advertise knockoff products or products they do not intend to deliver, along with advertising jobs that may not exist, all in an attempt to get your money. You can protect yourself from fraudsters by educating yourself, recognizing warning signs and rejecting and reporting suspicious activities to the RCMP and the Canadian Anti-Fraud Centre.

Common Internet Scams:

Internet scams can take a variety of forms designed to separate you from your money or personal information or let the fraudster access your computer. Here are three examples that you might see during the pandemic:

<u>Fake websites</u> – Fraudsters make their websites and products appear authentic by stealing company logos, trademarks and product images from legitimate sources. Fake websites may offer luxury or other items at much cheaper prices and will not deliver the products you paid for. Fake websites may also try to collect your personal identity and payment card information.

<u>Fake advertisements</u> – Fraudsters offer items that may take advantage of heightened demand, which currently may include facemasks, hand sanitizer and cleaning supplies. Fraudsters will keep your money without delivering items. Do your research when purchasing online from unknown suppliers or look elsewhere.

<u>Mystery shopper</u> – A fake job offer that has you pay a fee to be secret shopper, deposit a cheque and transfer its funds to another bank account or attend a store and buy things with a gift card. The cheque or gift cards provided may be fake. These ads can be online or by mail and may include legitimate looking surveys to convince you the job is real.

Protect Yourself from Internet Scams:

- **NEVER** pay to be an employee for any company. Remember honest companies pay their employees. Research the company through a reliable source before you provide any personal information.
- **DO NOT** allow anyone to cash cheques in your bank account even if compensation is promised.
- **NEVER** make bank or wire transfers on another person's behalf.
- **DO NOT** click on suspicious website links. Look for spelling or grammar mistakes or logo's that appear odd.
- **HANG UP** on uninitiated tech support calls. If you did not request computer assistance, you probably do not need it. Protect your computer with trusted anti-virus software.
- **DO NOT** give a stranger remote access to your computer.
- **DO NOT** feel pressured to give out your financial or personal information.
- IF IT SEEMS TO GOOD TO BE TRUE, IT PROBABLY IS!

When to Contact the Police



If you are a victim of fraud in which you have incurred a financial loss and/or given out your personal information, call your local police to report the incident. Record details of your interaction with the fraudster including phone numbers, email addresses and communication with the fraudster. Photographs or screenshots of the messages are helpful. If you have **not** been a victim of a fraud but have information related to scams, please report this to the Canadian Anti-Fraud Centre through the website or email at <u>info@antifraudcentre.ca</u>.

Helpful Links

Canadian Anti-Fraud Centre - <u>https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm</u>

Consumer Protection BC - https://www.consumerprotectionbc.ca/consumer-help/scams/

BBB - <u>https://www.bbb.org/article/news-releases/19251-scam-alert-dont-lose-money-to-fake-lookalike-websites</u>

Desjardins - https://www.desjardins.com/ca/security/fraud-trends/mystery-shopper/index.jsp