# Better Business Bureau's Top 10 Scams of 2018

March 1, 2019

### 1. Romance Scams

More than \$22.5 million lost

Canadians were victimized financially, emotionally, psychologically and socially by this scam. Catphishing through online dating continues to be a very lucrative and seductive business for scammers.

- Never wire or transfer money to someone you have not met. Look out for sob stories, plans to visit the country to meet you and tales about family emergencies.
- Do not share personal information like your home address or telephone number on dating sites.
- Be wary of people who say they are out of the country or can never meet with you in person.

### 2. Income Tax Extortion Scams

More than \$6 million lost

Due to nationwide reports about threatening telephone calls, texts and phishing emails, this scam is one of the most prevalent around. While we are much better at recognizing it, many still fall victim. There are also calls and email extortion campaigns where people are being blackmailed for money, as well as prize scams that fraudulently use CRA's name to swindle money from you.

- The <u>CRA</u> does not make threatening phone calls or request personal information over the phone or by email.
- Delete texts and emails claiming to be from CRA, especially where they request your SIN.
- Canadian government agencies do not accept payment in Bitcoin or through gift cards.

### 3. Online Purchase Scams

More than \$3.5 million lost

Two spots down from last year, this scam is still one of the most diverse risks, as it ranges from fake websites and free trial traps to purchasing counterfeit goods and receiving fraudulent cheques from a buyer on sites like Craigslist.

- Always shop on legitimate websites and use reputable payment portals.
- Never wire money to someone you do not know and be aware of offers that are too good to be true.
- If possible, do transactions locally and in person.

### 4. Employment Scams

More than \$4.5 million lost

Holding its place from 2017, this scams is an ongoing problem for job-seekers, even those using reputable employment sites. Scammers may send cheques with a significant overpayment and request that you forward the excess to someone else. However, the cheque is fake and you will face the expense of covering the costs.

- Do your research on a company before accepting a job offer. Look out for poor grammar, unrealistic salary offers and insufficient details about the job.
- If you did not apply for a job, you did not get hired for one.
- A legitimate company will not ask you to forward money for any reason or pay an administration fee.

# 5. Phishing

Losses Unknown

Phishing takes many forms – from fake invoices and online endorsements to wire fraud. Fraudulent emails and fake websites that are created to deceive the public into believing they are authentic, continue to be a huge problem.

- If you receive an email that looks and feels suspicious, contact the business directly. Do not share personal information or click on links if you have doubts about the sender of the email.
- Only shop on legitimate websites. Avoid pop-up ads and impulse spending online.
- Compare details of the invoice with your order. Implement payment redundancies and educate your employees about these scams.

# 6. Subscription Scams

Losses Unknown

Be wary of online advertisements and pop-ups promoting skincare and cosmetic products, as well weight loss and diet pills. Canadians have been enticed by fake celebrity endorsements and the promise of a 'risk free trial', but end up falling into subscription traps with large monthly charges to their credit card.

 Read all the terms and conditions. Know when the free trial ends. Be wary of websites where this information is not readily accessible.

- If it looks too good to be true, it probably is. Contact BBB to verify the business and see customer reviews.
- Check if the order includes pre-checked boxes. These may sign you up for unwanted products and charges.

### 7. Advance Fee Loans

Almost \$1 million lost

Scammers prey on people in a financial bind, especially if they do not qualify for loans through reputable lenders. In most cases, they request an upfront fee to secure a loan, but this is illegal in Canada.

- If a company demands money to secure a loan, walk away.
- Be suspicious if a company guarantees a loan before doing a credit check.
- Check BBB for reputable lending organizations.

# 8. Tech Support Scams

Almost \$1 million lost

Scammers may call pretending to be computer techs from well-known companies like Microsoft or Apple. Others may send pop-up messages that warn about computer problems. They will say they have detected viruses or other malware on your computer and need you to give them remote access to your device. Eventually, they will diagnose a non-existent problem and ask you to pay for unnecessary or even harmful services.

- Never give control of your computer to a third party unless you know it is the representative of a computer support team you contacted.
- Legitimate tech support companies do not call out of the blue.
- Do not click on links in unfamiliar emails.

### 9. Home Improvement Scams

Losses Unknown

These scams may start with a knock on the door, a flyer or an advertisement. Door-to-door solicitors offer quick, low-cost repairs and then take payments without returning, do shoddy work, leave incomplete projects or create issues that dramatically raise the price. One common hook is when the scammer claims to be working in your neighborhood on another project and has leftover supplies.

- Say no to cash-only deals, high-pressure sales tactics, high upfront payments, handshake deals without a contract, and on-site inspections. Always get a written contract with the price, materials, timeline and details about what each person is responsible for.
- Check with BBB to see what other customers have experienced.
- Work with local businesses that have proper identification, licensing and insurance. Confirm that your vendor will get all the relevant permits.

### 10. Bank Investigator Scams

More than \$2 million lost

It starts with an early morning phone call from someone claiming to be a bank representative, law enforcement officer or an investigator and they tell you that there is fraudulent activity on your account. They may ask for your credit card details to cancel the transaction. Other times, the victim is told to call the number on the back of the card, but the caller does not disconnect the call. The victim may also be asked to transfer funds to another account for protection until the investigation is over or accept a deposit to later transfer it to another account. However, the deposit is not real, and victims transfer real money to the scammer.

- Banks do not ask clients to participate in investigations or to transfer funds to another account for safekeeping.
- Be wary of early morning phone calls claiming to be from your bank.
- Cryptocurrencies, binary options and investment fraud are also connected to this scam. Check BBB for reputable financial and investment firms and only invest what you can afford to lose.

ROYAL LEPAGE

Sandra Jackson

cell 416-579-7862 SJ@SandraJackson.biz