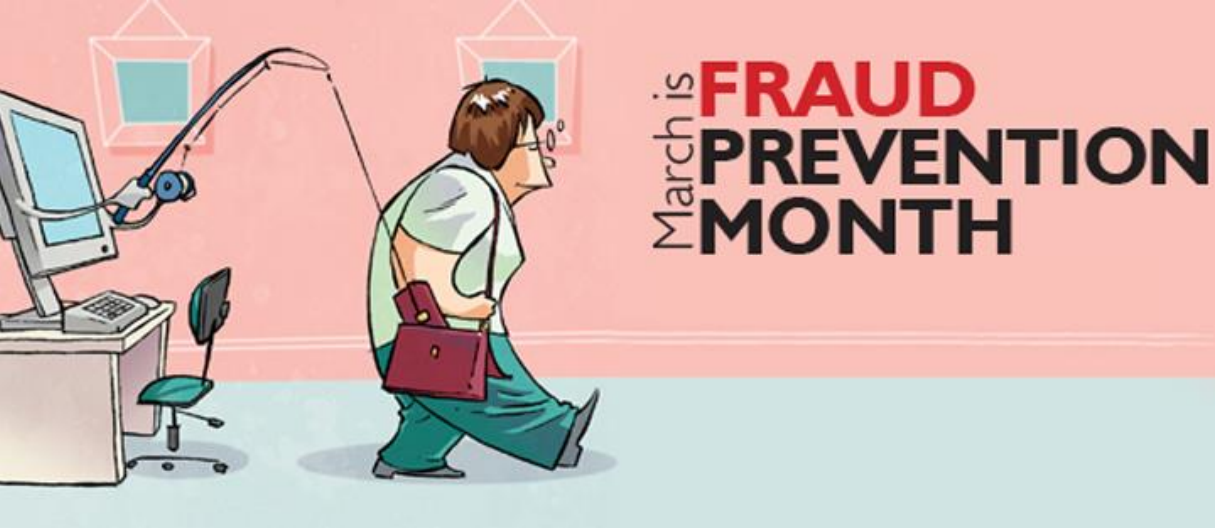



# Top 10 Scams of 2018

BETTER BUSINESS BUREAU

Adapted by:

Brian Freedman
Ballantrae Geek

Al Moldon
PC Doctor

# 1. Romance Scans

More than $22.5 million lost

- Seniors are the primary targets since they often spend more time alone as they age;
- Scammer sets up an account on a dating site with fake information and photos;
- Once target has been established, the scam usually escalates to the thief unveiling a money problem;
- Typical scenarios include the request for funds so he or she can visit you in person or help a sick relative;

# 1. Romance Scams

More than $22.5 million lost


- 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/or tales about family emergencies;
- Be wary of people who say that they are out of the country or can never meet with you in person;
- Do not share personal information like your home address or telephone number on dating sites.

# 2. Income Tax Extortion Scams

More than $6.0 million lost

- Email and telephone schemes that try to fool you into thinking they're from the CRA or partners in the tax community;
- May request banking information in order to process a refund;
- Threatening calls or emails regarding money owed and potential for arrest;
- Recorded messages left on your voicemail that leave the impression that if you do not call back, the CRA will issue a warrant for your arrest.

# 2. Income Tax Extortion Scams

More than $6.0 million lost


- CRA does not make threatening phone calls or request personal information over the phone or through email;
- Delete texts or emails claiming to be from the CRA;
- Canadian government agencies do not accept payment in Bitcoin or through gift cards.

# 3. Online Purchase Scams

More than $3.5 million lost

- One of the most diverse risks as can take many forms;
- Purchasing non existent items from a fake website;
- Airbnb scam involving fake homes and directing the renter to a fraudulent or *spoof* website to finalize payment;
- Free trial traps;
- Concert/event ticket scams.

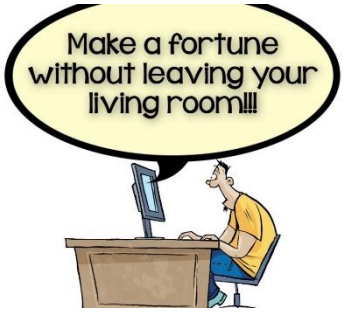
# 3. Online Purchase Scams

More than $3.5 million lost


- Always shop on legitimate websites and use reputable payment portals;
- Use credit card for purchases rather than cash, cheque or wire transfer;
- Be wary of offers that are too good to be true;
- Review potential purchase with knowledgeable (computer) family member or friend prior to making commitment;
- Stay *in-app* for booking, fulfillment and payment;
- When possible, conduct large $ transactions in person.

# 4. Employment Scams

More than $4.5 million lost




- Ongoing problem for job seekers, even those using reputable employment sites;
- Most common type of scam is when you are charged a fee for help finding a job that may not exist;
- Might be positioned as a “training fee” but once paid you are either not contacted or directed to public job boards;
- Scammers may also require you to provide personal information, especially your SIN#.

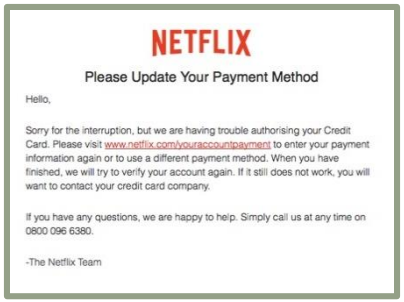
# 4. Employment Scams

More than $4.5 million lost


- 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, then 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



NETFLIX

Please Update Your Payment Method

Hello,

Sorry for the interruption, but we are having trouble authorising your Credit Card. Please visit www.netflix.com/youraccountpayment to enter your payment information again or to use a different payment method. When you have finished, we will try to verify your account again. If it still does not work, you will want to contact your credit card company.

If you have any questions, we are happy to help. Simply call us at any time on 0800 096 6380.

-The Netflix Team

- Phishing takes many forms, from fake invoices, receipts to wire fraud;
- Fraudulent emails and fake websites that are created to deceive the public into believing they are authentic:
  - Netflix -> "Payment Declined
  - Apple -> Apple or Itunes Purchase Receipt
  - Yahoo -> Problem with email account
  - CIBC -> Suspicious activity in your account
  - Google -> Confirm identify
  - UPS -> Confirm delivery details
  - Amazon -> Order cancellation

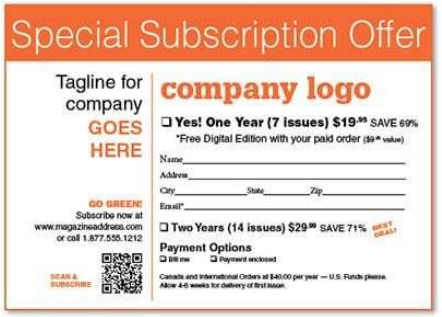
# 5. Phishing

## Losses Unknown


- Look behind the display name to the actual sender's email address for clues;
- Look behind the link display names to the actual URL for clues;
- Look for poor grammar, spelling mistakes, branding treatment and anything unbecoming of a major corporate brand
- Do not share personal information or click on supplied links;
- Avoid pop-up ads and impulse spending online;
- Compare details of the invoice with your original order.

# 6. Subscription Scams

Losses Unknown




- Most notably online advertisements and pop-ups promoting skincare and cosmetic products, as well as weight loss and diet pills;
- Often accompanied by fake celebrity endorsements and promise of “risk free trial”;
- Many Canadians falling into subscription traps with large monthly charges to their credit card.

# 6. Subscription Scams

Losses Unknown


- Read all the terms and conditions;
- Know when the free trial ends;
- Be wary of websites where this information is not easily accessible;
- If it looks too good to be true, it probably is;
- Contact BBB to verify the business and see customer reviews and conduct a broader search on the internet;
- Look out for pre-checked boxes while placing your order as these may sign you up for unwanted products and charges.

# 7. Advance Fee Loans

Almost $1.0 million lost


- Scammers prey on people in a financial bind;
- Seniors can be targeted as many do not qualify for loans through traditional lenders;
- In most cases, scammers request an upfront fee to secure a loan.

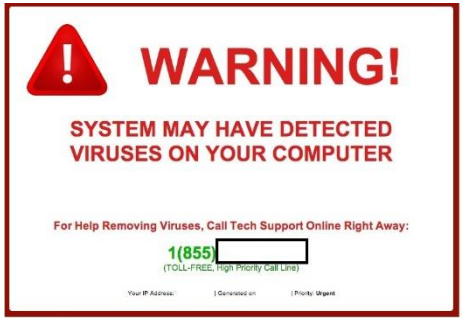
# 7. Advance Fee Loans

Almost $1.0 million lost


- 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 and online for reputable lending organizations.

# 8. Tech Support Scams

Almost $1.0 million lost




- Scammers may call pretending to be computer techs from well known companies like Microsoft, Apple or “Windows”;
- Others may involve computer pop up messages that warn about computer problems;
- They will claim to have detected viruses or other malware on your computer and request remote access to your computer;
- They will diagnose an existent problem and ask you to pay for unnecessary and often harmful services;
- May disguise themselves as the manufacturer or authorized manufacturer service agency on internet search.

# 8. Tech Support Scams

Almost $1.0 million lost


- Never give control of your computer to a third party unless you know it is the representative of a computer support team that YOU have contacted;
- Legitimate tech support companies do not call out of the blue;
- Do not respond to pop-ups and do not contact in response;
- Do not click on links in unfamiliar emails.
- Most pop ups are elimated by rebooting the computer. A hard boot may be required if the pop up freezes your computer.

# 9. Home Improvement Scams

Losses unknown

Photo: By Denphumi/Shutterstock.com

- Scams may start with a knock on the door, a flyer or an advertisement;
- Often offering quick, low cost repairs;
- Often take payment up front without returning, do shoddy work, leave incomplete projects or create issues that significantly increase the cost of the job;
- May claim to be “working in your neighbourhood” and have left over supplies from a nearby job.

# 9. Home Improvement Scams

Losses unknown


- Say no to “cash-only” deals, high pressure sales tactics, and high upfront payments;
- Always get a written contract with the price, materials, and timeline;
- Check with BBB, internet, even other Ballantrae residents to see what other customers have experienced;
- Work with local businesses that have proper identification, licensing and insurance;
- You have leverage with contractors who rely on the Ballantrae community for their livelihood!

# 10. Bank Investigator Scams

More than $2 million lost

- Call from someone claiming to be a bank representative, law enforcement officer or investigator advising of fraudulent activity in your account;
- May request credit card and related details in order to cancel the transaction;
- Or victim told to call the # on the back of the card but caller does not disconnect the phone;
- Victim may be asked to transfer funds to another account for protection until the investigation is over;
- Victim may be asked to accept a deposit for transfer to another account however deposit is not real and victims transfer their own money to the scammers.

# 10. Bank Investigator Scams

More than $2 million lost


- 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 and investment fraud are also closely related to this type of scam;
- Contact your bank and/or your investment advisor independently for confirmation or if you have questions/concerns;
- Always do your due diligence prior to making “investments” and seek professional advice.