HUMAN RESOURCE DEPARTMENT
Bldg. 8A – 7201 Vedder Road, Chilliwack, B.C. V2R 4G5
Tel: No. (604) 824-3200/FAX No. (604) 824-5342
Toll Free: 1-800-565-6004

August 1, 2024

Protect yourself from scams and fraud

https://antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm

Scammers can target any Canadian or Canadian business. Here are some tips and tricks to protect yourself or your business from scams and fraud. **Remember, if it seems too good to be true, it is.**

Don't be afraid to say no

Do not be intimidated by high-pressure sales tactics. If a telemarketer tries to get you to buy something or to send them money right away:

- Request the information in writing
- Hang up

Watch out for urgent pleas that play on your emotions.

Do your research

Always verify that the organization you are dealing with is legitimate before you take any other action:

- Verify Canadian charities with the Canada Revenue Agency
- Verify collection agencies with the appropriate provincial agency
- Look online for contact information for the company that called you, and call them to confirm
- Verify any calls with your credit card company by calling the phone number on the back of your credit card
    a. If you have received a call or other contact from a family member in trouble, talk to other family members to confirm the situation.

Watch out for fake or deceptive ads, or spoofed emails. Always verify the company and its services are real before you contact them.

Do not give out personal information

Beware of unsolicited calls where the caller asks you for personal information, such as:

- Your name
- Your address
- Your birthdate
- Your Social Insurance Number (SIN)
- Your credit card or banking information

If you did not initiate the call, you do not know who you're talking to.
Know how to protect your Social Insurance Number (SIN).
Know what to expect if the real Canada Revenue Agency contacts you.

Beware of upfront fees

Many scams request you to pay fees in advance of receiving goods, services, or a prize. It is illegal for a company to ask you to pay a fee upfront before they will give you a loan.
There are no prize fees or taxes in Canada. If you won it, it is free.

Protect your computer

Watch out for urgent-looking messages that pop up while you are browsing online. Do not click on them or call the number they provide. No legitimate company will call and claim your computer is infected

with a virus. Some websites, such as music, game, movie, and adult sites, may try to install viruses or malware without your knowledge. Watch out for emails with spelling and formatting errors and be wary of clicking on any attachments or links. They may contain viruses or spyware.

Make sure you have anti-virus software installed and keep your operating system up to date.
Never give anyone remote access to your computer. If you are having problems with your system, bring it to a local technician.

Be careful who you share images with
Carefully consider who you are sharing explicit videos and photographs with. Do not perform any explicit acts online.

Disable your webcam or any other camera connected to the internet when you are not using it. Hackers can get remote access and record you.

Protect your online accounts
By taking the following steps, you can better protect your online accounts from fraud and data breaches:

- Create a strong password by:
  - Using a minimum of 8 characters including upper- and lower-case letters, and at least 1 number and a symbol
  - Creating unique passwords for every online account including social networks, emails, financial and other accounts
  - Using a combination of passphrases that are easy for you to remember but hard for others to guess
- Enable multi-factor authentication
- Only log into your accounts from trusted sources
- Do not reveal personal information over social media

Learn more about securing your accounts by visiting Get Cyber Safe.

Recognize spoofing
Spoofing is used by fraudsters to mislead victims and convince them that they are communicating with legitimate people, companies, or organizations. Here are the main types of spoofing used by fraudsters:

Caller ID spoofing
Fraudsters have the ability to manipulate the phone number appearing on call display either by call or text message. Fraudsters can display legitimate phone numbers for law enforcement agencies, financial institutions, government agencies or service providers.

Email spoofing
Similar to Caller ID spoofing, fraudsters can manipulate the sender's email address in order to make you believe that the email you are receiving is from a legitimate source.

Website spoofing
Fraudsters will create fraudulent websites that look legitimate. The fake websites can pretend to be a financial institution, company offering employment, investment company or government

agency. In many cases, fraudsters will use a similar domain/website URL to the legitimate company or organization with a minor spelling difference.

Protect yourself from spoofing by

- Never assuming that phone numbers appearing on your call display are accurate
- Hang up and make the outgoing call when someone claims to be contacting you from your financial institution, service provider, law enforcement or government agency
- Call the company or agency in question directly, if you receive a text message or email. Make sure you research their contact information and do not use the information provided in the first message
- Never clicking on links received via text message or email
- When visiting a website, always verify the URL and domain to make sure you are on the official website

If you become a victim

If you think you have been targeted by identity fraud or identity theft, there are actions you should take to address the situation. Depending on the circumstances, you might need to:

2. Report the incident to local police if the matter involved a theft/crime
3. Report the incident to the Canadian Anti-Fraud Centre (1-888-495-8501) if the matter involved a scam or fraud
4. Advise your bank and credit card companies. Request new bank or credit cards with new numerical identifiers on them
5. Report any missing identity documents or cards, such as a driver's licence, a health card or immigration documents to the appropriate organization

*Additional tips can be found here: Identity theft and you - Office of the Privacy Commissioner of Canada.