



Businesses

Know who you're dealing with

Watch out for invoices using the name of legitimate companies. Scammers will use real company names, like Yellow Pages, to make the invoices seem authentic. Make sure you inspect invoices thoroughly before you make a payment.

Compile a list of companies your business uses to help employees know which contacts are real and which aren't.

Don't give out information on unsolicited calls

Educate employees at every level to be wary of unsolicited calls. If they didn't initiate the call, they shouldn't provide or confirm any information, including:

- the business's address
- the business's phone number
- any account numbers
- any information about equipment in the office (e.g. make and model of the printer)

Limit your employees' authority

Only allow a small number of staff to approve purchases and pay bills.

Watch for anomalies

Beware of:

- · larger than normal orders
- multiple orders for the same product
- orders made up of "big-ticket" items

These orders may be fraudulent.



Volunteer with Crime Prevention

Contact us.

Crime Prevention Unit

North Shore Community Policing Office 915 7th Street Kamloops BC V2B 2W7 Phone: 250-376-5099

Email: kamloops_crime_prevention@rcmp-grc.gc.ca

Kamloops RCMP

Emergency **9-1-1**

Non-Emergency **250-828-3000** Victim Services **250-828-3223**

Protect yourself from SCAMS AND FRAUD



Kamloops.ca/CrimePrevention

Scammers can target any Canadian individual or business. Here are some tips and tricks from the Canadian Anti-Fraud Centre to protect yourself or your business from scams and fraud.

Remember—if it seems too good to be true, it is.

Individuals

Don't be afraid to say no

Don't 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're 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 supposedly 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

If you've 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.

Don't give out personal information

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

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

If you didn't initiate the call, you don't know who you're talking to.

Beware of upfront fees

Many scams request that you to pay fees in advance of receiving goods, services, or a prize. It's illegal for a company to ask you to pay a fee upfront before they'll give you a loan.

There are no prize fees or taxes in Canada. If you won it, it's free.





Protect your computer

Watch out for urgent-looking messages that pop up while you're browsing online. Don't 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, bring your computer to a local technician.

Be careful who you share images with

Carefully consider who you're sharing explicit videos and photographs with. Don't perform any explicit acts online.

Disable your webcam or any other camera connected to the Internet when you aren't using it. Hackers can get remote access and record you.