PROTECT YOURSELF FROM SCAMS AND FRAUD

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
- 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

· Your address

· Your birthdate

· Your Social Insurance Number (SIN)

· Your credit card or banking information

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

Know how to protect your Social Insurance Number (SIN) by visiting online: www.canada.ca/en/employment-social-development/services/sin/protection.html

Why protect your SIN?

Your SIN is confidential. If it falls into the wrong hands, it could lead to several serious issues:

· Invasion of privacy and identity theft:

Unauthorized use of your SIN can lead to breaches of your privacy. If someone uses your SIN to commit fraud, it could ruin your credit rating

· Loss of money or credit:

Unauthorized use of your SIN could result in the loss of government benefits, tax refunds, or bank credits

· Unlawful employment issues:

If your SIN is used illegally for work, you could end up owing taxes to the Canada Revenue Agency for money you never earned

It is important to protect your SIN to protect yourself against fraud and identity theft. This will help you avoid problems and keep your money and personal information safe.

Beware of upfront fees

Many scams request 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 with your system, bring it 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.

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 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
- Don't reveal personal information over social media

Learn more about securing your accounts by visiting www.getcybersafe.gc.ca/en/secure-your-accounts

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're 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

· 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

· Call the company or agency in question directly, if you receive a text message or email. Make sure you research their contact information and don't use the information provided in the first message

· Never clicking on links received via text message or email

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:

· Any account numbers

· Any information about equipment in the office (e.g., make and model of the printer, etc.)

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.