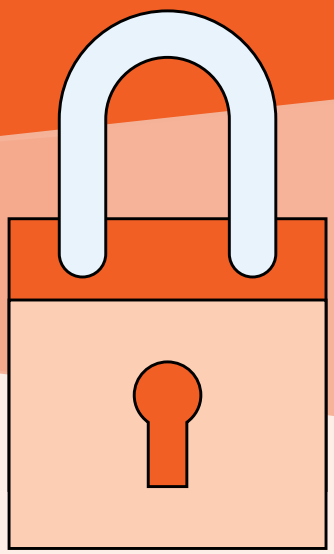
Cyber Security Toolkit for Newcomers



We are all in this together. Banks in Canada are working around the clock

Unfortunately, criminals also use the Internet to try to gain access to personal information such as passwords, personal banking and credit card details and social insurance numbers to commit fraud.

This risk is especially pertinent for newcomers, who may be

and common scam practices prevalent in Canada.

Our increasingly connected world means that your personal

Cyber Hygiene Checklist

Protecting your devices and information from cyber attacks

Cyber hygiene is a great way to think about the importance of taking regular steps to proactively protect your connected devices, such as our mobile phones, laptops, desktop computers and smart appliances from cyber threats.

While banks in Canada use sophisticated technology and layers of security to help protect customers from fraud there are steps that you can, and should, take to protect yourself.

system has a _____ or download one to help protect your device from malicious intrusions.

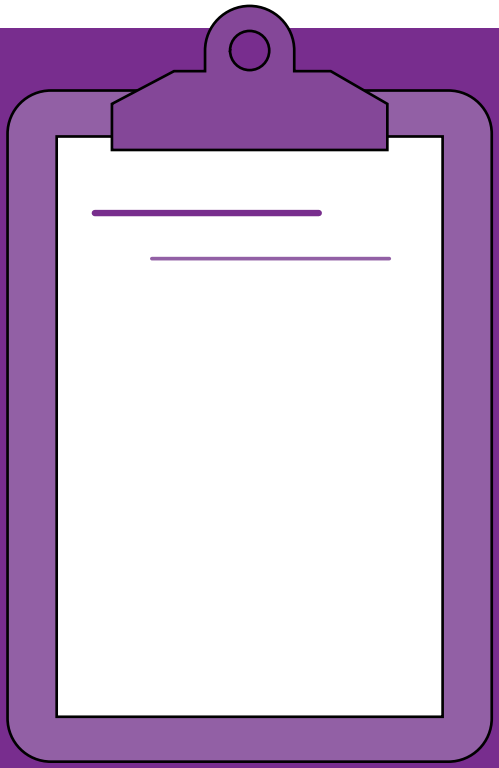
known vulnerabilities.

Ensure that you create strong and unique passwords or passphrases for each website and enable Multi-Factor

the event of a security breach at one site in which your password is handed to criminals who may try to use it at other sites, they

or know that your password has been compromised, be sure to

where you have reused it.



There are several common scams you should be aware of including:

- Email Fraud or Phishing Scams
- One-Time Passcode Scams
- Phone or Voicemail Scams
- Tax Season Scams
- Fake Job Opportunities
- Identifying Fake Websites and Applications
- Protecting Against Ransomware

Many scams are variations on a set of tactics cyber criminals use to attempt to trick you into revealing sensitive personal information.

Social engineering is the process criminals use to exploit our basic human urge to respond to urgent requests, be useful or help a friend in need, to lure us into providing information that can
fraud. Social engineering tactics try to trick us into clicking on malicious links and attachments or into providing sensitive information that can be

Protecting Against Phishing Scams

Phishing scams

true that spelling and grammatical mistakes in an email

The calls, texts or voice messages use threatening and aggressive language to frighten and bully you into paying the fake fees or providing your login credentials. A common tactic used by cyber criminals is to claim that you have an outstanding debt with your bank.

The calls or messages include

Spotting tax season scams

pose as representatives of the Canada Revenue Agency (CRA)

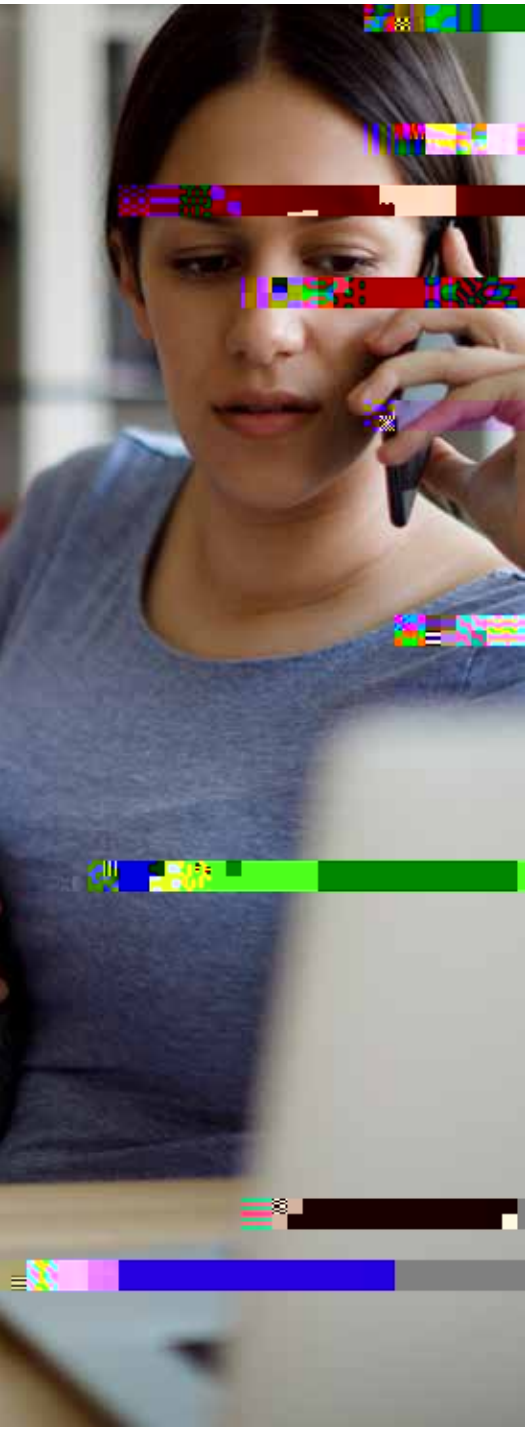
“debts” or into providing sensitive personal information that they can use to commit fraud.

Cyber criminals might send you

messages by text, phone call or email such as:

If you receive a call saying you owe money to the CRA, contact them directly or check your online CRA account. If you believe you have

Avoiding Online Employment and Job Scams



including:

- a text or email with promises of easy money.
- asks you to cash the cheque and send a portion of the money to another overpayment scam.
- You apply to an online job ad for a requires you to deposit payments from account and then redirect those funds could be the proceeds of crime and the cyber criminal has hired you to launder the funds as a money mule.

Always verify that a legitimate company is

Validate the job posting is legitimate by

online job boards or by calling the company using a phone number you know is correct

Never accept funds on behalf of someone

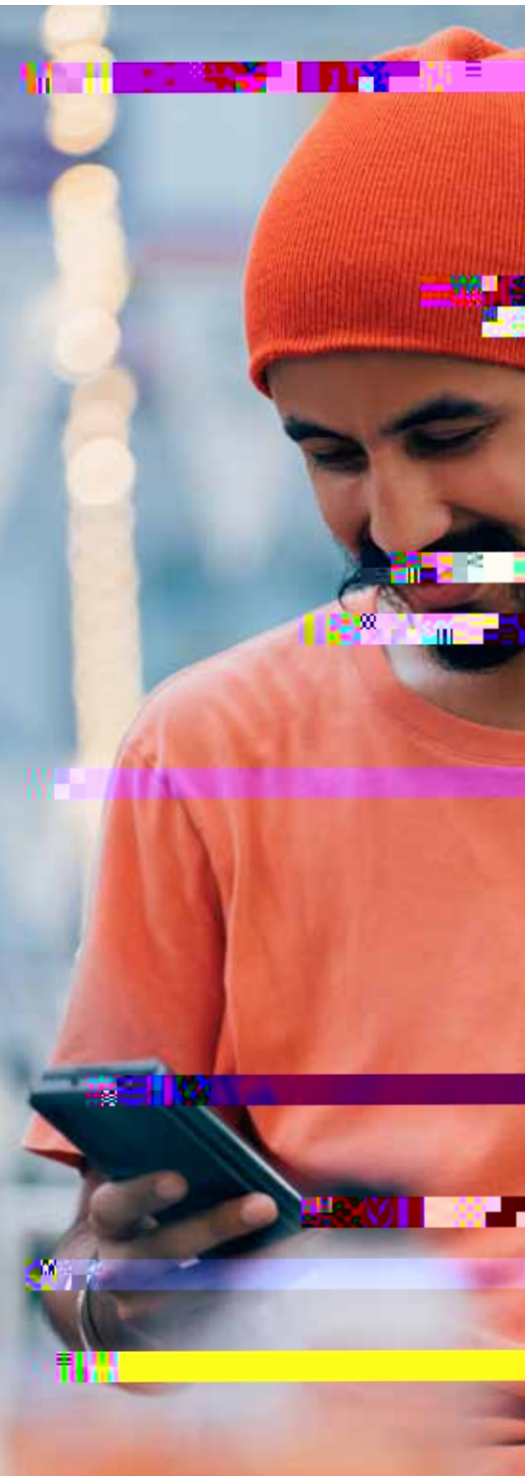
The Canadian Anti-Fraud Centre provides a listing of common job scams on their website.

How to Spot Fake Websites and Apps

Cyber criminals create online shopping websites and apps that have a similar look and feel to genuine retailers under an intentionally misleading, legitimate-sounding name.

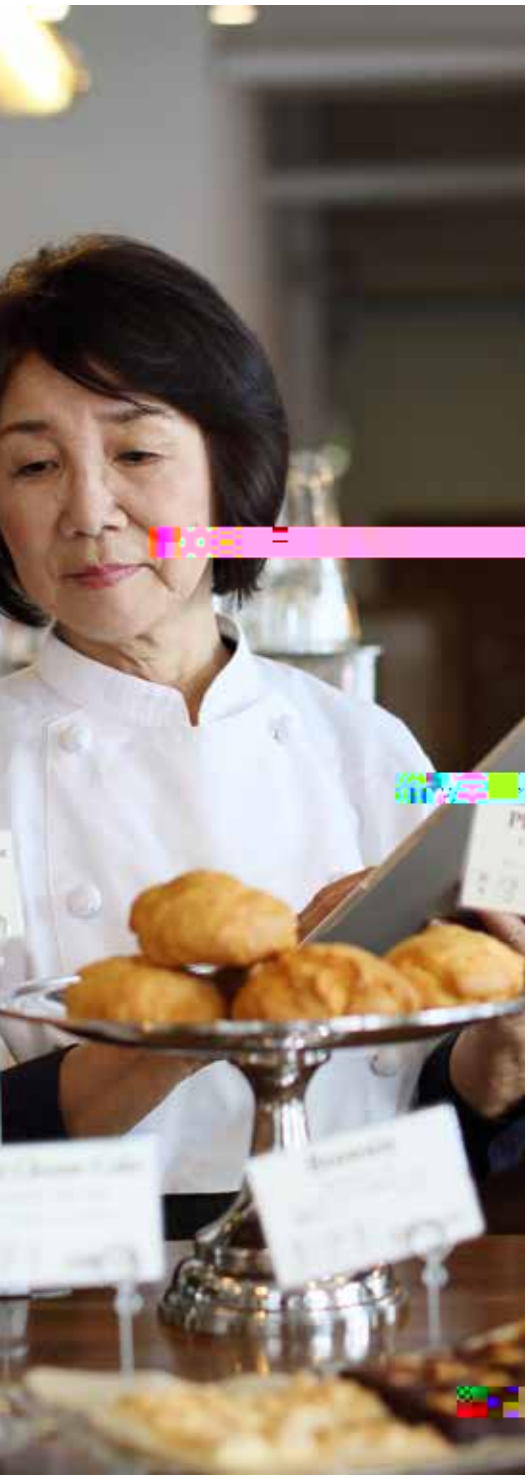
These spoofed websites and apps are a front to steal your credit card details and sensitive personal information.

Here are a few clues to help you identify a fake website or app.



- the site looks poorly designed, unprofessional and has broken links,
- the site URL has typos or uses unrelated terms and acronyms,
- the site has an unlocked padlock or

  unencrypted, therefore your information is unsecure. A green, locked padlock and https at the beginning of the URL are signs that the website is using encryption to securemation



Install reputable, up-to-date anti-virus

on all your devices and keep on top of updates.

Take the time to update and install the latest version of your operating system and applications.

on all systems and accounts to have an additional layer of security.

external source, such as an external drive or cloud-based storage, that is not linked to your computer. Keep highly

using a USB or external hard drive. If they are linked, your backed-up data could be encrypted too.

Be careful to not click on links or open attachments from unknown addresses

could unknowingly download malware by enabling a macro, clicking on an email attachment, link or online pop-up window.

your

from

your computer. If you are the victim of ransomware, you can consider the following:

Check with your anti-virus provider

If you are familiar with data recovery, you may try to remove the malware yourself. Some anti-virus providers can detect this malware and may have

Consult an IT security specialist

A professional may be able to help you remove the ransomware and restore

Change your passwords

Change your online passwords for compromised and connected accounts. That will help stop the criminals from accessing your accounts if they were able to access your passwords.

Report the scam

Choosing strong unique passwords for your sensitive online accounts like your main **email account and your financial** accounts is important since a

How to report fraud

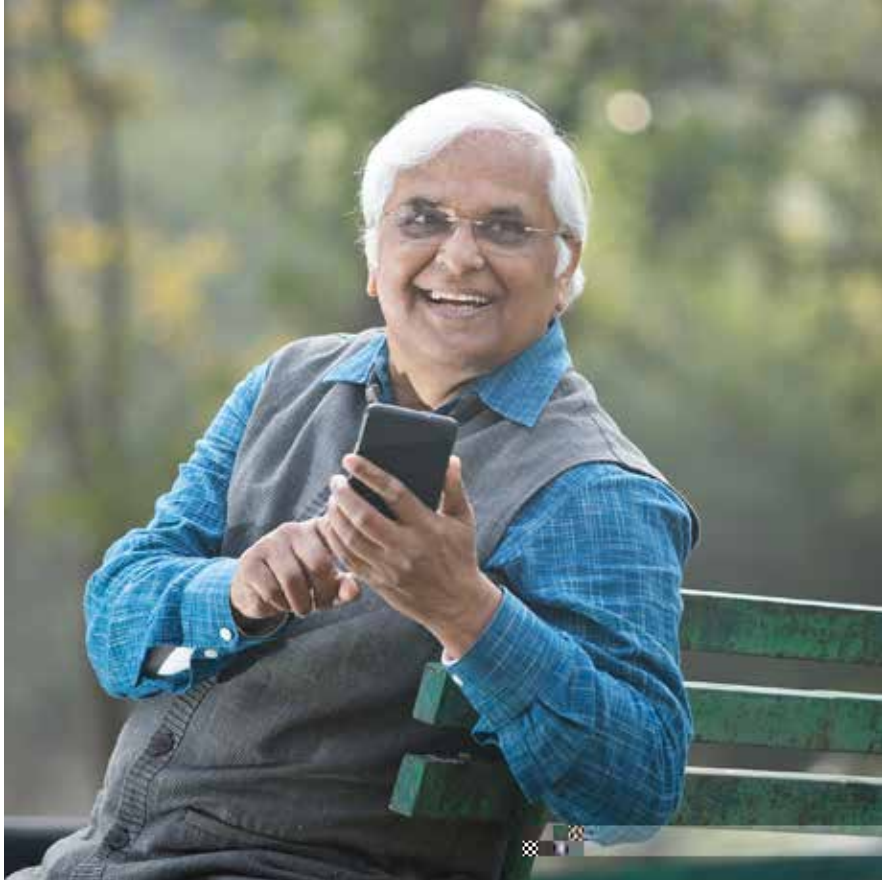
Remember, being the victim of a scam or fraud is not your fault. You can help yourself, and others, by taking immediate action.

If you think you may have provided bank account access, credit card

bank right away using a phone number that you know is correct (for

Report any incidence of fraud to your local police. They may be able to help and you might prevent others from becoming victims of a scam.

You can report frauds and scams to the Canadian Anti-Fraud Centre



Canadian Bankers Association
Fraud Prevention website:
cba.ca/fraud

Cyber Security Awareness Quiz Site:
cbacybersafety.ca

Canadian Bankers Association
Free fraud prevention newsletter.
Subscribe online.