Your 10 power tools of protection

There are ways to approach life on line that will reduce your chances of being scammed. Use these and you'll be safer. No approach is fool proof, so use your best detective skills to find the truth.

1. Just say no!

When scammers start to pressure you to send money right away or tell you someone will go hungry or die if you don't give (emotional request), say no:

- Get their information and research the company online or at the library
- Do not ask for anything in writing if it gives them access to your home address.
- Only ask for it in writing if they have your address
- Hang up. You do not have to be polite. Just hang up.

2. Research – Check it out first

Look online, in the phone book or at the library for contact information for the company that called you, and then call them to see if they are the ones who contacted you. You are protecting yourself and the companies that the scammers are pretending to represent. Those companies are innocent victims, too.

- Look out for fake or deceptive advertisements, or emails that are disguised to look like a trusted company but are in fact something scammers have created. Always verify the company and its services are real.
- You can look and see if Canadian charities are real by going to the Canada Revenue Agency. https://apps.cra-arc.gc.ca/ebci/hacc/srch/pub/dsplyBscSrch?request_locale=en
- Find out if the collection agency is real by checking with consumer affairs in your province: http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02982.html#ab
- Verify any calls with your credit card company by calling the phone number on the back of your credit card

3. Protect your computer

- Online advertisements and pop-up offers are hard to resist clicking on. Scammer know this. Do not click on them or call the number because they will then begin their high-pressure manipulations.
- Microsoft, HP, Apple, Asus, etc. or any of the other real computer companies know if your computer is infected with a virus. No real computer or software

company is going to call you and say your computer is infected with a virus. You know this because you have a good virus protection on your computer

- Unless you called a company, you know for computer help, like the Edmonton Seniors Centre, do not give anyone remote access to your computer.
- Do not click on links or attachments in odd emails or even on ones the look real. If they have spelling mistakes or fuzzy logos don't click. They may contain viruses or spyware that gives scammers access to everything you do on your computer, including financial transactions.
- Make sure you have anti-virus software installed and keep your operating system up to date.

4. Learn to Spot Fake Documents

Not all fake documents look like fakes. Seals, logos, certifications, and signatures can all be faked. Many fakes will look like the real things. So how do you tell? The seals can't be found on the internet are real company seals. Do a Google image search. Some fake companies even claim to be registered with a government agency. Simply go to that agency and search for their incorporation papers and the date

The message in the documents creates a sense of urgency so you won't look at it too closely. If you believe your power is going to be cut or your Netflix cancelled, you tend to click without thinking. When you see a threat, even a mild one, in an email or over the phone, stop and investigate carefully.

Does the message use a generic greeting, e.g., to whom it may concern, hi, hello, dear account holder? If it doesn't know your name, delete it.

When you search for more information online, does the company exist? No? Delete the message. If it does exist, it doesn't mean the email if real. Check the address the email came from. Does it match the email address of the company's website email? No? Delete the email.

If the message is poorly written, e.g., poor grammar, misspelling, fuzzy (pixelated) fonts. Poor usage of words and phrases that don't really fit it is a fake. Some of the language may use big words that are meant to be intimidating, but that is to try and make it sound official. Do the words fit the meaning of the message content?

5. Keep Personal Information Safe

Never give out the personal information to someone who calls you or contacts you by email. Be aware that sometimes companies you have done business with in the past, like Apple, IBM, Microsoft, Amazon, iTunes etc. appear to be sending you an email asking for you update your information or telling you that you owe them money or that they want to refund you money.

Do not follow the links in those emails. They are a way of getting your information which can then be used to enrich the criminals. Or worse yet, it can be sold on the dark web to people looking to steal your identity, which is then sold to other criminals.

Never give out the following to someone who contacted you:

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

There is information here on how to protect your SIN number: Your Social Insurance Number: A shared responsibility - Canada.ca

If you don't have an online CRA account, set one up. Registration process to access the CRA login services - Canada.ca

This is a great way to communicate directly with the CRA.

6. Don't pay in advance

If someone contacts you and asks you to pay fees in advance of receiving goods, services, or a prize, it is a scam. You power comes in refusing the temptation of something that is too good to be true.

Note: It's illegal for a company to ask you to pay a fee upfront before they'll give you a loan or a prize. Canada has no prize fees or taxes. If you won it, it's free.

7. Don't share pictures online without thinking it through carefully. The Internet is forever.

Once a picture is on the internet it is there forever.

- Criminals and those who deal in child pornography look for innocent pictures of children to use for horrible purposes. Be careful about what you put on your social media and never share personal information about your family, including schools they are going to, where they live, how old they are, when they are going on vacation, etc. Love them enough to protect them.

- Set your social media privacy settings on high but remember if your friends can see it, they can innocently share it. Don't label your pictures with the names of your family. That information can be used in scams if you don't set it high
    - For example, you get a phone call. "Granny, this is your grandson George. I'm in real trouble and need $5000 in the next two hours." In fact, **it is not George**, it is someone pretending to be George and faking trouble.
- The scammer got all his information from your social media account and he will use it to convince you he is George
- . From the pictures you posted the scammer knows:
    - what kind of car George drives,
    - his girlfriend's name and what she looks like,
    - the university he attends and his major,
    - his address because you took a photo outside his apartment and you unknowingly captured his address in the picture.
    - the scammer knows your husband just died from your posts and that you are grieving and might not be thinking clearly.

  With all that information he can make a pretty good case that he is your beloved George.
- Turn off your webcam or any other camera connected to the internet when you aren't using it. Criminals can get remote access and record you.
- Carefully consider who you're sharing explicit videos and photographs with. Remember those sexy photos will never go away and can be shared without your permission.
- Don't perform any explicit acts online.
- Remember, even though you delete it, is can be retrieved. Nothing ever dies on the internet. The internet and everything you put on it is there forever.

8. Password and family safe word protections

Scammers love it when you use passwords like 1234, or your name. Here are some ways to create strong passwords:

- Use at least 8 characters, including upper and lower case letters, and at least 1 number plus a symbol, e.g., #)@*#%~@!*. For example: Kldijls12@slbiil#. You can keep track of passwords by locking them away at home or you can get an online password manager. Here you can read a review of potential managers: https://www.wired.com/story/best-password-managers/

- Enable multi-factor authentication. This is used to ensure that the person asking to use the device, or account are who they say they are. This is done by requiring that they provide at least two pieces of evidence to prove their identity. For example: it can be questions only you know the answers to plus a code send to your cell phone, or it can be a question only you know the answer to and a PIN number you created when you set up the account. This helps protect you from criminals who want to break into your accounts
- If a scammer has figured out one of your factors, the second one usually proves too much for them
- Make a unique password 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. A passphrase is like a password, but longer and more secure.

Safe Words and Phrases

You can help yourself by talking to your family and finding a "safe word or phrase" that the caller has to use to identify they are actually whom you believe is calling. You can also come up with an agreed upon hint that does not give the safe word away. For example:

- "Granny, this is George. I am in trouble and I need $5000 in the next two hours."

  "George, how awful for you. I hope you're ok. Can you tell me the family safe word?"

  "I've forgotten it Granny. I'm too scared to think straight. Please help me."

  "As soon as I hear that safe word, George, the money is all yours. Let me give you a hint. The Owl in the tree calls squee, squee, squee."

  "The password is Hoot, Gran."

Granny knows it is not "hoot" and she knows he's never called her Gran in his life. She hangs up the phone and immediately calls George.

What was the safe word? It is a phrase that the family decided on together: the first four lines of the *Owl and the Pussycat* by Edward Lear, a poem the family used to read together, so it is easy for them all to remember.

9. Learn baby Learn

Education is your best defense. Take courses, read reputable websites, like the Government of Canada's Little Black Book of Scams, or the RCMP scams website.

Alter others when you uncover a scam by reporting them. Digital literacy is something that you can learn and that will be your shield of steel against these super villains.

10. Ask yourself hard questions

The minute you begin to feel fear, panic or pressure to act, stop! Take a deep breath and begin asking yourself questions that your friend would ask you? Is this reasonable? Who am I really talking to? The CRA doesn't threaten people, so why is this person threatening me?

If you are feeling too anxious to do that, hang up or leave the email and phone a friend, someone you trust.