BIPT
BURNABY
INTERCULTURAL
PLANNING TABLE

Scams, Fraud, Internet Safety, and Cyberbullying

Tips for Youth, Parents, and Seniors

Funded by: Immigration, Refugees and Citizenship Canada
Financé par : Immigration, Réfugiés et Citoyenneté Canada

Table of Contents

Acknowledgements

Intercultural Connections Working Group

Andisheh Fard - SFU
Cindy Chang – City of Burnaby Recreation & Cultural Services
Darae Lee - MOSAIC
Deborah Baker – Squamish Nation
Duncan Olenick – Burnaby Public Library
Evelyn McGowan – Purpose Society / Burnaby Youth Hub
Gabriella Maio – Ministry of Children and Families Development
Heather McCain – Citizens for Accessible Neighbourhoods
Kimberly Barwich – Burnaby Neighbourhood House
Melody Monro – Fraser Health
Natalya Khan – Burnaby School District #41
Rebekah Mahaffey – City of Burnaby
Sangeeta Bhonsale – Burnaby Family Life
Shae Wiswanathan – SUCCESS
Tarana Sultan – PIRS
Thea Fiddick – ISS of BC

Immigrant Advisory Council

Abeer Hattab
Derek Chen
Mary Blanca de Battenberg
Sherwan Azad
Sossan Kayoumi
Tedros Geday
Tom Su
Zarif Ahmad Akbarian

Internet Safety Tips for Parents

Talk About Internet Safety - From privacy concerns to identity theft, dangers exist on the internet. Children and teenagers need supervision when using the internet whether they are 5 or 15 years old, and adults need to remain attentive as well. Attention to safety concerns, such as sharing whereabouts, photos and personal information will go a long way to protect your loved ones.

- How to Structure Homework and Time Online: https://childdevelopmentinfo.com/family-building/structure-homework-time-online/#.XQgWjTZ8CM8
- **10 Internet Safety and Technology Use Tips for Parents:** https://www.kathleenamorris.com/2019/05/16/internet-safety-parents/
- Internet Safety Advice: Top Tips for Parents: https://www.webwise.ie/parents/advice-top-10-tips-for-parents/

Unsupervised/Early Internet Use - In a survey by Shared Hope International one out of eight parents allow their children to use the internet from the age of two and only one out of 10 allow their children use the internet when they are 10 or older, (as recommended by experts). As a result, many children are using the internet while unsupervised at an early age. Here's how to protect your kids while online:

- https://protectkidsonline.ca/app/en/interests_and_risks-5_to_7
- https://protectkidsonline.ca/app/en/interests_and_risks-8_to_10
- https://protectkidsonline.ca/app/en/interests_and_risks-11_to_12
- https://protectkidsonline.ca/app/en/interests_and_risks-13_to_15

Monitoring Your Children's Online Activities - Unfortunately, regardless of parental involvement, many teenagers hide or delete their browsing history from their parents. It is imperative for parents to be diligent. Teens have also have email or social media accounts that their parents maybe unaware of. In some cases, children lie about their ages to create these accounts.

- https://protectkidsonline.ca/app/en/info_monitoring_online_activities
- For parent support in cases where children experience peer victimization, parents should refer to the "Pyramid of Support" resource at: https://witsprogram.ca/pdfs/families/pyramid-of-support.pdf

Cell Phones - Cell phones are great for keeping in touch and in case of emergencies. Approximately 69 percent of 11 to 14-year-olds have their own cell phones. Cell phone users must understand and be aware that a cell phone's GPS can reveal the user's exact physical location. Also, always be cautious about posting personal cell phone numbers online.

- When to Give Your Child a Phone: https://childdevelopmentinfo.com/child-activities/when-to-give-your-child-a-phone/#.XQgW-zZ8CM8
- Cellphone Safety Tips: https://protectkidsonline.ca/app/en/info_phone_safety
- The First Cell Phone: Rules for Responsibility: https://www.ahaparenting.com/Ages-stages/tweens/Cell-Phone-Rules-Safe-Responsible-Kids
- Parental Monitoring App to Track cell phones across Canada and beyond the borders: https://pumpic.com/parental-monitoring-app-canada.html

Online Bullying - There are several anonymous conversational apps and websites where questions or information about others may be posted (anonymously). These anonymous apps, which include Whisper, Yik Yak, and Ask.FM, are dangerous because they have been known to promote bullying. Hiding their anonymous identities, bullies easily taunt, tease, and put others down. It is important to always remain diligent and report any abuse, whether suspected or proven.

- PREVNet: Promoting Relationships and Eliminating Violence Network is Canada's authority on research and resources for bullying prevention.
- What to do if your child is being Cyberbullied?: https://needhelpnow.ca/app/en/resources_cyberbullying
- WITSProgram: The WITS Programs bring schools, families and communities together to create supportive environments that help children deal with bullying and peer victimization
- RCMP's Centre for Youth Crime Prevention: provides Canadians with age appropriate crime prevention information and tools to prevent youth crime and victimization.
- Kids Help Line, is a good resource for parents and their children. It provides access to counseling **Need help right now? Text CONNECT to 686868 to chat with a volunteer Crisis Responder 24/7.** https://kidshelpphone.ca/search/?keys=Cyberbullying

Explicit Photos - Research indicates that one in seven teenagers have taken a nude or semi-nude photograph of themselves, and over half of those photographs were shared with someone else via the internet. It is important to note that once information is posted on the internet, there may be no way to remove it completely.

- Cybertip.ca: Canada's tip line to report the online sexual exploitation of children.
- https://protectkidsonline.ca/app/en/info_self_peer_exploitation
- https://protectkidsonline.ca/app/en/info_online_extortion
- https://protectkidsonline.ca/app/en/info_online_luring

Online Shopping, Identity Theft, Surfing the Web - It is important to be careful when surfing the web. Your web activity history is constantly being tracked. Visiting insecure or inappropriate websites can compromise your personal and financial information or harm your computer. It is important to have adequate security and ant-virus software installed on all computers. One should always use a secure connection, never use a public computer, and ensure websites are legitimate and secure before placing an order online. Following these precautions will provide users with a safer experience. Children are victims of identity theft more often than not. In fact, compared to adults, children under the age of 18 are 51 times more likely to have their identities stolen. Criminals target children because they have clean credit records and, as previously reported, frequently post personal information online.

- How to find a child's credit status, step-by-step instructions on how to check your child's credit report: https://www.creditcards.com/credit-card-news/instructions-how-to-check-child-credit-report.php

Video Games - Video games have come a long way in recent years. With the many gaming options available, parents need to be aware that most gaming devices can directly connect children to the internet and other players. Fortunately, most gaming devices have parental controls and safety settings. Parents should limit the amount of time their children play video games.

- Recommended online educational games to teach children & teen in grades 4 to 8 about how to be safe when using the internet: http://mediasmarts.ca/digital-media-literacy/educational-games

TALKING ABOUT INTERNET SAFETY WITH YOUR KIDS:

SOURCE: http://www.family.ca/internet-safety-tips/

1. Keep your personal information private – don't give out your name, phone number, school or address without a parent/guardian's permission.

2. Most social networking sites such as Facebook and Twitter will let you choose who can view your posts. Ask an adult to help you change your privacy settings.

3. Keep in mind that anything you share on social media – even in private – could be viewed by someone else. Always think twice before clicking "post" or "send"!

4. If you see anything inappropriate online, ask a parent or trusted adult for advice. Remember, it's not your fault you saw this!

5. If someone sends you something rude over email or social media, DO NOT RESPOND – instead, speak to a responsible or trusted adult.

6. If you're sharing photos or videos that have other people in them, always ask for permission first.

7. Never buy something online or download anything without permission from a parent/or guardian.

8. Never agree to meet in-person with someone you've only known online. Remember that people may not be who they say they are!

9. Keep your passwords SECRET! Not even your BFFs need to know!

10. Stand up against Bullying – don't gossip or humiliate anyone! If you want more information about cyber-bullying or bullying in general, visit http://www.family.ca/standup/

FRAUDULENT CALLS:

Beware of callers falsely claiming to represent a trusted company or organization.
https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdInt-clls-en.aspx

WHAT TO DO IF YOU GET A CALL:

If you get such a call, hang up. Never give remote access to your computer in response to an unsolicited call. If you are unsure, contact the company or organization's customer service center. We strongly encourage Canadians to report such instances of fraud to the Canadian Anti-Fraud Centre at: http://www.antifraudcentre-centreantifraude.ca or by calling 1-888-495-8501.

ONLINE SCAMS AND FRAUD:

It's not always easy to determine whether an email, contest or promotion is real or an Internet scam or fraud. The offers might seem too good to be true – and they may be. The key to being safe is recognizing the signs of scam artists. **https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx**

WHERE CAN I FIND OUT MORE?

There are many good on-line sources of information about fraud and scams. **The Financial Consumer Agency of Canada website**, provides information about your rights in dealing with banks and other financial institutions.

To order additional copies of this publication, or for help finding a phone number in your province or territory, call 1 800 O-Canada (1-800-622-6232), TTY: 1-800-926-9105.

WHAT SHOULD I DO IF I THINK I HAVE BEEN SCAMMED?

One of the most common scams in Canada is a phishing or smishing scam, where a scammer poses as a business or government organization. Take for example scams claiming to be from the Canada Revenue Agency. Sometimes the intended victim is told they owe a steep balance, and if they don't pay, the RCMP will come to arrest them. Sometimes the intended victim is told they can "click on a link to accept your refund". Some are simply told to follow a link to review changes to their information, or to fill out a form with their personal information.

WHAT SHOULD I DO IF I THINK I HAVE BEEN SCAMMED?

If you are unsure if the message is legitimate, don't respond! Visit the organization's website and call them directly to verify the information you received. As many of us have received a fraudulent CRA message demanding payment for taxes, the CRA provides the following advice:

- The CRA never asks for personal information via email or text,
- The CRA also does not request payments by bitcoin or gift cards.

If you receive a call, text message, or email saying you owe money to the CRA, or are owed a refund or benefit payment, login or sign up for My Account or My Business Account to verify your tax status, or call CRA's Individual Income Tax Enquiries line at 1-800-959-8281.

If you fall victim to a scam, there may be a number of steps to take:

1. Report **fraud** to your local police in your community: Burnaby RCMP's **Non-emergency (24-hour)** Tel: 604-646-9999 and website: **http://burnaby.rcmp-grc.gc.ca**

2. If your **Social Insurance Number** has been stolen, contact **Service Canada** at 1-800-206-7218 to report it.

3. Report a **scam** to the RCMP's **Canadian Anti-Fraud Centre**. You will be asked to use a sign-in partner (i.e. your bank) or a GCKey (just as you do to access your CRA account). This ensures your own security when reporting scams. You can also call the Anti-Fraud Centre at 1-888-495-8501.

Scammers use similar tactics when pretending to represent a bank or credit card company. For example, you may receive an email or text from a bank you do not deal with asking you to review your statement. It's easy to recognize phishing or smishing when the message doesn't come from your own bank. But, if you're concerned that it could be from your bank, don't respond to the message--reach out to the bank directly by telephone or in-person or log in to your online banking site or app (**using a secure internet connection**, of course) to verify if it's real. And don't forget to report the phishing/smishing message to your bank.

For more information on other cyber incidents and reporting, visit the **Canadian Centre for Cyber Security**.

FOLLOW GET CYBER SAFE ON TWITTER, FACEBOOK AND INSTAGRAM.

5 Ways to Protect Your Privacy on a Smart Device (Smartphones/Tablets/Smartwatches):

These tips are for any device that connects to the Internet that you may have at home. While connected devices (also known as “smart devices”) are fun and make our lives easier, they also provide opportunities for hackers to access personal and private information. Take steps to protect you and your family, by following these tips:

1. **SECURE YOUR HOME WI-FI NETWORK:**
   Smart devices use the Internet to send and collect data. If your home Wi-Fi connection is not secure, your data is not secure! When using Wi-Fi, the minimum security you should have is wireless encryption and password protection. Under your wireless settings, make sure your router has WPA2 encryption enabled. Then, lock your wireless network with a strong a unique password. A strong password includes uppercase and lowercase letters, numbers, and special characters.
   If you are an advanced user, create a separate network zone on your Wi-Fi network to connect your smart devices. This is called "device isolation" and functions similarly to "Guest Wi-Fi" networks. When using your smart device on-the-go, connect only to trusted, password-protected networks, and turn off settings that automatically search for Wi-Fi networks.

2. **TURN OFF GEOLOCATION WHEN NOT IN USE:**
   Many smart devices have apps that use geolocation to provide services, such as fitness tracking or maps. If an application can see your location, a hacker could too. In your device’s settings, turn off geolocation when you are not using it.

3. **BEFORE INSTALLING APPS, UNDERSTAND THE APP'S PRIVACY POLICY AND TERMS OF USE:**
   All apps have privacy settings that help control who can see your information, and what they see. Customize these privacy settings so personal information, such as full names and contact details, are hidden. Also, be wary of apps asking for unnecessary or excessive information. Take a good look at the permissions, and don't just click “allow” for everything.

4. **DISABLE MICROPHONES AND CAMERAS WHEN NOT IN USE:**
   Most gaming headsets, smart TVs, smartwatches, and smart speakers come with a microphone and/or camera. If not secure, your device could transmit information you don’t intend it to. Turn off your camera, and mute your microphone, when you are not using it.

5. **CREATE USERNAMES THAT DON'T CONTAIN IDENTIFYING INFORMATION:**
   Oversharing could put your privacy at risk. When setting up a login for your device (or for a game or app), make sure your username does not contain identifying information, such as your name, age, location, or contact information.

6. **BE SMARTPHONE SAVVY**:
   Smartphones can track your location and reveal information about you, including your contacts. Be careful to only download and use reputable apps and be sure to password (or fingerprint) protect your phone. Know how to use tools to find or erase personal data from lost phones. You'll find more information at **ConnectSafely.org/cellphone-safety-tips**.

7. **SECURE YOUR INTERNET ROUTER**:
   There is likely a small device in your home, called a router or broadband modem that connects you to the Internet. That device has a password and username and sometimes the default passwords are very easy to guess. Routers can be hard to configure so if you're in doubt, contact an expert or your Internet service provider for advice on how to change the password.

PROTECT YOUR DEVICES:
By ensuring they are password protected and, in the case of computers, make sure you have good security and firewall software in place. If you need help, reach out to knowledgeable friends or family, or your Internet service provider or mobile operator. SHAW and some other Internet service providers may offer free anti-virus software, or you can purchase or obtain free security software from a reputable company such as the ones listed at **ConnectSafely.org/securityvendors**.

OTHER RECOMMENDED RESOURCES FOR ADDITIONAL TIPS VISIT:

FightSpam.gc.ca: help for Canadians and business to avoid spam and other electronic threats

Youth Privacy: Information and tools from the Office of the Privacy Commissioner to help youth protect their privacy online

ONLINE SHOPPING - HOW TO PROTECT YOURSELF WHEN YOU'RE SHOPPING ONLINE:

USE STRONG AND UNIQUE PASSWORDS: Once again, *strong passwords* are essential, just as they are with email and social media accounts. Never share your passwords with anyone, unless you have designated someone you trust to manage your accounts. Make sure your passwords have at least eight characters. Include numbers, upper and lower case letters, and symbols, and do not use names or dictionary words. At **ConnectSafely.org/passwords**, you'll find tips and information on how to use multi-factor authentication and fingerprint recognition for more advanced security.

DON'T CLICK ON LINKS: in email or on social media from banks, credit card companies, government agencies, or other organizations, unless you're 100% certain they are legitimate. There is a common scam, called *phishing*, where someone sends you a link to what looks like a legitimate website, but it's actually a scam site created by criminals to steal your login or other personal information. Even if the company name is part of the Web address, it could still be a scam. Your safest bet is to type in the Web address like you normally do and if in doubt, call the organization.

BE WARY OF ANY OFFER THAT'S TOO GOOD TO BE TRUE: such as being told you've won a contest that you didn't enter, or you're being offered an incredible price on a vacation or product way below what you'd expect to pay. Be especially careful about offers for low-cost medications or medical coverage.

ONLY SHOP AT REPUTABLE ONLINE MERCHANTS: Be careful about any online merchant that you have never heard of. Many are legitimate but some might be out to steal your credit card number or other financial information, or simply fail to deliver what you've paid for. When in doubt, ask someone familiar with online shopping or do some online research to see if there are reviews or comments about the merchant.

WHEN SHOPPING OR BANKING LOOK FOR SECURE WEBSITES: With an *https* in the browser's address bar. The "s" stands for "secure." If it's just *http*, it's not a secure site. If you shop or bank using a mobile app, be sure it was issued by that company. Look for reviews from others or ask an expert if you're not sure.

USE CREDIT CARDS IF POSSIBLE: Otherwise use debit cards or safe online payment services, such as Paypal. Never send cash, cashier's checks, or money orders. Even sending a personal cheques can be dangerous. It's best to use a credit card because, if there is a dispute, the credit card company will stop the charge or refund your money while they investigate your claim. Debit cards also have protections but sometimes you have to wait to get your money back. Services like Paypal, Android Pay, and Apple Pay also have some protections but credit cards are still the best bet.

BE CAREFUL BEFORE YOU CLICK: There are certain things that you may not be able to undo, such as buying or selling the wrong stock or buying a non-refundable flight or hotel room. Carefully review all transactions before confirming them. If you do make a mistake contact the company right away to see if it's possible to undo it. Many online merchants have a cancellation feature that lets you back out of a purchase, but you must do so promptly. Once an item is ready to be shipped it may be too late to cancel the order. You can often return your purchases, but you're likely to have to pay for return shipping.

Make sure you understand the return policies from online merchants and know all of the charges, including shipping, handling fees, and taxes.

DO SOME RESEARCH BEFORE DONATING TO ONLINE CAUSES: Crowd-funding sites like Kickstarter, Indiegogo, and GoFundMe are great places to be among the first supporters or purchasers of new products, donate to worthy causes and organizations, and even provide financial support for people with a compelling need, but you should proceed with caution. Read all the fine print and do a little research on the person or organization behind the pitch. If they're raising money for a cause, try to find out if it's real, and if they are launching a cool new product, make sure their pitch is realistic. When in doubt, move on.

PROTECT AGAINST IDENTITY THEFT: Never enter your Social Insurance Number (S.I.N.) online unless you know you are at a legitimate site that has a real need for that information, such as applying for a bank account, credit card or loan (from a legitimate financial institution), or getting a credit report. Unless you're sure it's a legitimate site, avoid posting your full birth date and place of birth, and be cautious when asked to enter any other personal information, such as your home address. Legitimate media sites like Facebook and financial institutions may be required to ask for your date of birth. Only disclose credit card numbers to legitimate online merchants. When in doubt, do some research to see what other people and reviewers say about them.

MONITOR YOUR ONLINE FINANCIAL ACCOUNTS: Look for recent activity to be sure that there are no fraudulent charges to your credit, debit, or bank accounts. Check your online investment accounts to make sure there has been no unauthorized activity. If you find something suspicious, report it right away to the financial institution's fraud department or the toll free number on your credit or debit card. Even if you don't bank online, there is still a risk that you could be a victim of fraud. Let the institution know right away if there is an issue. In most cases you are protected against fraud **but you must report it**.

CHARITY SCAMS: Most charities have websites and the option to donate online. That's fine as long as you're sure you're on the right site and that it's a legitimate charity that you support. Be careful if you get an email from what appears to be a charity asking you to make an online donation. If you're not familiar with the organization, check it out at CharityNavigator.org and if you are going to donate online, be certain that you're going to the charity's legitimate site. To be safe, type in the charity's Web address in the browser rather than clicking on a link.

Quick Tips for Online Shopping

(Source: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx)

A FEW CLUES THAT A SHOPPING SITE ISN'T TRUSTWORTHY

- The site looks poorly designed, unprofessional and contains broken web links.
- You can't find an address or phone number for the business.
- Sales, return and privacy policies are hard to find or unclear.
- The back button is disabled. In other words, you get stuck on a page and can't go back.
- You're asked for credit card information anytime other than when you are making a purchase.

HOW TO PROTECT YOURSELF WHEN YOU'RE SHOPPING ONLINE

- Pay by credit card if you can. Do not send cash.
- Be on the lookout for prices that are too good to be true. They're likely counterfeits.
- Don't use public Wi-Fi to shop online.
- Read the privacy policy and find out how your information will be used.
- Don't respond to an email or pop-up message that asks for financial information. Legitimate companies don't ask for this information this way.
- Read your credit card statements and check for unauthorized charges.
- Make sure your firewall is “on”. For example, Windows Firewall is on by default on the latest version of Windows, but make sure it isn't turned off:
    - Open Windows Firewall by clicking the Start button then the Control Panel
    - In the search box type “firewall” then click Windows Firewall
    - In the left pane, click Turn Windows Firewall on or off
- Don't allow auto fill for your passwords or personal information, like your address, and never allow a site to store your credit card information.

Senior Safety: 10 Tips to Avoid Being a Victim of Fraud

(Source: https://www.freedomshowers.com/blog/senior-safety-10-tips-avoid-victim-fraud/**)**

One day you are enjoying a cup of tea at home and the phone rings.

"Hello Grandma, it's your grandson calling. I've been traveling and I lost my wallet and passport. Could you send me some money?" The voice is a bit muffled, and you can't tell which grandson is calling, but you might offend him if you ask. Every caring grandmother would instantly want to help their grandson out of trouble, so you ask him where to send the money too. Unfortunately, the caller is not your grandson, but a scam artist targeting seniors to steal your money. They prey on your caring nature.

Calls like this are happening all the time robbing people of their hard earned money. The frequency of fraudulent transactions are increasing at an alarming rate. The actual number is probably much higher since many victims of fraud don't report it.

Prevention Tips

- Police, judges or legal and government entities will never request that money be sent through money service businesses.
- Never give out personal information to the caller.
- Confirm with other relatives the whereabouts of the family member or friend in question before even considering sending money.
- Never send money through money wire services to persons you don't know personally. Verify the person's identity before you take any steps to help. The money can be picked up anywhere in the world once it is given a transaction number.

10 TIPS TO PREVENT BEING A VICTIM OF FRAUD:

1. My mother always told me, **if it seems too good to be true, it probably is**. Con artists thrive on our desire for quick fixes, miracle cures, and easy money. By offering free products or services, hard to resist bargain prices or big prizes, they lure people into signing up for something they don't want and convince them to pay a fee for shipping or transaction fees. These are most often scams, where they take your "fee" and do not provide the product, service or prize that was promised. **TIP: Ask to receive all offers or prize details in writing, so you can read it over before making any commitments, signing or agreeing to anything. Get a second opinion from someone you trust.**

2. It is okay to say "No, thank you" "Not right now" or "Let me think about it." Legitimate companies and organizations will understand if you request information in writing or want time to do research. **TIP: If you are feeling pressured to sign something or make a payment, hang up or walk away**.

3. Do not release any banking or credit card information, social security numbers, insurance or Medicare numbers over the phone or internet to unsolicited callers or emails. Again legitimate companies will understand your diligence. **TIP: Only share personal and financial information with familiar companies that you have contacted and researched**.

4. Beware of charmers or official sounding callers. Scammers are smart and know that many people can be convinced to hand over money or information if they seem official or are really nice. Banks, police officers or government officials will never require you to pay them over the phone or at the door. If someone tells you that you owe money, tell them you will check your records and contact the offices directly. **TIP: Go to official buildings to make any payments or contact the organization yourself to confirm money owed.**

5. Representatives or repair people will always notify you ahead of time if they are sending someone to your home. **If any stranger knocks on your door, err on the side of caution**. If you aren't expecting anyone, you don't have to open the door. Ask them to come back at a later time, and make sure you are not alone when they do. If you are expecting someone, you should still ask them to show ID. It is okay to ask them to wait outside, while you call the company they are from to confirm whether they have sent someone. This even applies to the police. **TIP: Do not allow unknown or unexpected people into your home.**

6. Take time to read the fine print. Many people don't read the terms and conditions and this could land you in trouble, or commit you to something you don't want. There was an experiment done in London a couple of years ago, where people agreed to the terms and conditions to get free Wi-Fi, without reading it, not realizing what they had actually signed. **Read that article here.** **TIP: Never sign any piece of paper, if you don't fully understand what you are signing.**

7. Check the legitimacy of any company, organization, contest or person who is asking you for information or money, before signing up or paying for anything. Make sure they are registered and or licensed locally. You can check with the Better Business Bureau if there have been previous complaints. Most legitimate companies will have a website, an address, and hopefully some customer reviews, but beware that even that information can be faked. When in doubt, ask around. If you are on social media like Facebook, ask your friends and family if they know the company. **TIP: Make sure you know who you are giving your money or information too, and if they are trustworthy.**

8. Be an informed consumer. Take time to shop around, compare pricing and quality. Ask lots of questions, and double check information that a sales person is telling you. **TIP: Do your research before purchasing. Make sure you are getting what you want and need.**

9. Never wire transfer money to anyone you don't know. Wire transfers are near impossible to trace, track or reverse. It's like sending cash which makes it one of the best ways for a con artist to get away with their scams. Of all the money lost to scammers in 2014, 30% of it was sent through wire transfers. Another 30% of consumers paid scammers with pre-paid gift cards. **TIP: If someone asked you to pay them via a method that is untraceable and non-refundable, be suspicious and do not pay.**

10. If you find you have been a victim of fraud, report it to the police. Too often, fraud does not get reported because people are embarrassed that they "fell for it" or "should've known better". The truth is fraudsters are good at what they do, and if you fell victim to their extremely convincing techniques, you did nothing wrong. If you report it, you might have a small chance of recovering lost funds and perhaps you can save someone else from similar crimes. Also, if you believe someone has gained access to sensitive information, notify your financial institutions to see what can be done to protect you.

What Should I Do if I Think I Have Been Scammed or a Victim of Fraud?

All fraud and scams should be reported, even if you are embarrassed or feel the amount of money is too small to worry about. While you might not be able to get your money back, you can help stop the con artist from scamming other people. You can report all fraud and scams to:

1. The local police in your community: Burnaby RCMP's **Non-emergency (24-hour)** Tel: 604-646-9999 and website: **http://burnaby.rcmp-grc.gc.ca**

2. Canadian Anti-Fraud Centre **Toll Free within Canada: 1-888-495-8501 or visit website: https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/report-fraud.html**

3. **Financial Consumer Agency of Canada (FCAC):** provides information about your rights in dealing with banks and other financial institutions. Tel: 1-866-461-3222 (TTY 613-947-7771, or 1-866-914-6097), Website: **fcac.gc.ca**

4. For more information, visit **Canada.ca/Seniors** or visit your local Service Canada office.

STEPS TO REPORTING A FRAUD, OR A SCAM:

Step 1: Gather all of the information you have about the fraud. This includes documents, receipts, and copies of emails or text messages.

Step 2: Report the incident to your local police. This ensures that they are aware of which scams are targeting their residents and businesses. Keep a log of all your calls and record all file or occurrence numbers.

Step 3: Contact the **Canadian Anti-Fraud Centre**, by phone Tel: 1-888-495-8501
Hours of operation: Mon-Fri from 9:00 am - 4:45 pm (Eastern Time)

Step 4: Report the incident to the financial institution where the money was sent (e.g., money service business such as Western Union or MoneyGram, bank or credit union, credit card company or internet payment service provider).

Step 5: If the fraud took place online through Facebook, eBay, a classified ad such as Kijiji or a dating website, be sure to report the incident directly to the website. These details can be found under "report abuse" or "report an ad."

Step 6: Victims of identity fraud should place flags on all their accounts and report to both credit bureaus, Equifax (**https://www.consumer.equifax.ca/personal/**) and TransUnion (**https://www.transunion.ca/**)

18 Internet Safety Tips for Seniors

(Source: **http://www.vistaspringsliving.com/blog/18-internet-safety-tips-for-seniors**)

GENERAL SAFETY & SECURITY:

1. Make sure your passwords are unique and secure. Use strong passwords that don't include any personal information, and try to avoid dictionary words and common phrases. Many websites recommend a mix of lower and uppercase letters, numbers, and symbols. In addition, never use the same password for more than one account.

2. Use anti-malware software and other protective tools. Be sure that your computer has some sort of trusted security software installed, and set it to automatically update so that you're protected against the latest risks. Ask an expert or trusted tech-savvy person if you're unsure what to install.

3. Don't download unknown attachments and software. Never download documents, images, or software if you don't know and trust the source. Scammers and hackers will often disguise viruses and other malware as "free" software tools or interesting content to download.

4. Consider authorizing a trusted friend or family member to access your accounts. In case of emergency, it can be difficult or impossible for trusted friends and family to access online email, bank, and file storage accounts. Plan ahead and work with an attorney to authorize someone you trust to access your accounts.

EMAIL AND SOCIAL MEDIA:

5. Understand "spam" filters. Spam refers to unwanted, unsolicited emails. Most email providers have spam filters that remove these emails from your main inbox.

6. Use social media privacy settings. Be aware of what you're posting on any social media sites, and use privacy settings to restrict access to your posts to people you trust with personal information.

7. Report any and all instances of abuse. Cyberbullying may be associated with children and teens, but that doesn't mean that adults don't get abused online. Don't respond. Instead, report abuse - both to the platform you're on and to people who can help, and remember that abuse is not your fault.

8. Know the signs of a scam. If it's too good to be true, it usually is. Offers of low-priced or free big-ticket items such as vacations, electronics, and medicines are usually scam attempts. On the other hand, scammers will sometimes send you requests for money from friends' personal accounts; never reply or send funds without first verifying the request with the person in some other way.

MONEY & PURCHASING:

9. Look for secure websites. Whenever you're prompted to enter your payment information into a website, first check that the website is secure. In the URL bar at the top of your internet browser, look for "https://" for a secure site. (The "s" stands for secure.)

10. Understand and avoid phishing attempts. Be wary of links to sites that ask you to make a purchase

or enter your payment information. One common scam, “phishing,” makes a phony site look like a trusted site, then gives your information to the scammer. Look for grammatical errors, spelling mistakes, and URLs that look different than you’re used to. When in doubt, enter the web address you know to be correct directly into the URL bar.

11. Do not enter personal or payment information into an unknown site. On a similar note, be sure to verify the website if you’re going to enter personal or payment information. Look for reviews of online retailers, and in the case of banking or government portals, never respond to requests for information. Banks and government agencies will never solicit passwords, Social Security numbers, or payment information.

12. Monitor your financial accounts. Even when you take every precaution, there is a chance that your payment information may be leaked or stolen from a trusted vendor. Watch your bank accounts and credit cards for unauthorized purchases.

MEETING NEW PEOPLE:

13. Exercise caution. Unfortunately, not everyone on the internet is who they say they are. There are many online opportunities to meet new people, from dating sites to hobby groups and forums, but not everyone is trustworthy. Be cautious when interacting with new people, and don’t give out too much personal information where people can find it.

14. Do not send money to new acquaintances. Similarly to personal information, some people will use the relative anonymity of the internet to get close to their targets, then request money and never be heard from again. Don’t be swayed by stories of personal tragedy or requests for money to visit unless you’re positive of the person’s good intentions.

15. When meeting up in person, be safe. If you choose to meet someone from a dating website or a friend you met online, choose a public place and let a friend or family member know where you’re going and who you’re meeting. You can never be too safe, even if you feel you know the person well.

WELL-BEING & HEALTH:

16. Know fact from fiction. Websites such as news publishers and health advice blogs often make money by attracting visitors to view and click ads on their pages, and will publish sensational headlines to get those views. Not everything published on a website is true, no matter how official it may look.

17. Avoid self-diagnosis and armchair healthcare advice. It’s incredibly easy to look up your symptoms on a search engine and find a list of possible diseases, or a forum discussing a diagnosis. Only a licensed healthcare professional who understands your health background should make diagnoses and prescribe treatments. Attempting to use the internet to do so could mean the condition goes untreated or becomes worse.

18. Follow up with a professional. Of course, not every piece of health advice on the internet is life and death. There are many helpful resources online for nutritional advice, well-being, and fitness, but it’s always good to consult a professional (doctor, health nurse, dietician, and nutritionist) before making any changes that could impact your health, such as a new diet or exercise plan.

By educating yourself, you can stay safe. Here are some other resources to check out:

RCMP’s Seniors Guidebook to Safety and Security - http://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7

How to protect yourself while shopping online: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx

Basic Online Tips & Advice: https://www.stopthinkconnect.org/resources/preview/tip-sheet-basic-tips-and-advice
Online shopping, banking, charity and travel - https://www.connectsafely.org/seniors/
Top 10 tips to protect your inbox, computer and mobile device: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/spam/casl_tips_ind/