BIPT

BURNABY
INTERCULTURAL
PLANNING TABLE

詐騙　欺詐　互聯網安全和網絡欺凌

給青少年　父母和長者的提示

Funded by:

Immigration, Refugees and Citizenship Canada

Finance par :

Immigration, Refugies et Citoyennete Canada

詐騙、欺詐、互聯網安全和網絡欺凌

給青少年、父母和長者的提示

Table of Contents: 目錄

Acknowledgements: 致謝

Intercultural Connections Working Group

跨文化聯繫工作組

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

Translations: 翻譯

Arabic:	Abeer Hattab
Chinese:	Derek Chen
	Tom Su
Farsi:	Sossan Kayoumi
	Nabila Akbari
	Zarif Akbarian
Korean:	Darae Lee
Spanish:	Mary Blanca Battenberg
	Pilar Sain
Tigrinya:	Tigist Dubus Tesfamariam
	Daniel Debesay Michael
	Tedros Gebrengus
	Enbakom Berhane
	Asmait Tekle

Internet Safety Tips for Parents
給父母的互聯網安全提示

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**.**

談論互聯網安全 - 從隱私問題到身份盜用，互聯網上存在危險。兒童和青少年在使用互聯網時需要監督，無論他們是 5 歲還是 15 歲，成年人也需要保持專注。注意安全問題，例如分享行踪，照片和個人信息，將大大有助於保護您的親人。

- How to Structure Homework and Time Online: 如何在線上構建家庭作業和時間：
  https://childdevelopmentinfo.com/family-building/structure-homework-time-online/#.XQgWjTZ8CM8
- **10 Internet Safety and Technology Use Tips for Parents: 給**家長的 10 個互聯網安全和技術使用技**巧**
  https://www.kathleenamorris.com/2019/05/16/internet-safety-parents/
- Internet Safety Advice: Top Tips for Parents: 互聯網安全建議：**給**家長的重要提示：
  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:

無人監督/早期互聯網使用 - 在一項共享希望國際的調查中，八分之一的父母允許他們的孩子從兩歲開始使用互聯網，只有十分之一允許他們的孩子在 10 歲或以上時使用互聯網，（專家的建議）。結果，許多孩子在使用互聯網的同時無人監督。以下是在線保護孩子的方法：

- 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.

監控孩子的在線活動 - 不幸的是，無論父母參與，許多青少年都隱藏或刪除了他們的瀏覽歷史。父母必須勤勞。青少年也有他們的父母可能不知道的電子郵件或社交媒體帳戶。在某些情況下，孩子會說謊他們的年齡來創建這些帳戶。

- 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:
  對於兒童遭受同伴受害的情況, 父母應提供支持，父母可在以下情況下參考"金字塔支持"資源：**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.

手機- 手機非常適合保持聯繫並在緊急情況下使用。 11 至 14 歲的人中約有 69％擁有自己的手機。手機用戶必須了解並註意手機的 GPS 可以顯示用戶的確切地理位置。此外，在網上發布個人手機號碼時要小心謹慎。

- When to Give Your Child a Phone: 什麼時候給孩子電話：
  https://childdevelopmentinfo.com/child-activities/when-to-give-your-child-a-phone/#.XQgW-zZ8CM8
- Cellphone Safety Tips: **手機安全提示**
  https://protectkidsonline.ca/app/en/info_phone_safety
- The First Cell Phone: Rules for Responsibility: **第一部手機：責任規則**：
  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:
  家長監控應用程式 APP，**用於跟踪加拿大以及境外的手機**：
  https://pumpic.com/parental-monitoring-app-canada.html

Talking About Internet Safety with Your Kids

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.

在線欺凌 –
有幾個匿名會話應用程式和網站，其中可能會發布（匿名）有關他人的問題或信息。這些匿名應用程序，包括Whisper，YikYak和Ask.FM，都很危險，因為眾所周知它們會促進欺凌行為。欺騙他們的匿名身份，惡霸輕易嘲諷，挑逗，並讓其他人失望。重要的是始終保持並報告任何濫用，無論是懷疑還是證實。

- PREVNet: Promoting Relationships and Eliminating Violence Network is Canada's authority on research and resources for bullying prevention.
  PREVNet：促進良好關係和消除暴力網絡是加拿大在欺凌預防研究和資源方面的權威。
- What to do if your child is being Cyberbullied?: 如果您的孩子被互聯網欺凌怎麼辦？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
  WITS計劃將學校，家庭和社區聚集在一起，創造相互支持環境，幫助兒童應對欺凌和同伴受害
- RCMP's Centre for Youth Crime Prevention: provides Canadians with age appropriate crime prevention information and tools to prevent youth crime and victimization.
  皇家騎警青年預防犯罪中心：為加拿大人提供適合其年齡的犯罪預防信息和工具，以防止青少年犯罪和受害。
- 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.** 兒童幫助熱線，是父母及其子女的良好資源。它提供諮詢服務·現在需要幫助嗎？傳短訊到686868與義工Crisis Responder 24/7聊聊。
  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.

赤裸露骨照片 –
研究表明，七分之一的青少年拍攝了自己的裸體或半裸照片，其中一半以上的照片是通過互聯網與其他人分享的。重要的是要注意，一旦在互聯網上發布信息，可能無法完全刪除它。

- Cybertip.ca: Canada's tip line to report the online sexual exploitation of children.
  Cybertip.ca:加拿大的提示熱線報告了對兒童的在線性剝削。

- 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.

在線購物，身份盜竊，上網搜尋– 在網上搜尋時要小心。您的網絡活動歷史記錄會不斷被跟踪。造訪不安全或不適當的網站可能會危及您的個人和財務信息或損害您的電腦。在所有電腦上安裝足夠的安全和防病毒軟件非常重要。應始終使用安全連接，永遠不要使用公共電腦，並確保網站在網上下訂單之前是合法和安全的。遵循這些預防措施將為用戶提供更安全的體驗。兒童往往是身份盜竊的受害者。事實上，與成年人相比，18 歲以下的兒童被盜身份的可能性要高 51 倍。犯罪分子針對兒童，因為他們擁有乾淨的信用記錄，並且如先前報導的那樣，經常在網上發布個人信息。

- How to find a child's credit status, step-by-step instructions on how to check your child's credit report: 如何查找孩子的信用狀況，檢查孩子的信用狀況報告分步說明：
  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.

電子遊戲 – 近年來電子遊戲已經發展迅速。有了許多遊戲選項，家長需要注意大多數遊戲設備可以直接將兒童連接到互聯網和其他玩家。幸運的是，大多數遊戲設備都有家長控制和安全設置。家長應該限制孩子玩電子遊戲的時間。

- Recommended online educational games to teach children & teen in grades 4 to 8 about how to be safe when using the internet:
  建議的在線教育遊戲，教導 4 至 8 年級兒童和青少年如何在使用互聯網時保持安全：
  http://mediasmarts.ca/digital-media-literacy/educational-games

Talking about Internet Safety with your kids: 與您的孩子談論互聯網安全：

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.
保密您的個人信息 – 未經父母/監護人的許可，不要透露您的姓名，電話號碼，學校或地址。

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.
Facebook 和 Twitter 等大多數社交網站都會讓您選擇誰可以查看您的貼文。要求成年人幫助您更改隱私設置。

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"!
請記住，您在社交媒體上分享的任何內容 – 即使設定為隱私 – 都可能被其他人看見。在點擊“發布”或“發送”之前，請務必三思而後行！

4. If you see anything inappropriate online, ask a parent or trusted adult for advice. Remember, it's not your fault you saw this!
如果您在網上看到任何不當內容，請向家長或可信賴的成人諮詢。記住，您看到這個不是您的錯！

5. If someone sends you something rude over email or social media, DO NOT RESPOND – instead, speak to a responsible or trusted adult.
如果有人通過電子郵件或社交媒體向您發送粗魯的內容，請勿回覆 – 可向負責任或信任的成年人交談。

6. If you're sharing photos or videos that have other people in them, always ask for permission first.
如果您要分享其中包含其他人的照片或視頻，請務必先獲得許可。

7. Never buy something online or download anything without permission from a parent/or guardian. 未經父母/監護人許可，切勿在線購買或下載任何內容。

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!
永遠不要同意與您在網上認識的人親自見面。請記住，那個人可能不是他們所說的！

9. Keep your passwords SECRET! Not even your BFFs need to know!
保持密碼秘密！甚至您最好的朋友都不需要知道！

10. Stand up against Bullying – don't gossip or humiliate anyone! If you want more information about cyber-bullying or bullying in general,
站起來反對欺凌 – 不要閒聊或羞辱任何人！如果您想了解有關網絡欺凌或欺凌的更多信息，請造訪：

Visit： http://www.family.ca/standup/

Tip Sheet for Adults: Scams, Fraud and Cyber Safety

給成年人提示：騙局，詐騙和網絡安全

FRAUDULENT CALLS: 欺詐電話：

Beware of callers falsely claiming to represent a trusted company or organization.
謹防號稱受信任公司或組織的欺詐電話。
https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdlnt-clls-en.aspx

WHAT TO DO IF YOU GET A CALL: 如果您接到這類電話該怎麼辦：

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.
如果您接到這樣的電話，請掛斷電話。永遠不要遠程連接您的電腦來接聽未經請求的電話。如果您不確定，請聯繫公司或組織的客戶服務中心。我們強烈建議加拿大人向加拿大反欺詐中心報告此類欺詐事件，網址為：**http：//www.antifraudcentre-centreantifraude.ca** 或致電 1-888-495-8501。

ONLINE SCAMS AND FRAUD: 網路騙局和欺詐：

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.
要知道得獎或促銷廣告是真實的還是互聯網騙局或欺詐並不總是容易的。這些優惠可能看起來好得令人難以置信 - 而且可能會如此。安全的關鍵是看穿詐騙的技術及跡象。
https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx

WHERE CAN I FIND OUT MORE? 我在哪裡可以找到更多？

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.
在網上有許多關於欺詐和詐騙的資訊。”加拿大金融消費者機構網站”提供有關您與銀行和其他金融機構交涉權利得資訊。

要訂購本出版物，或在您所在省份或地區尋找電話號碼的幫助，請致電1 800 O-Canada（1-800-622-6232），TTY：1-800-926-9105。

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

如果我認為我已經被詐騙了，我該怎麼辦？

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. 加拿大最常見的詐騙之一是網絡釣魚或掠奪騙局，騙子構成企業或政府組織。例如，聲稱來自加拿大稅務局的騙局。有時候，被鎖定的受害者被告知他們欠費，如果他們不付錢，加拿大皇家騎警就會逮捕他們。有時，目標受害者被告知他們可以"點擊鏈接接受退款"。有些人只是被告知要查看鏈接以查看其信息的變更，或填寫表格及其個人信息。

WHAT SHOULD I DO IF I THINK I HAVE BEEN SCAMMED? 如果我認為我已經被詐騙了，我該怎麼辦？

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.

如果您不確定該消息是否合法，請不要回覆！訪問該組織的網站並直接致電他們以驗證您收到的信息。由於我們許多人收到了要求繳納稅款的欺詐性 CRA消息，CRA提供了以下建議：

•CRA 從不通過電子郵件或文本要求提供個人信息，
•CRA也不要求比特幣或禮品卡付款。

如果您收到來自CRA的電話，短信或電子郵件，或者欠退款或福利金，登錄或註冊"我的帳戶"或"我的公司帳戶"以驗證您的納稅身份，或致電 CRA的個人收入稅務諮詢熱線 1-800-959-8281。

If you fall victim to a scam, there may be a number of steps to take:
如果您成為騙局的受害者，可能需要採取以下措施：

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.

1. 向您所在社區的當地警方報告欺詐行為：BurnabyRCMP的非緊急情況（24小時）電話：604-646-9999和網站：http：//burnaby.rcmp-grc.gc.ca
2.如果您的社會保險號碼被盜，請撥打1-800-206-7218聯繫加拿大服務部報告。

3. 向加拿大皇家騎警隊的加拿大反欺詐中心報告騙局。您將被要求使用登錄合作夥伴（即您的銀行）或GCKey（就像您登錄 CRA帳戶一樣）。報告詐騙時，這可確保您自己的安全。您也可致電1-888-495-8501聯繫反欺詐中心。

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**.

騙子在假裝代表銀行或信用卡公司時使用類似的策略。例如，您可能會收到來自您未處理的銀行的電子郵件或文本，要求您查看您的對帳單。當消息不是來自您自己的銀行時，很容易識別網絡釣魚或躲避。但是，如果您擔心它可能來自您的銀行，請不要回覆此消息 – 直接通過電話或親自聯繫銀行或登錄您的在線銀行網站或應用程序（當然是使用安全互聯網連接）驗證它是否真實。並且不要忘記向您的銀行報告網絡釣魚/瀏覽消息。
有關其他網絡事件和報告的更多信息，請訪問加拿大網絡安全中心。

FOLLOW GET CYBER SAFE ON TWITTER, FACEBOOK AND INSTAGRAM.

以下是在Twitter，FACEBOOK 和 INSTAGRAM 上讓網絡安全。

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

在智能設備上保護隱私的 *5* 種方法（智能手機/平板電腦/智能手錶）

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:

這些提示適用於您在家中連接到Internet的任何設備。雖然連接設備（也稱為“智能設備”）很有趣並且讓我們的生活更輕鬆，但它們也為駭客提供了訪問個人和私人信息的機會。按照以下提示採取措施保護您和您的家人：

1. **SECURE YOUR HOME WI-FI NETWORK:** 保護您的家庭 WI-FI 網絡：

   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.

   智能設備使用Internet 發送和收集數據。如果您的家庭Wi-Fi 連接不安全，則您的數據不安全！使用Wi-Fi 時，您應具備的最低安全性是無線加密和密碼保護。在您的無線設置下，確保您的路由器啟用了WPA2 加密。然後，使用複雜密碼鎖定您的無線網絡。強密碼包括大寫和小寫字母，數字和特殊字符。 如果您是高級用戶，請在Wi-Fi 網絡上創建單獨的網絡區域以連接智能設備。這稱為“設備隔離”，其功能類似於“訪客 Wi-Fi”網絡。在移動中使用智能設備時，僅連接受信任的受密碼保護的網絡，並關閉自動搜索Wi-Fi 網絡的設置。

2. **TURN OFF GEOLOCATION WHEN NOT IN USE:** 在不使用時關閉地理位置：

   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.

許多智能設備都有使用地理定位來提供服務的應用，例如健身追踪或地圖。如果應用程序可以看到您的位置，那麼黑客也可以。在設備的設置中，請在不使用時關閉地理位置。

3. **BEFORE INSTALLING APPS, UNDERSTAND THE APP'S PRIVACY POLICY AND TERMS OF USE:** 在安裝應用程序之前，了解應用程序的隱私政策和使用條款：
   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.

   所有應用都具有隱私設置，可幫助控制誰可以查看您的信息以及他們看到的內容。自定義這些隱私設置，以隱藏個人信息，如全名和聯繫人詳細信息。此外，要警惕要求不必要或過多信息的應用程序。仔細查看權限，不要只為所有內容單擊“允許”。

4. **DISABLE MICROPHONES AND CAMERAS WHEN NOT IN USE:** 不使用時關閉麥克風和相機
   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.

   大多數遊戲耳機，智能電視，智能手錶和智能揚聲器都配有麥克風和/或攝像頭。如果不安全，您的設備可能會傳輸您不想要的信息。不使用時，請關閉相機並將麥克風靜音。

5. **CREATE USERNAMES THAT DON'T CONTAIN IDENTIFYING INFORMATION:**
   用戶名不包含識別信息：
   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.

   過多分享可能會使您的隱私受到威脅。在為您的設備（或遊戲或應用）設置登錄信息時，請確保您的用戶名不包含識別信息，例如您的姓名，年齡，位置或聯繫信息。

6. **BE SMARTPHONE SAVVY:** 手機專家
   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**.

   智能手機可以跟踪您的位置並顯示有關您的信息，包括您的聯繫人。小心只下載和使用信譽良好的應用程序，並確保密碼（或指紋）保護您的手機。了解如何使用工具查找或刪除丟失手機中的個人數據。您可以在 ConnectSafely.org/cellphone-safety-tips上找到更多信息。

7. **SECURE YOUR INTERNET ROUTER:** 保護您的互聯網路由器：

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.

您家中可能有一個小設備，稱為路由器或寬帶調製解調器，可將您連接到Internet。該設備有密碼和用戶名，有時密碼很容易猜到。路由器可能很難配置，因此如果您有疑問，請聯繫專家或您的網路服務提供商，獲取有關如何更改密碼的建議。

8．**PROTECT YOUR DEVICES:** 保護您的設備:

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**.

通過確保它們受密碼保護，並且在電腦上，確保您具有良好的安全性和防火牆軟件。如果您需要幫助，請與知識淵博的朋友或家人，或您的互聯網服務提供商或移動商聯繫。SHAW和其他一些互聯網服務提供商可能會提供免費的防病毒軟件，或者您可以從信譽良好的公司購買或獲取免費的安全軟件，例如**ConnectSafely.org/securityvendors**上列出的公司。

OTHER RECOMMENDED RESOURCES FOR ADDITIONAL TIPS VISIT:

其他推薦的額外提示資源：

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

FightSpam.gc.ca：幫助加拿大人和企業避免垃圾郵件和其他電子威脅

青年隱私：隱私專員辦公室提供的信息和工具，幫助青少年保護他們的在線隱私

Online Shopping – How to Protect Yourself When You're Shopping Online:

網上購物–如何在網上購物時保護自己

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.

使用牢固和特殊的密碼：再次強調，牢固的密碼是很重要的，就像電子郵件和社交媒體的帳號一樣。任何時候都不要把密碼告訴任何人，除非那個人您信任並願意把您的帳戶放心交付給他管理。密碼最少需要有八個位元組，其中包括數位、大寫及小寫字母以及特殊符號。不要使用名字或單詞。在這個 ConnectSafely.org/passwords 網站，您可以找到如何使用多重鑒定和指紋識別而達到高級安全水準的技巧。

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.

不要點選連結：除非您能 100%肯定是合法的，在電子郵件或社交媒體中收到銀行、信用卡公司、政府機構或其它組織的連結，千萬不要點擊。這是一種很常見的 "釣魚' 騙局：當有人發給您一條看似正常的連結，但實際上它有可能是一個不法分子創建的欺詐網站，一旦您點擊了連結，您的登錄密碼和個人資訊就可能會失竊。有時儘管在網址中包含了公司名，仍然有可能是騙局。最安全的做法是像平常一樣，自己輸入網址而不是點選連結。如有任何懷疑，應致電相關公司查詢。 **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.

提防那些令人難以置信的好事：比如有人告訴您說您無端端中獎了，或者說您贏了一個大獎送您去度假或者讓您低價購買一個產品。特別小心那些低價醫藥產品或者醫保專案的促銷。

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.
只在聲譽好的網上商家購物：小心任何您沒有聽過的商家。有很多是正規的，但有些可能就是為了盜取您的信用卡號碼或其它金融機構的資訊，或者就是無法交付您支付的商品。有任何懷疑的時候，向熟悉網上購物的人諮詢，或者上網調查看看別人對商家的評價和評論。

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.
網上購物或使用網上銀行時須留意安全的網址：在流覽器的位址欄裡輸入https，其中的 s 代表安全的意思。如果只是http，就不是一個安全的網站。如果您使用手機購物或手機銀行軟體，確保軟體是那家公司自己發佈的。如果您不確認，參考別人的評價或者請教專家。

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.
如果可能請使用信用卡支付：否則使用借記卡或者安全的網上支付方式，比如貝寶 Paypal。從不應該寄現金，銀行支票或匯票。甚至個人支票也可能有危險。最好使用信用卡，因為一旦有爭議，信用卡公司可以停止這筆交易，在調查索賠時已經可以退款。借記卡也有保護，但有時您要等退款。貝寶、安卓支付、蘋果支付也有保護，但信用卡仍然時最好的選擇。

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.
點擊前小心謹慎：有些事情您點擊以後也許就不能撤回，例如下單、賣錯股票又或者購買了不能退款的機票或酒店。所有的交易在確認之前應仔細檢查。萬一出錯請立即聯繫對方公司看是否可以撤回重來。許多網上商家有取消的特別功能，令您可以撤銷購買，但您必須動作迅速。一旦商品已經準備發運，再想取消訂單就太遲了。通常您可以退貨，但您很有可能要支付退貨的運費。

Make sure you understand the return policies from online merchants and know all of the charges, including shipping, handling fees, and taxes.
確保您理解網上商家的退貨條款，知道所有收費項目，包括運費、手續費和稅費。

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.

網上捐贈前請先做好調查：如 Kickstarter, Indiegogo, GoFundMe 這些眾籌資金的網站是購買新產品、捐贈給有價值的目的和組織、以及為有需要的人提供資金支援的好地方，但也需要特別小心。仔細閱讀所有的資訊，並對提案的相關人士或機構做些調查。如果他們籌集資金是為了某種善舉，嘗試查查看是否真實。如果他們在推出一款很酷的新產品，確保項目切合實際。有疑問的時候不必繼續投資。

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.

做好盜竊身份的保護：不要在網上輸入您的 SIN 社保號碼，除非您知道這個網站的合法性，它確實有需要這個資訊，比如您在向一個合法的金融機構申請銀行帳戶、信用卡、借款或者信用記錄。除非您肯定網站是合法的，避免公開您的生日和出生地資訊，特別小心叫您輸入任何個人資訊，比如您的家庭位址。一些合法的社交媒體（如臉書）也許會要求您輸入生日。只向合法的網上商家提供信用卡號碼。一旦有疑問，調查看看其他人有什麼評價。

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**.

監控好您的網上財務帳戶：查看最近的帳戶交易活動，確保您的信用卡、借記卡或銀行帳戶沒有欺詐行為的記錄。檢查您的網上投資帳戶，確保沒有未經授權的交易活動。如果您發現有可疑情況，馬上向該金融機構報告，或者打信用卡或借記卡上的免費電話。即使您不使用網上銀行，您仍然有風險成為欺詐行為的受害者。馬上報告有問題。多數情況下您會受到保護免受欺詐，但您必須報告您遇到的問題。

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.

慈善騙局：大多數慈善機構都有網站，您可以選擇在網上捐款。只要您確保您在正確的網站，而且您支持的善舉是正規的，那就沒有問題。特別小心那種貌似慈善機構叫您在網上捐款的電子郵件。如果您不熟悉相關機構，可以在 CharityNavigator.org 這個網站上查詢。如果您打算在網上捐款，確保您是在該慈善機構的正規網站上。以往萬一，應在流覽器裡輸入公司網址，而不是點選連結。

Quick Tips for Online Shopping

網上購物的快速提示

(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 一個不可信的網上購物網站暴露的幾點線索提示

- The site looks poorly designed, unprofessional and contains broken web links. 網站看起來設計很差，不專業，而且網址有些破碎的連結。
- You can't find an address or phone number for the business. 無法查找到公司位址或電話。
- Sales, return and privacy policies are hard to find or unclear. 很難找到銷售、退貨以及隱私條款，或者非常不清晰。
- The back button is disabled. In other words, you get stuck on a page and can't go back. 返回鍵被禁用。也就是說，您卡在一個網頁裡無法返回。
- You're asked for credit card information anytime other than when you are making a purchase. 不是在付款的時候讓您提供信用卡的資訊。

HOW TO PROTECT YOURSELF WHEN YOU'RE SHOPPING ONLINE 網上購物時如何保護自己

- Pay by credit card if you can. Do not send cash. 如果可以，應該使用信用卡支付，不要郵寄現金。
- Be on the lookout for prices that are too good to be true. They're likely counterfeits. 特別小心那些難以置信的低價。很有可能是假貨。
- Don't use public Wi-Fi to shop online. 不要使用公眾場所的WiFi 進行網上購物。
- Read the privacy policy and find out how your information will be used. 閱讀隱私條款，瞭解您的資訊會被如何使用。
- 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. 不要回復問您要金融資訊的郵件或者彈窗資訊。正規網站從來不會這樣做。
- Read your credit card statements and check for unauthorized charges. 仔細檢查您的信用卡結算單看有沒有未經授權的收費。
- 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: 確保防火牆是 “打開” 狀態。比如，最新版本的 Windows 系統裡防火牆的預設狀態應該是打開的，確保不要是 “關閉” 狀態：

- Open Windows Firewall by clicking the Start button then the Control Panel 在 Windows 系統裡，點擊“開始”鍵，在“控制台”裡可以打開防火牆。
- In the search box type “firewall” then click Windows Firewall 在“桌面搜索”欄輸入“firewall”就可以打開防火牆。
- In the left pane, click Turn Windows Firewall on or off 在左邊窗格裡可以打開或關閉防火牆。

- 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. 不要自動輸入您的密碼及個人資訊（比如位址）。不要讓任何網站保存您的信用卡資訊。

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

長者安全：避免成為欺詐受害者的 *10* 個秘訣

資訊來源：

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.

有一天您在家裡喝茶，電話響了。

"奶奶，您好。我是您孫子。我在旅遊的時候錢包和護照丟了。您能寄錢給我嗎？" 因為聲音聽不清楚， 您不知道到底是哪個孫子給您打電話，如果您問他，可能您還覺得會得罪了他。每個奶奶知道孫子有麻煩的時候肯定第一時間想提供幫助，所以您就問他往哪裡寄錢。不幸的是，打電話給您的並不是您的孫子，而是一個專門騙老人家錢的騙子。他們就是利用您的好心令您上當。

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.
類似這樣的電話詐騙經常發生，許多人辛辛苦苦掙回來的血汗錢就這樣沒了。這種欺詐行為正以一種令人擔心的速度遞增。實際發生的數量很可能比我們知道的更多，因為並不是所有的受害者都會申報。

Prevention Tips 預防措施

- Police, judges or legal and government entities will never request that money be sent through money service businesses. 員警、法官或法律及政府機構從來不會要求匯款。
- Never give out personal information to the caller. 接到類似電話，絕不提供個人資訊。

- Confirm with other relatives the whereabouts of the family member or friend in question before even considering sending money. 在考慮匯款之前向其他親戚朋友瞭解情況。
- 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. 絕不向不認識的人匯款。在您提供任何幫助以前，確認對方的身份。一旦提供了交易號碼，款項可以在全世界任何地方被取走。

10 TIPS TO PREVENT BEING A VICTIM OF FRAUD: 防止成為騙局受害者的十個招數:

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.** 媽媽總是告訴我，**如果有些事情看起來好的不像真的，那很有可能就不是真的**。騙子就是利用我們對捷徑、奇跡和賺快錢的渴望來下手。他們給人提供免費的產品或服務、難以拒絕的特價或獎品，吸引人去登記購買根本不需要的東西，然後說服人支付運費或交易手續費。這些多數情況下是騙局，因為他們收了錢後不會遵守承諾提供相關產品、服務或者獎品。**提示：請對方書面提供具體細節，這樣您就可以在下定決心簽訂任何協定之前仔細閱讀。可以找一個您信任的人尋求意見。**

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**. **完全可以回答"不要，謝謝"** "現在不考慮"或者"讓我考慮一下"。正規的公司會理解您需要書面的資訊或者需要時間去調查。**提示：如果對方向您施壓要求您簽署任何檔或者付款，請掛斷電話或者離開。**

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**. 如果有人通過電話或者網上向您推銷，**不要向對方透露任何銀行或者信用卡資訊**、社保號碼、保險或者醫保號碼。再次強調，正規的公司會理解您的。**提示：只向您聯繫過的熟悉的公司提供個人或者金融信息。**

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. 小心口甜舌滑或者聽起來像官方的電話。騙子很狡猾，他們知道如果他們在電話裡聽起來很官方或者很友好，很多人也許會相信他們，向他們匯款或者提供資訊。銀行、員警、或者政府官員從來不會要求您在電話裡或者在您家門口付款。如果有人說您欠款，告訴他們您會查看您的記錄並直接聯繫相關機構。**提示：去相關機構的官方辦事地點繳費，自己聯繫相關機構確認是否欠費。**

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.** 公司代表或者維修人員如果派人到您家之前一定會提前通知您。**如果有任何陌生人敲門，寧願犯錯也要特別小心謹慎。**如果您並沒有期待任何人來訪，您不一定非得開門。請他們以後再來，並確保他們再來的時候您不是一個人在家。假如您在等人來，您應該請對方出示證件。您可以讓他們在門外等待，同時打電話給相關公司確認是否派了人來訪。對員警都甚至可以這樣做。**提示：不要讓任何非請自來的人進入家門。**

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. 花點時間閱讀文檔。**許多人根本沒有閱讀條款就簽名，結果導致許多後續的麻煩，或者把自己陷入無法脫離的境地。兩年前在倫敦曾經有人做過一個實驗，很多人為了使用免費 Wi-Fi 沒有閱讀就同意了登錄條款，根本沒有意識到他們到底簽名同意了什麼。**可以點擊此連結閱讀該文章。提示：如果您沒有完全明白您簽名同意的條款，不要簽署任何文檔。**

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.** 如果有任何公司、組織、比賽或個人向您索取個人資訊或金錢，在簽署任何文檔或付款之前應該**查清楚是否正規**。確認對方有注冊或有本地執照。您可以在 Better Business Bureau 查詢之前是否有過投訴。大多數正規的公司都有網頁、地址以及顧客的評論，不過小心這些信息也一樣可以造假。當有疑問的時候，問問周圍的人。如果您使用臉書這種社交媒體，可以向親戚朋友瞭解看他們是麼偶認識該公司。**提示：確保您提供信息或付款給您瞭解並信任的公司。**

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. 做個精明的消費者。**花時間在不同

的商家比較價格和質量。銷售代表告訴您的事情可以多提問題，重複確認。**提示：在購買商品之前先做好調查，確保您買的商品是您需要的。**

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. 絕不電匯款項給任何您不認識的人。**就像直接寄現金一樣，電匯很難追蹤、跟進或撤回，所以電匯是騙子最喜歡的收錢方式。2014 年所有的金錢損失的詐騙案件中，30%的付款方式都是電匯，還有 30%的消費者給了騙子預付的購物卡。**提示：如果有人讓您使用一種無法追蹤並無法退款的方式付款，應持懷疑態度並拒絕付款。**

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. 如果您發現您是欺詐行爲的受害者，請向警方報告。很多時候，欺詐案件並沒有向警方報告，因爲很多人覺得自己被騙很不好意思。事實是騙子精心設置了騙局，再通過花言巧語，所以您上當也很正常。如果您報警了，也許您還有點機會挽回損失，又或者可以令其他人免受同類型案件的欺騙。同時，如果您覺得別人也許獲取了您的敏感信息，應馬上通知您的相關金融機構看看是否有任何保護您的措施。

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

如果我認爲被騙或者成爲欺詐案件的受害者時應做什麼？

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: 所有的欺詐和騙局都應該上報，即使您覺得不好意思或者認爲金額太小不值得擔心。也許您無法把錢拿回來，但您可以幫助阻止騙子繼續向別人騙錢。您可以上報給以下機構：

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** 社區本地警察局：本那比市皇家騎警的 24 **小時非緊急**電話： 604-646-9999 網址： **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** 加拿大反欺詐中心 **加拿大國內免費電話: 1-888-495-8501 網址: 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** **加拿大消費者金融機構可以向您提供與銀行和其它金融機構打交道的資訊。**電話： 1-866-461-3222 (TTY 613-947-7771, or 1-866-914-6097), 網址： **fcac.gc.ca**

4. For more information, visit **Canada.ca/Seniors** or visit your local Service Canada office. 要瞭解更多資訊，請查看網站 **Canada.ca/Seniors** 或訪問加拿大本地服務機構。

STEPS TO REPORTING A FRAUD, OR A SCAM: 報告欺詐或騙局的步驟：

Step 1: Gather all of the information you have about the fraud. This includes documents, receipts, and copies of emails or text messages.
第 1 步：收集所有關於該欺詐案件的信息，包括文件、單據、郵件或手機短訊。

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.
第 2 步：向當地警方上報。這樣可以讓警方瞭解有什麼針對當地居民或商業的騙局。記錄您的電話及所有的文件號碼。

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)
第 3 步：聯係**加拿大反欺詐中心**, 電話： 1-888-495-8501 營業時間：周一至周五上午 9 點至下午 4:45（東部時間）。

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).
第 4 步：向相關金融機構上報款項匯到哪裏（比如通過西聯或速匯金等公司、或通過銀行、信用合作社、信用卡公司或網絡付款的服務）。

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."
第 5 步：如果欺詐行爲發生在網上，比如通過臉書、易趣、Kijiji 這種分類廣告網站、又或者約會網站，確保向該網站報告。具體可以點擊“報告問題”或“報告廣告”等。

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/**)
第 6 步：身份欺詐案件的受害者應向信用局、Equifax (**https://www.consumer.equifax.ca/personal/**) 和 TransUnion (**https://www.transunion.ca/**) 報告賬戶的問題。

18 Internet Safety Tips for Seniors

針對長者的 *18* 招互聯網安全秘訣

GENERAL SAFETY & SECURITY: 一般安全問題

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. 確保您的密碼是獨一無二並安全的。使用强力的密碼，不要在密碼內包含任何個人信息，並盡量避免使用詞典裏常用的單詞和短語。許多網站建議使用大小寫字母、數字和特殊符號結合的密碼。另外，不要在多個賬戶裏使用相同的密碼。

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. 使用反惡意軟件以及其它的保護工具。確保您的電腦安裝了可信的安全軟件，並設置了自動更新，這樣您的電腦在新風險下仍然可以受到保護。如果您不知道應該安裝什麼軟件，請向專家或懂電腦的人請教。

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. **不要下載任何不明的附件或軟件。**如果您不知道或者不信任來源，不要下載任何文件、圖片或軟件。騙子或者黑客通常會把病毒和惡意軟件僞裝成"免費"的軟件或者有意思的內容引誘您下載。

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. 考慮授予給一個您信任的朋友或家人權限進入您的賬戶。萬一有緊急情況，您信任的朋友或家人都很難甚至不可能進入您的網上賬戶，如郵箱、銀行和文件存儲等。提前計劃讓律師協助您授權給人進入您的賬戶。

EMAIL AND SOCIAL MEDIA 電子郵件和社交媒體:

5. Understand "spam" filters. **Spam refers to unwanted, unsolicited emails. Most email providers have spam filters that remove these emails from your main inbox.** 瞭解"垃圾郵件"的過濾設置。垃圾郵件指那些不想要、不請自來的郵件。**大多數電子郵箱都有過濾設置可以把那些垃圾郵件從收件箱移除。**

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. **使用社交媒體的隱私設置。**小心您在任何社交媒體上發佈的任何帖子，使用隱私設置限制除了您信任的人外，任何人都不可以查看您的貼子和個人信息。

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. **報告任何欺凌問題。**網絡欺凌也許和青少年相關，但並不意味著不會發生在成年人身上。不要回應，而應該向網絡平臺以及可以幫助這些人的機構報告。記住欺凌問題不是您的錯。

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. **知道騙局的跡象。**如果好得難以置信，通常都是騙局。超低價或免費的大獎，如旅游、電子及醫藥產品，就是騙子經常使用的手段。另一方面，騙子又是會使用朋友的個人賬戶向您要錢，在沒有親自向朋友確認之前絕不回復及匯款。

MONEY & PURCHASING 金錢及購物:

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.) **查找安全的網站。**任何時候出現彈窗需要輸入您的付款信息時，首先查看網頁是否安全。在網絡瀏覽器的輸入欄裏查找是否有 https://，其中的 s 代表安全。

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. **瞭解並避免被釣魚。**小心任何鏈接點擊后鏈接到網站叫您購買任何任何東西或輸入付款信息。一種常見的騙局就是把一個"釣魚"網站做的像一個可信的網站，您的信息輸入以後就會被騙子獲取。查看是否有任何語法錯誤、拼寫錯誤或者看起來和平時不一樣的網址。當有疑問時，應該在地址欄直接輸入您知道的正確網址。

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. **不要在不明網站輸入任何個人信息或付款信息。**同樣，如果您準備輸入個人或付款信息，確保檢查網站是否正確。查看網上商家的評價，在銀行或政府主頁，絕不回復向您索要個人信息的要求。銀行和政府機構從來不會索要的您密碼、社保號碼或付款信息。

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. **監控您的金融賬戶。**即使您非常小心謹慎，您的付款信息仍然有可能在可信的商家被泄露或者被盜取。監控您的銀行賬戶和信用卡賬單看有沒有任何未經授權的交易記錄。

MEETING NEW PEOPLE 與不認識的人見面:

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. **特別小心。**可惜網上不是每個人都是他自稱的人。網上有很多認識新朋友的機會，比如在約會網站、興趣小組和論壇，但不是每個人都值得信任。與不認識的人打交道的時候應特別小心，不要透露太多個人信息給別人找到。

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. **不要匯款給新認識的人。**與個人信息類似，有些人利

用互聯網相對的匿名屬性去接近他們的目標，騙錢成功后您就再也找不到他們了。不要被那些悲慘的故事打動而去送錢，除非您確定真的是好人在做好事。

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. **見面時注意安全。**如果您要和在約會網上認識的人或網友見面，請選擇公衆場所，並讓朋友或家人知道您去哪裏和誰見面。注意安全總不會有錯，即使您覺得您已經很熟悉對方了。

WELL-BEING & HEALTH 幸福和健康:

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. 知道現實和虛構的區別。類似新聞發佈和健康指南的博客通常通過吸引訪問者瀏覽並點擊廣告掙錢，發佈轟動的頭條吸引人去查看。并不是所有發佈在網上的信息都是真實的，不論看起來有多官方。

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. 避免自己給自己診斷，不要聽信輪椅健康建議。很容易在搜索引擎搜索您的症狀然後找到一系列有可能的疾病，或者討論診斷的論壇。只有持牌的保健專業人士并瞭解您的健康背景可以做出診斷并開藥給您。在網上自己嘗試意味著病情拖延甚至惡化。

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. 與專業人士跟進。當然，并不是網上所有的健康建議都是關係生死的。網上有很多關於營養、健康及體質的資源都很有幫助，但在做出任何可能會影響健康的改變（比如新的飲食或運動計劃）之前，最好還是向專業人士（如醫生、護士、飲食學家和營養學家）咨詢。

By educating yourself, you can stay safe. Here are some other resources to check out: 通過教育您自己，您可以保持安全。以下列舉了其他資源供參考：

RCMP's Seniors Guidebook to Safety and Security 皇家騎警的長者安全指南- http://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7

How to protect yourself while shopping online 如何在網上購物時保護自己: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx

Basic Online Tips & Advice 上網的基本提示和建議: https://www.stopthinkconnect.org/resources/preview/tip-sheet-basic-tips-and-advice

Online shopping, banking, charity and travel 網上購物、銀行、慈善和旅游- https://www.connectsafely.org/seniors/

Top 10 tips to protect your inbox, computer and mobile device 保護您的郵箱、電腦和手機的 10 個提示: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/spam/casl_tips_ind/