BIPT

BURNABY
INTERCULTURAL
PLANNING TABLE

欺诈、互联网安全和网络欺凌

给青少年、父母和长者的提示

Funded by:
Immigration, Refugees and Citizenship Canada

Finance par :
Immigration, Refugies et Citoyennete Canada

诈骗、欺诈、互联网安全和网络欺凌

给青少年、父母和长者的提示

Table of Contents 目录

Acknowledgements 致谢

Intercultural Connections Working Group
跨文化联系工作组

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: 翻译

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

给父母的互联网安全提示

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.

谈论互联网安全 - 从隐私问题到身份盗用，互联网上存在危险。儿童和青少年在使用互联网时需要监督，无论他们是 5 岁还是 15 岁，成年人也需要保持专注。注意安全问题，例如分享行踪，照片和个人信息，将大大有助于保护您的亲人。

- How to Structure Homework and Time Online: 如何在在线构建家庭作业和时间：
  https://childdevelopmentinfo.com/family-building/structure-homework-time-online/#.XQgWjTZ8CM8
- **10 Internet Safety and Technology Use Tips for Parents: 给**家长的 10 个互联网安全和技术使用技巧
- https://www.kathleenamorris.com/2019/05/16/internet-safety-parents/
- Internet Safety Advice: Top Tips for Parents: 互联网安全建议：**给**家长的重要提示：
  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:

无人监督/早期互联网使用 - 在一项共享希望国际的调查中，八分之一的父母允许他们的孩子从两岁开始使用互联网，只有十分之一允许他们的孩子在 10 岁或以上时使用互联网，（专家的建议）。结果，许多孩子在使用互联网的同时无人监督。以下是在线保护孩子的方法：

- 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.

监控孩子的在线活动 - 不幸的是，无论父母参与，许多青少年都隐藏或删除了他们的浏览历史。父母必须勤劳。青少年也有他们的父母可能不知道的电子邮件或社交媒体帐户。在某些情况下，孩子会说谎他们的年龄来创建这些账户。

- 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:

  对于儿童遭受同伴受害的情况, 父母应提供支持，父母可在以下情况下参考"金字塔支持"资源：**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.

手机 - 手机非常适合保持联系并在紧急情况下使用。 11 至 14 岁的人中约有 69%拥有自己的手机。手机用户必须了解并注意手机的 GPS 可以显示用户的确切地理位置。此外，在网上发布个人手机号码时要小心谨慎。

- When to Give Your Child a Phone: 什么时候给孩子电话：
  https://childdevelopmentinfo.com/child-activities/when-to-give-your-child-a-phone/#.XQgW-zZ8CM8
- Cellphone Safety Tips: 手机安全提示 https://protectkidsonline.ca/app/en/info_phone_safety
- The First Cell Phone: Rules for Responsibility: 第一部手机：责任规则：
  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: 家长监控应用程序 APP，用于跟踪加拿大以及境外的手机：
  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.

在线欺凌 – 有几个匿名会话应用程序和网站，其中可能会发布（匿名）有关他人的问题或信息。这些匿名应用程序，包括 Whisper，YikYak 和 Ask.FM，都很危险，因为众所周知它们会促进欺凌行为。欺骗他们的匿名身份，恶霸轻易嘲讽，挑逗，并让其他人失望。重要的是始终保持并报告任何滥用，无论是怀疑还是证实。

- PREVNet: Promoting Relationships and Eliminating Violence Network is Canada's authority on research and resources for bullying prevention.

PREVNet:促进良好关系和消除暴力网络是加拿大在欺凌预防研究和资源方面的权威。

- What to do if your child is being Cyberbullied?: 如果您的孩子被互联网欺凌怎么办？ https://needhelpnow.ca/app/en/resources_cyberbullying
- WITSProgram：WITS 计划将学校，家庭和小区聚集在一起，创造相互支持环境，帮助儿童应对欺凌和同伴受害
- RCMP's Centre for Youth Crime Prevention: provides Canadians with age appropriate crime prevention information and tools to prevent youth crime and victimization. 皇家骑警青年预防犯罪中心：为加拿大人提供适合其年龄的犯罪预防信息和工具，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.** 儿童帮助热线，是父母及其子女的良好资源。它提供咨询服务. 现在需要帮助吗？传短讯到 **686868** 与义工 **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摄了自己的裸体或半裸照片，其中一半以上的照片是通过互联网与其他人分享的。重要的是要注意，一旦在互联网上发布信息，可能无法完全删除它。

- Cybertip.ca: Canada's tip line to report the online sexual exploitation of children.
  Cybertip.ca:加拿大的提示热线报告了对儿童的在线性剥削。
- 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.

在线购物，身份盗窃，上网搜寻– 在网上搜寻时要小心。您的网络活动历史记录会不断被跟踪。造访不安全或不适当的网站可能会危及您的个人和财务信息或损害您的计算机。在所有计算机上安装足够的安全和防病毒软件非常重要。应始终使用安全连接，永远不要使用公共计算机，并确保网站在网上下订单之前是合法和安全的。遵循这些预防措施将为用户提供更安全的体验。儿童往往是身份盗窃的受害者。事实上，与成年人相比，18 岁以下的儿童被盗身份的可能性要高 51 倍。犯罪分子针对儿童，因为他们拥有干净的信用记录，并且如先前报导的那样，经常在网上发布个人信息。

- **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状况，检查孩子的信用状况报告分步说明：
  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.

电子游戏 – 近年来电子游戏已经发展迅速。有了许多游戏选项，家长需要注意大多数游戏设备可以直接将儿童连接到互联网和其他玩家。幸运的是，大多数游戏设备都有家长控制和安全设置。家长应该限制孩子玩电子游戏的时间。

- Recommended online educational games to teach children & teen in grades 4 to 8 about how to be safe when using the internet:
  建议的在线教育游戏，教导 4 至 8 年级儿童和青少年如何在使用互联网时保持安全：
  http://mediasmarts.ca/digital-media-literacy/educational-games

Talking about Internet Safety with your kids:

与您的孩子谈论互联网安全：

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.
保密您的个人信息 – 未经父母/监护人的许可，不要透露您的姓名，电话号码，学校或地址。

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 等大多数社交网站都会让您选择谁可以查看您的贴文。要求成年人帮助您更改隐私设置。

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"!
请记住，您在社交媒体上分享的任何内容 – 即使设定为隐私 – 都可能被其他人看见。在点击"发布"或"发送"之前，请务必三思而后行！

4. If you see anything inappropriate online, ask a parent or trusted adult for advice. Remember, it's not your fault you saw this!
如果您在网上看到任何不当内容，请向家长或可信赖的成人咨询。记住，您看到这个不是您的错！

5. If someone sends you something rude over email or social media, DO NOT RESPOND – instead, speak to a responsible or trusted adult.
如果有人通过电子邮件或社交媒体向您发送粗鲁的内容，请勿回复 – 可向负责任或信任的成年人交谈。

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视频，请务必先获得许可。

7. Never buy something online or download anything without permission from a parent/or guardian.
未经父母/监护人许可，切勿在线购买或下载任何内容。

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!
永远不要同意与您在网上认识的人亲自见面。请记住，那个人可能不是他们所说的！

9. Keep your passwords SECRET! Not even your BFFs need to know!
保持密码秘密！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,

站起来反对欺凌 – 不要闲聊或羞辱任何人！如果您想了解有关网络欺凌或欺凌的更多信息，请造访：

Visit： http://www.family.ca/standup/

TIP SHEET FOR ADULTS: SCAMS, FRAUDS & CYBER SAFETY

给成年人提示：骗局，诈骗和网络安全

FRAUDULENT CALLS: 欺诈电话：

Beware of callers falsely claiming to represent a trusted company or organization.
谨防号称受信任公司或组织的欺诈电话。

https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/frdlnt-clls-en.aspx

WHAT TO DO IF YOU GET A CALL: 如果您接到这类电话该怎么办：

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.

如果您接到这样的电话，请挂断电话。永远不要远程连接您的计算机来接听未经请求的电话。如果您不确定，请联系公司或组织的客户服务中心。我们强烈建议加拿大人向加拿大反欺诈中心报告此类欺诈事件，网址为：**http://www.antifraudcentre-centreantifraude.ca** 或致电 1-888-495-8501。

ONLINE SCAMS AND FRAUD: 网络骗局和欺诈：

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.

要知道得奖或促销广告是真实的还是互联网骗局或欺诈并不总是容易的。这些优惠可能看起来好得令人难以置信 - 而且可能会如此。安全的关键是看穿诈骗的技术及迹象。

https://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/index-en.aspx

WHERE CAN I FIND OUT MORE? 我在哪里可以找到更多？

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.

在网上有许多关于欺诈和诈骗的信息。”加拿大金融消费者机构网站”提供有关您与银行和其他金融机构交涉权利得信息。

要订购本出版物，或在您所在省份或地区寻找电话号码的帮助，请致电 1 800 O-Canada（1-800-622-6232), TTY：1-800-926-9105。

WHAT SHOULD I DO IF I THINK I HAVE BEEN SCAMMED? 如果我认为我已经被诈骗了，我该怎么办？

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. 加拿大最常见的诈骗之一是网络钓鱼或掠夺骗局，骗子构成企业或政府组织。例如，声称来自加拿大税务局的骗局。有时候，被锁定的受害者被告知他们欠费，如果他们不付钱，加拿大皇家骑警就会逮捕他们。有时，目标受害者被告知他们可以"点击链接接受退款"。有些人只是被告知要查看链接以查看其信息的变更，或填写表格及其个人信息。

WHAT SHOULD I DO IF I THINK I HAVE BEEN SCAMMED? 如果我认为我已经被诈骗了，我该怎么办？

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.
如果您不确定该消息是否合法，请不要回复！访问该组织的网站并直接致电他们以验证您收到的信息。由于我们许多人收到了要求缴纳税款的欺诈性 CRA 消息，CRA 提供了以下建议：
•CRA 从不通过电子邮件或文本要求提供个人信息，
•CRA 也不要求比特币或礼品卡付款。

如果您收到来自 CRA 的电话，短信或电子邮件，或者欠退款或福利金，登录或注册"我的账户"或"我的公司账户"以验证您的纳税身份，或致电 CRA 的个人收入税务咨询热线 1-800-959-8281。

If you fall victim to a scam, there may be a number of steps to take: 如果您成为骗局的受害者，可能需要采取以下措施：

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. 向您所在小区的当地警方报告欺诈行为：BurnabyRCMP 的非紧急情况（24 小时）电话：604-646-9999 和网站：http：//burnaby.rcmp-grc.gc.ca
2.如果您的社会保险号码被盗，请拨打 1-800-206-7218 联系加拿大服务部报告。
3.向加拿大皇家骑警队的加拿大反欺诈中心报告骗局。您将被要求使用登录合作伙伴（即您的银行）或 GCKey（就像您登录 CRA 账户一样）。报告诈骗时，这可确保您自己的安全。您也可致电 1-888-495-8501 联系反欺诈中心。

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**.

骗子在假装代表银行或信用卡公司时使用类似的策略。例如，您可能会收到来自您未处理的银行的电子邮件或文本，要求您查看您的对账单。当消息不是来自您自己的银行时，很容易识别网络钓鱼或躲避。但是，如果您担心它可能来自您的银行，请不要回复此消息 - 直接通过电话或亲自联系银行或登录您的在线银行网站或应用程序（当然是使用安全互联网连接）验证它是否真实。并且不要忘记向您的银行报告网络钓鱼/浏览消息。
有关其他网络事件和报告的更多信息，请访问加拿大网络安全中心。

FOLLOW GET CYBER SAFE ON TWITTER, FACEBOOK AND INSTAGRAM.

以下是在 Twitter，FACEBOOK 和 INSTAGRAM 上让网络安全。

5 Ways to Protect Your Privacy on a Smart Device (SMARTPHONES/TABLETS/SMARTWATCHES):

在智能设备上保护隐私的 5 种方法（智能手机/平板计算机/智能手表）

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:

这些提示适用于您在家中连接到 Internet 的任何设备。虽然连接设备（也称为“智能设备”）很有趣并且让我们的生活更轻松，但它们也为黑客提供了访问个人和私人信息的机会。按照以下提示采取措施保护您和您的家人：

1 . SECURE YOUR HOME WI-FI NETWORK : 保护您的家庭 WI-FI 网络：

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.

智能设备使用 Internet 发送和收集数据。如果您的家庭Wi-Fi 连接不安全，则您的数据不安全！使用 Wi-Fi 时，您应具备的最低安全性是无线加密和密码保护。在您的无线设置下，确保您的路由器启用了 WPA2 加密。然后，使用复杂密码锁定您的无线网络。强密码包括大写和小写字母，数字和特殊字符。 如果您是高级用户，请在Wi-Fi 网络上创建单独的网络区域以连接智能设备。这称为“设备隔离”，其功能类似于“访客 Wi-Fi”网络。在移动中使用智能设备时，仅连接受信任的受密码保护的网络，并关闭自动搜索 Wi-Fi 网络的设置。

2 . TURN OFF GEOLOCATION WHEN NOT IN USE: 在不使用时关闭地理位置：

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.

许多智能设备都有使用地理定位来提供服务的应用，例如健身追踪或地图。如果应用程序可以看到您的位置，那么黑客也可以。在设备的设置中，请在不使用时关闭地理位置 。

3. BEFORE INSTALLING APPS, UNDERSTAND THE APP'S PRIVACY POLICY AND TERMS OF USE: 在安装应用程序之前，了解应用程序的隐私政策和使用条款：

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.

所有应用都具有隐私设置，可帮助控制谁可以查看您的信息以及他们看到的内容。自定义这些隐私设置，以隐藏个人信息，如全名和联系人详细信息。此外，要警惕要求不必要或过多信息的应用程序。仔细查看权限，不要只为所有内容单击"允许"。

4. DISABLE MICROPHONES AND CAMERAS WHEN NOT IN USE:

不使用时关闭麦克风和相机：

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.

大多数游戏耳机，智能电视，智能手表和智能扬声器都配有麦克风和/或摄像头。如果不安全，您的设备可能会传输您不想要的信息。不使用时，请关闭相机并将麦克风静音。

5. CREATE USERNAMES THAT DON'T CONTAIN IDENTIFYING INFORMATION:

用户名不包含识别信息：

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.

过多分享可能会使您的隐私受到威胁。在为您的设备（或游戏或应用）设置登录信息时，请确保您的用户名不包含识别信息，例如您的姓名，年龄，位置或联系信息。

6. BE SMARTPHONE SAVVY: 手机专家

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**.

智能手机可以跟踪您的位置并显示有关您的信息，包括您的联系人。小心只下载和使用信誉良好的应用程序，并确保密码（或指纹）保护您的手机。了解如何使用工具查找或删除丢失手机中的个人数据。您可以在 ConnectSafely.org/cellphone-safety-tips 上找到更多信息。

7. SECURE YOUR INTERNET ROUTER: 保护您的互联网络由器：

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.

您家中可能有一个小设备，称为路由器或宽带调制解调器，可将您连接到 Internet。该设备有密码和用户名，有时密码很容易猜到。路由器可能很难配置，因此如果您有疑问，请联系专家或您的网络服务提供商，获取有关如何更改密码的建议。

8. **PROTECT YOUR DEVICES:** 保护您的设备:

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**.

通过确保它们受密码保护，并且在计算机上，确保您具有良好的安全性和防火墙软件。如果您需要帮助，请与知识渊博的朋友或家人，或您的互联网服务提供商或移动商联系。 SHAW 和其他一些互联网服务提供商可能会提供免费的防病毒软件，或者您可以从信誉良好的公司购买或获取免费的安全软件，例如 ConnectSafely.org/securityvendors 上列出的公司。

OTHER RECOMMENDED RESOURCES FOR ADDITIONAL TIPS VISIT:
其他推荐的额外提示资源：

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：帮助加拿大人和企业避免垃圾邮件和其他电子威胁
青年隐
私
：隐私专员办公室提供的信息和工具，帮助青少年保护他们的在线隐私

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

网上购物 –如何在网上购物时保护自己

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码：再次强调，牢固的密码是很重要的，就像电子邮件和社交媒体的账号一样。任何时候都不要把密码告诉任何人，除非那个人您信任并愿意把您的账户放心交付给他管理。密码最少需要有八个字节，其中包括数字、大写及小写字母以及特殊符号。不要使用名字或单词。在这个 ConnectSafely.org/passwords 网站，您可以找到如何使用多重鉴定和指纹识别而达到高级安全水平的技巧。

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.

不要点击链接：除非您能 100%肯定是合法的，在电子邮件或社交媒体中收到银行、信用卡公司、政府机构或其它组织的链接，千万不要点击。这是一种很常见的“钓鱼”骗局：当有人发给您一条看似正常的连结，但实际上它有可能是一个不法分子创建的欺诈网站，一旦您点击了链接，您的登录密码和个人信息就可能会失窃。有时尽管在网址中包含了公司名，仍然有可能是骗局。最安全的做法是像平常一样，自己输入网址而不是点击链接。如有任何怀疑，应致电相关公司查询。

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.

提防那些令人难以置信的好事：比如有人告诉您说您无端端中奖了，或者说您赢了一个大奖送您去度假或者让您低价购买一个产品。特别小心那些低价医药产品或者医保项目的促销。

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.

只在声誉好的网上商家购物：小心任何您没有听过的商家。有很多是正规的，但有些可能就是为了盗取您的信用卡号码或其它金融机构的信息，或者就是无法交付您支付的商品。有任何怀疑的时候，向熟悉网上购物的人咨 询，或者上网调查看看别人对商家的评价和评论。

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.

网上购物或使用网上银行时须留意安全的网址：在浏览器的地址栏里输入 https，其中的s 代表安全的意思。如果只是 http，就不是一个安全的网站。如果您使用手机购物或手机银行软件，确保软件是那家公司自己发布的。如果您不确认，参考别人的评价或者请教专家。

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.

如果可能请使用信用卡支付：否则使用借记卡或者安全的网上支付方式，比如贝宝Paypal。从不应该寄现金，银行支票或汇票。甚至个人支票也可能有危险。最好使用信用卡，因为一旦有争议，信用卡公司可以停止这笔交易，在调查索赔时已经可以退款。借记卡也有保护，但有时您要等退款。贝宝、安卓支付、苹果支付也有保护，但信用卡仍然时最好的选择。

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.

点击前小心谨慎：有些事情您点击以后也许就不能撤回，例如下单、卖错股票又或者购买了不能退款的机票或酒店。所有的交易在确认之前应仔细检查。万一出错请立即联系对方公司看是否可以撤回重来。许多网上商家有取消的特别功能，令您可以撤销购买，但您必须动作迅速。一旦商品已经准备发运，再想取消订单就太迟了。通常您可以退货，但您很有可能要支付退货的运费。

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

确保您理解网上商家的退货条款，知道所有收费项目，包括运费、手续费和税费。

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.

网上捐赠前请先做好调查：如 Kickstarter, Indiegogo, GoFundMe 这些众筹资金的网站是购买新产品、捐赠给有价值的目的和组织、以及为有需要的人提供资金支持的好地方，但也需要特别小心。仔细阅读所有的信息，并对提案的相关人士或机构做些调查。如果他们筹集资金是为了某种善举，尝试查查看是否真实。如果他们在推出一款很酷的新产品，确保项目切合实际。有疑问的时候不必继续投资。

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.

做好盗窃身份的保护：不要在网上输入您的 SIN 社保号码，除非您知道这个网站的合法性，它确实有需要这个信息，比如您在向一个合法的金融机构申请银行账户、信用卡、借款或者信用记录。除非您肯定网站是合法的，避免公开您的生日和出生地信息，特别小心叫您输入任何个人信息，比如您的家庭地址。一些合法的社交媒体（如脸书）也许会要求您输入生日。只向合法的网上商家提供信用卡号码。一旦有疑问，调查看看其他人有什么评价。

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**.

监控好您的网上财务账户：查看最近的帐户交易活动，确保您的信用卡、借记卡或银行账户没有欺诈行为的记录。检查您的网上投资账户，确保没有未经授权的交易活动。如果您发现有可疑情况，马上向该金融机构报告，或者打信用卡或借记卡上的免费电话。即使您不使用网上银行，您仍然有风险成为欺诈行为的受害者。马上报告有问题。多数情况下您会受到保护免受欺诈，但您必须报告您遇到的问题。

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.

慈善骗局：大多数慈善机构都有网站，您可以选择在网上捐款。只要您确保您在正确的网站，而且您支持的善举是正规的，那就没有问题。特别小心那种貌似慈善机构叫您在网上捐款的电子邮件。如果您不熟悉相关机构，可以在 CharityNavigator.org 这个网站上查询。如果您打算在网上捐款，确保您是在该慈善机构的正规网站上。以往万一，应在浏览器里输入公司网址，而不是点击链接。

Quick Tips for Online Shopping: 网上购物的快速提示

(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

一个不可信的网上购物网站暴露的几点线索提示

- The site looks poorly designed, unprofessional and contains broken web links. 网站看起来设计很差，不专业，而且网址有些破碎的连结。
- You can't find an address or phone number for the business. 无法查找到公司地址或电话。
- Sales, return and privacy policies are hard to find or unclear. 很难找到销售、退货以及隐私条款，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. 返回键被禁用。也就是说，您卡在一个网页里无法返回。
- You're asked for credit card information anytime other than when you are making a purchase. 不是在付款的时候让您提供信用卡的信息。

HOW TO PROTECT YOURSELF WHEN YOU'RE SHOPPING ONLINE

网上购物时如何保护自己

- Pay by credit card if you can. Do not send cash. 如果可以，应该使用信用卡支付，不要邮寄现金。
- Be on the lookout for prices that are too good to be true. They're likely counterfeits. 特别小心那些难以置信的低价。很有可能是假货。
- Don't use public Wi-Fi to shop online. 不要使用公众场所的WiFi 进行网上购物。
- Read the privacy policy and find out how your information will be used. 阅读隐私条款，了解您的信息会被如何使用。
- 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. 不要回复问您要金融信息的邮件或者弹窗信息。正规网站从来不会这样做。
- Read your credit card statements and check for unauthorized charges. 仔细检查您的信用卡结算单看有没有未经授权的收费。
- 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: 确保防火墙是“打开”状态。比如，最新版本的Windows 系统里防火墙的默认状态应该是打开的，确保不要是“关闭”状态：

    - Open Windows Firewall by clicking the Start button then the Control Panel 在 Windows 系统里，点击“开始”键，在“控制台”里可以打开防火墙。
    - In the search box type “firewall” then click Windows Firewall 在“桌面搜索”栏输入“firewall”就可以打开防火墙。
    - In the left pane, click Turn Windows Firewall on or off 在左边窗格里可以打开或关闭防火墙。
- 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. 不要自动输入您的密码及个人信息（比如地址）。不要让任何网站保存您的信用卡信息。

SENIOR SAFETY: 10 TIPS TO AVOID BEING A VICTIM OF FRAUD
长者安全：避免成为欺诈受害者的 *10* 个秘诀

(Source: 信息来源： 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.

有一天您在家里喝茶，电话响了。

"奶奶，您好。我是您孙子。我在旅游的时候钱包和护照丢了。您能寄钱给我吗？"因为声音听不清楚， 您不知道到底是哪个孙子给您打电话，如果您问他，可能您还觉得会得罪了他。每个奶奶知道孙子有麻烦的时候肯定第一时间想提供帮助，所以您就问他往哪里寄钱。不幸的是，打电话给您的并不是您的孙子，而是一个专门骗老人家钱的骗子。他们就是利用您的好心令您上当。

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.

类似这样的电话诈骗经常发生，许多人辛辛苦苦挣回来的血汗钱就这样没了。这种欺诈行为正以一种令人担心的速度递增。实际发生的数量很可能比我们知道的更多，因为并不是所有的受害者都会申报。

Prevention Tips 预防措施

- Police, judges or legal and government entities will never request that money be sent through money service businesses. 警察、法官或法律及政府机构从来不会要求汇款。
- Never give out personal information to the caller. 接到类似电话，绝不提供个人信息。
- Confirm with other relatives the whereabouts of the family member or friend in question before even considering sending money. 在考虑汇款之前向其他亲戚朋友了解情况。
- 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. 绝不向不认识的人汇款。在您提供任何帮助以前，确认对方的身份。一旦提供了事务号码，款项可以在全世界任何地方被取走。

10 TIPS TO PREVENT BEING A VICTIM OF FRAUD:
防止成为骗局受害者的十个招数:

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.** 妈妈总是告诉我，**如果有些事情看起来好的不像真的，那很有可能就不是真的**。骗子就是利用我们对快捷方式、奇迹和赚快钱的渴望来下手。他们给人提供免费的产品或服务、难以拒绝的特价或奖品，吸引人去登记购买根本不需要的东西，然后说服人支付运费或交易手续费。这些多数情况下是骗局，因为他们收了钱后不会遵守承诺提供相关产品、服务或者奖品。**提示：请对方书面提供具体细节，这样您就可以在下定决心签订任何协议之前仔细阅读。可以找一个您信任的人寻求意见。**

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，谢谢"**"现在不考虑"或者"让我考虑一下"。正规的公司会理解您需要书面的信息或者需要时间去调查。**提示：如果对方向您施压要求您签署任何档或者付款，请挂断电话或者离开。**

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**. 如果有人通过电话或者网上向您推销，**不要向对方透露任何银行或者信用卡信息**、社保号码、保险或者医保号码。再次强调，正规的公司会理解您的。**提示：只向您联系过的熟悉的公司提供个人或者金融信息。**

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.** **小心口甜舌滑或者听起来像官方的电话。**骗子很狡猾，他们知道如果他们在电话里听起来很官方或者很友好，很多人也许会相信他们，向他们汇款或者提供信息。银行、警察、或者政府官员从来不会要求您在电话里或者在您家门口付款。如果有人说您欠款，告诉他们您会查看您的记录并直接联系相关机构。**提示：去相关机构的官方办事地点缴费，自己联系相关机构确认是否欠费。**

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.** 公司代表或者维修人员如果派人到您家之前一定会提前通知您。**如果有任何陌生人敲门，宁愿犯错也要特别小心谨慎。**如果您并没有期待任何人来访，您不一定非得开门。请他们以后再来，并确保他们再来的时候您不是一个人在家。假如您在等人来，您应该请对方出示证件。您可以让他们在门外等待，同时打电话给相关公司确认是否派了人来访。对警察都甚至可以这样做。**提示：不要让任何非请自来的人进入家门。**

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. 花点时间阅读文檔。**许多人根本没有阅读条款就签名，结果导致许多后续的麻烦，或者把自己陷入无法脱离的境地。两年前在伦敦曾经有人做过一个实验，很多人为了使用免费 Wi-Fi 没有阅读就同意了登录条款，根本没有意识到他们到底签名同意了什么。**可以点击此连结阅读该文章。提示：如果您没有完全明白您签名同意的条款，不要签署任何文檔。**

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、组织、比赛或个人向您索取个人信息或金钱，在签署任何文檔或付款之前应该**查清楚是否正规**。确认对方有注册或有本地执照。您可以在 Better Business Bureau 查询之前是否有过投诉。大多数正规的公司都有网页、地址以及顾客的评论，不过小心这些信息也一样可以造假。当有疑问的时候，问问周围的人。如果您使用脸书这种社交媒体，可以向亲戚朋友了解看他们是勠偶认识该公司。**提示：确保您提供信息或付款给您了解并信任的公司。**

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. 做个精明的消费者。**花时间在不同的商家比较价格和质量。销售代表告诉您的事情可以多提问题，重复确认。**提示：在购买商品之前先做好调查，确保您买的商品是您需要的。**

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. 绝不电汇款项给任何您不认识的人。就像直接寄现金一样，电汇很难追踪、跟进或撤回，所以电汇是骗子最喜欢的收钱方式。2014 年所有的金钱损失的诈骗案件中，30%的付款方式都是电汇，还有 30%的消费者给了骗子预付的购物卡。**提示：如果有人让您使用一种无法追踪并无法退款的方式付款，应持怀疑态度并拒绝付款。**

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. 如果您发现您是欺诈行为的受害者，请向警方报告。很多时候，欺诈案件并没有向警方报告，因为很多人觉得自己被骗很不好意思。事实是骗子精心设置了骗局，再通过花言巧语，所以您上当也很正常。如果您报警了，也许您还有点机会挽回损失，又或者可以令其他人免受同类型案件的欺骗。同时，如果您觉得别人也许获取了您的敏感信息，应马上通知您的相关金融机构看看是否有任何保护您的措施。

What Should I do If I Think I have been Scammed or A Victim of Fraud?

如果我认为被骗或者成为欺诈案件的受害者时应做什么？

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: 所有的欺诈和骗局都应该上报，即使您觉得不好意思或者认为金额太小不值得担心。也许您无法把钱拿回来，但您可以帮助阻止骗子继续向别人骗钱。您可以上报给以下机构：

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** 小区本地警察局：本那比市皇家骑警的 24 **小时非紧急**电话： 604-646-9999 网址： **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** 加拿大反欺诈中心 **加拿大国内免费电话: 1-888-495-8501 网址: 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** **加拿大消费者金融机构可以向您提供与银行和其它金融机构打交道的信息。**电话： 1-866-461-3222 (TTY 613-947-7771, or 1-866-914-6097), 网址： **fcac.gc.ca**

4. For more information, visit **Canada.ca/Seniors** or visit your local Service Canada office. 要了解更多信息，请查看网站 **Canada.ca/Seniors** 或访问加拿大本地服务机构。

STEPS TO REPORTING A FRAUD, OR A SCAM:
报告欺诈或骗局的步骤：

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：收集所有关于该欺诈案件的信息，包括文件、单据、邮件或手机短讯。

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：向当地警方上报。这样可以让警方了解有什么针对当地居民或商业的骗局。记录您的电话及所有的文件号码。

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：联系**加拿大反欺诈中心**, 电话： 1-888-495-8501 营业时间：周一至周五上午 9 点至下午 4:45（东部时间）。

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：向相关金融机构上报款项汇到哪里（比如通过西联或速汇金等公司、或通过银行、信用合作社、信用卡公司或网络付款的服务）。

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：如果欺诈行为发生在网上，比如通过脸书、易趣、Kijiji 这种分类广告网站、又或者约会网站，确保向该网站报告。具体可以点击“报告问题”或“报告广告”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：身份欺诈案件的受害者应向信用局、Equifax (https://www.consumer.equifax.ca/personal/) 和 TransUnion (**https://www.transunion.ca/**) 报告账户的问题。

18 INTERNET SAFETY TIPS FOR SENIORS

针对长者的 18 招互联网安全秘诀

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

GENERAL SAFETY & SECURITY: 一般安全问题

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. 确保您的密码是独一无二并安全的。使用强力的密码，不要在密码内包含任何个人信息，并尽量避免使用词典里常用的单词和短语。许多网站建议使用大小写字母、数字和特殊符号结合的密码。另外，不要在多个账户里使用相同的密码。

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. 使用反恶意软件以及其它的保护工具。确保您的计算机安装了可信的安全软件，并设置了自动更新，这样您的计算机在新风险下仍然可以受到保护。如果您不知道应该安装什么软件，请向专家或懂计算机的人请教。

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. **不要下载任何不明的附件或软件。**如果您不知道或者不信任来源，不要下载任何文件、图片或软件。骗子或者黑客通常会把病毒和恶意软件伪装成“免费”的软件或者有意思的内容引诱您下载。

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. 考虑授予给一个您信任的朋友或家人权限进入您的账户。万一有紧急情况，您信任的朋友或家人都很难甚至不可能进入您的网上账户，如邮箱、银行和文件存储等。提前计划让律师协助您授权给人进入您的账户。

EMAIL AND SOCIAL MEDIA 电子邮件和社交媒体:

5. Understand "spam" filters. **Spam refers to unwanted, unsolicited emails. Most email providers have spam filters that remove these emails from your main inbox.** 了解“垃圾邮件”的过滤设置。垃圾邮件指那些不想要、不请自来的邮件。**大多数电子邮箱都有过滤设置可以把那些垃圾邮件从收件箱移除。**

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. **使用社交媒体的隐私设置。**小心您在任何社交媒体上发布的任何帖子，使用隐私设置限制除了您信任的人外，任何人都不可以查看您的贴子和个人信息。

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. **报告任何欺凌问题。**网络欺凌也许和青少年相关，但并不意味着不会发生在成年人身上。不要回应，而应该向网络平台以及可以帮助这些人的机构报告。记住欺凌问题不是您的错。

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. **知道骗局的迹象。**如果好得难以置信，通常都是骗局。超低价或免费的大奖，如旅游、电子及医药产品，就是骗子经常使用的手段。另一方面，骗子又是会使用朋友的个人账户向您要钱，在没有亲自向朋友确认之前绝不回复及汇款。

MONEY & PURCHASING 金钱及购物:

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.) **查找安全的网站。**任何时候出现弹窗需要输入您的付款信息时，首先查看网页是否安全。在网络浏览器的输入栏里查找是否有 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. **了解并避免被钓鱼。**小心任何链接点击后链接到网站叫您购买任何任何东西或输入付款信息。一种常见的骗局就是把一个"钓鱼"网站做的像一个可信的网站，您的信息输入以后就会被骗子获取。查看是否有任何语法错误、拼写错误或者看起来和平时不一样的网址。当有疑问时，应该在地址栏直接输入您知道的正确网址。

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. **不要在不明网站输入任何个人信息或付款信息。**同样，如果您准备输入个人或付款信息，确保检查网站是否正确。查看网上商家的评价，在银行或政府主页，绝不回复向您索要个人信息的要求。银行和政府机构从来不会索要的您密码、社保号码或付款信息。

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. **监控您的金融账户。**即使您非常小心谨慎，您的付款信息仍然有可能在可信的商家被泄露或者被盗取。监控您的银行账户和信用卡账单看有没有任何未经授权的事务历史记录。

MEETING NEW PEOPLE 与不认识的人见面:

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. **特别小心。**可惜网上不是每个人都是他自称的人。网上有很多认识新朋友的机会，比如在约会网站、兴趣小组和论坛，但不是每个人都值得信任。与不认识的人打交道的时候应特别小心，不要透露太多个人信息给别人找到。

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. **不要汇款给新认识的人。**与个人信息类似，有些人利用互联网相对的匿名属性去接近他们的目标，骗钱成功后您就再也找不到他们了。不要被那些悲惨的故事打动而去送钱，除非您确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. **见面时注意安全。**如果您要和在约会网上认识的人或网友见面，请选择公众场所，并让朋友或家人知道您去哪里和谁见面。注意安全总不会有错，即使您觉得您已经很熟悉对方了。

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. 知道现实和虚构的区别。类似新闻发布和健康指南的博客通常通过吸引访问者浏览并点击广告挣钱，发布轰动的头条吸引人去查看。并不是所有发布在网上的信息都是真实的，不论看起来有多官方。

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. 避免自己给自己诊断，不要听信轮椅健康建议。很容易在搜索引擎搜索您的症状然后找到一系列有可能的疾病，或者讨论诊断的论坛。只有持牌的保健专业人士并了解您的健康背景可以做出诊断并开药给您。在网上自己尝试意味着病情拖延甚至恶化。

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. 与专业人士跟进。当然，并不是网上所有的健康建议都是关系生死的。网上有很多关于营养、健康及体质的资源都很有帮助，但在做出任何可能会影响健康的改变（比如新的饮食或运动计划）之前，最好还是向专业人士（如医生、护士、饮食学家和营养学家）咨询。

By educating yourself, you can stay safe. Here are some other resources to check out: 通过教育您自己，您可以保持安全。以下列举了其他资源供参考：

RCMP's Seniors Guidebook to Safety and Security 皇家骑警的长者安全指南-
http://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7
How to protect yourself while shopping online 如何在网上购物时保护自己:
https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-mn/nln-shpng-en.aspx
Basic Online Tips & Advice 上网的基本提示和建议:
https://www.stopthinkconnect.org/resources/preview/tip-sheet-basic-tips-and-advice
Online shopping, banking, charity and travel 网上购物、银行、慈善和旅游-
https://www.connectsafely.org/seniors/
Top 10 tips to protect your inbox, computer and mobile device 保护您的邮箱、计算机和手机的 10 个提示: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/spam/casl_tips_ind/