Competition Bureau Canada
Bureau de la concurrence Canada

防范诈骗迷你宝典

Canada

防范诈骗迷你宝典

第二版

由加拿大竞争局于2012年首次发布

本出版物不属于法律文件，我们希望通过这一便利方式，为公众提供一般性信息。

如需了解加拿大竞争局事务的相关信息，请联系：

Information Centre
Competition Bureau
50 Victoria Street
Gatineau QC K1A 0C9

电话：819-997-4282
免费电话：1-800-348-5358
听障专线：1-866-694-8389
传真：819-997-0324
网站：www.competitionbureau.gc.ca

如需获取本出版物的纸质或其他格式（盲文、大字体等）版本，请拨打上方电话号码，联系加拿大竞争局信息中心。

本出版物亦有HTML格式，请至以下页面获取： http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

复制许可

Cat. No. Iu54-42/2018Ch2-PDF
ISBN: 978-0-660-29915-0
2019-03-29

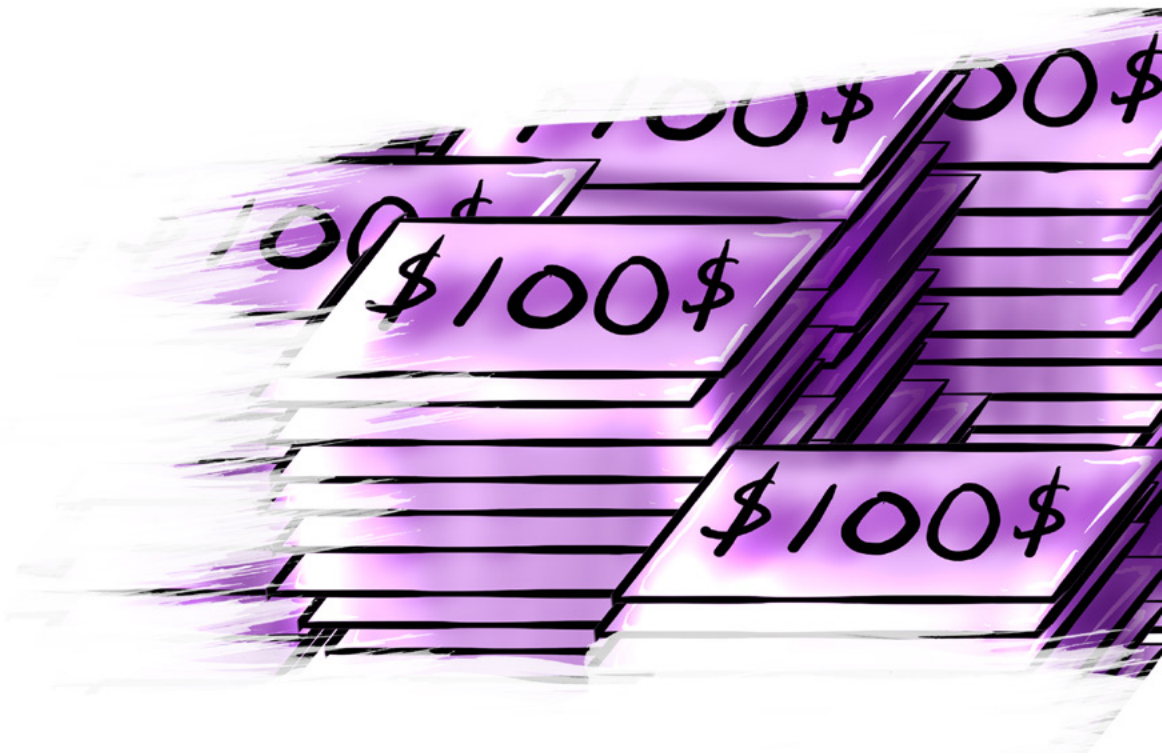
This publication is available through PDF on the web in the following languages: English, French, Chinese traditional, Punjabi, Spanish, Tagalog.

序言

诈骗者非常狡猾。无论是年轻人，还是退休长者，都是他们的潜在作案目标。企业单位也不能幸免。每个人都可能成为诈骗受害者。

有这样一群超级英雄，他们找到了对抗诈骗的办法。秘诀很简单：知识就是力量！

您也想成为反欺诈超级英雄吗？请继续阅读。我们也要请您与亲朋好友分享本手册，大家一起武装起来！



目录

防范诈骗基本要领

用必要的防骗信息和知识武装自己，保障您和家人的人身和财物安全，成为现实生活中的超级英雄。

您的钱财来之不易，理应花费在重要的地方——子女教育、令人兴奋的旅行，或是一部崭新的智能手机。

诈骗者是真实存在的。他们每天都在寻觅新的受害者。诈骗渠道多种多样——通过网络、手机、邮件，或是面对面的方式诱您上当。

每个人都是诈骗者的目标。每年，都有数以千计的加拿大人不幸落入陷阱，损失财产总计数百万。受骗的家庭和企业可能损失惨重，备受打击。

学习怎样防范诈骗。本手册涵盖了目前在加拿大最为常见的12种诈骗手段，同时介绍各种防范技巧和小贴士，帮助您保护自己，并了解一旦受骗，应采取哪些行动。

及时举报！无论是青少年、年迈的长辈还是企业高级官员，每个人都可能成为受害者。无论被骗钱款数目多少，您都应该向相关部门报案。不必觉得难为情，您的行动能帮助他人进行防范，避免上当受骗。

知识就是力量。尽力了解更多信息，更好地保护自己。除本手册外，还有许多值得信赖的网站，可供您浏览查询。

由加拿大皇家骑警、加拿大竞争局和安大略省警察局共同参与管理的加拿大反欺诈中心（Canadian Anti-Fraud Centre）提供了许多关于防范诈骗的信息。请浏览www.antifraudcentre.ca网站，增强防范意识！

订阅陷阱

令人垂涎的优惠，可能会引诱您落入高额陷阱。

这些订阅陷阱往往会让您“免费”或“低价”试用其产品或服务。常见的此类产品有减肥产品、健康食品、药物和抗衰老产品。

您一旦提供了信用卡信息来支付运费，就在不知情的情况下成为了月度订阅用户。到那时，再想取消订阅就异常困难了。

诈骗者会利用网站、电子邮件、社交网络平台、电话等渠道引诱人们落入陷阱。请牢记，像“限时优惠”这样的高压销售伎俩，只是为了让您匆忙、冲动地作出决定。

自我防范小贴士：

- 相信自己的直觉。如果觉得某项优惠是天上掉馅饼，请不要注册参与。
- 在注册试用产品或服务前，应先查找公司相关资料，阅读过往评价，尤其要留意差评。商誉促进局（Better Business Bureau）就是非常值得信赖的信息来源。
- 如果找不到或是无法理解商家的条款和条件，请不要注册参与。尤其要留意：默认打勾的选项、退货政策，以及任何含糊不清的收费项目。
- 如果决定进行试用，应保留好所有文件、收据、电子邮件和短信记录。
- 经常查看信用卡账单，留意是否有频繁或来源未知的扣款。
- 如在取消订阅时遇到问题，可与信用卡发行方、当地消费者保护组织或执法机构联系。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。

身份盗用

务必确保您的身份只属于您本人！

诈骗者永远都在伺机收集或复制您的个人信息，以进行欺诈。不法分子在窃取您的身份后，可以使用您的账户购物，用您的信息申领护照、政府补贴、贷款等等。您的生活可能因此遭受重大影响。

欺诈者会采取各种伎俩，有些直截了当，有些则经过精心设计，难以识破。他们可能会翻找您的垃圾箱，或偷取信件；而在互联网上，则可能使用间谍软件、病毒、黑客、网络钓鱼等手段（请见第13页）。

诈骗者通常会寻找以下信息：信用卡资料、银行帐户详细资料、全名和签名、出生日期、社会保险号、完整地址、母亲婚前姓氏、在线用户名和密码、驾照号码和护照号码。

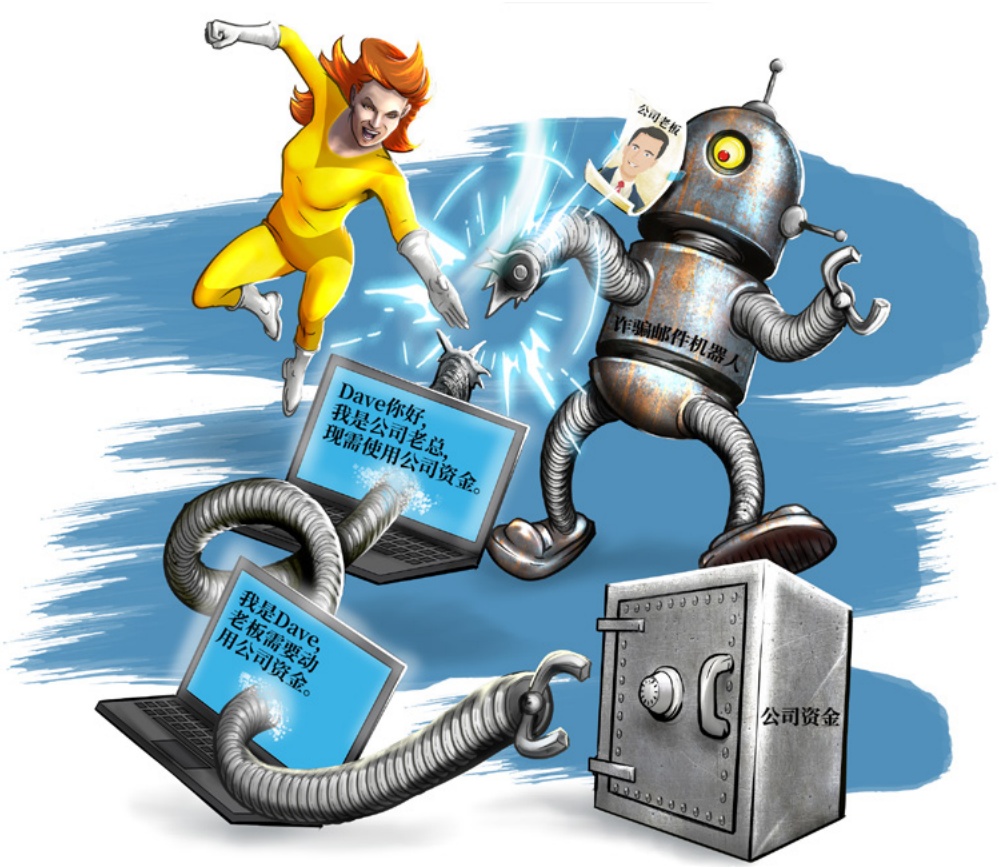
窃取他人身份是严重的犯罪行为！

自我防范小贴士：

- 切勿在电话、短信、电子邮件中或互联网上透露您的个人信息。
- 尽量不要用公共场所（例如咖啡馆）的电脑或Wi-Fi热点来访问或提交个人信息，这一行为会使您的信息有失窃风险。
- 为每一个在线账户分别创建安全性高的密码，同一密码不要重复使用。为您的设备和家庭Wi-Fi网络设置密码。
- 在线购物时，应使用安全且信誉良好的支付服务，请留意URL是否以“https”开头，其左侧是否有闭合的锁头符号。
- 不要在社交网络上透露个人信息。不法分子会同时使用您的个人信息和图片进行欺诈。
- 如使用银行卡支付，输密码时务必进行遮挡。如将银行卡交给收银员操作，也不要让卡片离开您的视线。
- 丢弃含有个人信息的文档时，应将其撕碎、销毁。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。



CEO诈骗

公司老板急需用钱?先确保电子邮件地址准确无误!

您是会计或金融领域的从业者吗?在工作中是否有转移钱款的权力?您的直接上司是不是位高权重的公司领导?如果您给出了肯定的回答,则要格外谨慎。此类诈骗专以您为目标!

在典型的“CEO诈骗”案件里,诈骗者往往通过窃取电子邮件或模仿的手段,化身公司高层主管,向您发送看起来并不值得怀疑的邮件,诱导您将钱款转给第三方。

诈骗者会在邮件中把情况描述得十万火急,但又不可对外泄露。需要用钱的理由可能是确保重要合同顺利签署,执行机密交易,或更新供应商的支付信息。

诈骗者发送邮件时,往往很有策略,看准主管不在或不便联络时,趁虚而入。此类骗局会给企业带来数万甚至数百万损失。

在全球范围内,CEO诈骗的威胁与日俱增,小型本土企业和大型公司,无一不是他们猎食的目标。

自我防范小贴士:

- 使用信誉良好的防病毒软件(更新至最新版本)和安全性高的密码,来保护您计算机系统的安全。
- 执行任何交易请求之前,均要致电或当面核实。切勿使用电子邮件中提及的联系方式。
- 核实发信人电邮——诈骗者的邮箱地址往往与真实地址非常相似,仅改动一两个字母。
- 鼓励您的公司创建一套需要多级审批的资金转移标准流程。
- 不要过多公布详细信息。诈骗者会使用网络和社交媒体上可获得的信息来寻找潜在的受害者和行骗时机。

如遇疑似欺诈行为,请务必举报。

请阅读第19、20页内容,了解更多信息。

健康与医疗诈骗

轻轻松松包治百病?请您擦亮眼睛。

有些不法分子试图将他人的疾苦变成自己的获利来源。健康诈骗最常见的三种类型, 分别是治病神药、减肥项目和虚假网上药店。这些产品和服务常常以社交媒体“推广帖文”或网站弹出窗口的形式进入您的视野。

诈骗者推广的产品和服务看似是合法的替代药物和治疗方法, 能够轻松、迅速地治愈严重疾病。其中一些似乎还有明星代言, 或是得到“已治愈患者”的大力推荐。

减肥骗局往往承诺使用者不费吹灰之力即可取得惊人成果。诈骗者推广的可能是不寻常的饮食方式、不同以往的运动模式、燃脂器械, 或是突破性的产品, 例如药丸、贴片或乳膏。

虚假网上药店则以极低的价格兜售各类药物, 且无需医生处方。欺诈者会在互联网上发布广告, 并发送垃圾邮件。即使您确实收到了商家承诺的产品, 药物的真实性和安全性也得不到保障。

自我防范小贴士:

- **请记住, 没有神奇药物或奇迹疗法可以实现快速减肥或治愈疾病。**
- **不要相信商家宣称的药物、补充剂疗效。咨询您的医护人员, 核实相关信息。**
- **不要因为身负压力而勉强作出决定, 如果商家要求您支付大额定金或签署长期合约, 则更要谨慎。**
- **合法的网上药店都需要您出示医生处方。**
- **明辨所谓的明星代言或推荐。**

如遇疑似欺诈行为, 请务必举报。

请阅读第19、20页内容, 了解更多信息。

恋爱诈骗

屏幕对面，到底是谁？

有些欺诈者会刻意迎合您浪漫、体恤他人的性格，让您不经意间就疏于防范。他们会在备受欢迎的合法交友网站下手，也会通过虚假伪造的平台诱您上当。

在真实的交友网站上，诈骗者可能会向您发送若干私信，以及样貌不错的“本人”照片。一旦您动了心，他们就会开口要钱。索要钱财的借口可能是家人重病，或是自己身陷绝境，急需帮助。而在收到您的钱款后，诈骗者往往消失得无影无踪。

欺诈者也可以自行创建虚假交友网站，而您在站内发送或接收私信都需要交费。为了吸引您继续使用这种付费服务，他们会给您发送内容模棱两可的邮件，表达对您的爱意和渴望。

许多时候，诈骗者甚至会提出与您见面，让您相信他们是真实存在的。

自我防范小贴士：

- 切勿通过交友网站汇款，或在网站上提供个人财务信息。
- 相信直觉，举棋不定时应立即发问核实，注册前仔细阅读网站条款。
- 明确了解免费和收费服务项目，以及如何注销账户。
- 务必使用信誉良好的合法交友服务。虚假站点常常模仿合法站点的网址，请仔细核对。
- 很少有人会在几次信函、邮件、电话交流或看到几张相片后，就对他人表达忠贞不渝的爱慕之情。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。

业务诈骗

针对企业的骗局不断变化，请时刻擦亮眼睛！

精心设计的骗局能使任何规模的组织机构沦为受害者，请务必明辨。

商业目录骗局就是其中非常典型的一种手段。诈骗者会向公司发送提议，称可在杂志、刊物、商业目录或在线目录中发布公司信息或广告。他们会打电话确认地址和其他细节。随后，公司会计部门将收到账单并进行支付，却根本不知道公司从未订购或授权此项服务。

兜售健康与安全产品也是一种常见的骗局。您可能会接到自称是省政府工作人员打来的电话，告知您公司需要更换急救用具，或开展新的健康安全培训。无论是哪一种理由，诈骗者都会催促您尽快采取行动。

另一种可能的骗局则涉及办公室用品。您会收到未曾订购的产品及其账单。

在许多情况下，诈骗者会不停向您追讨所谓的欠款，甚至会让您相信，他们将委托收债机构追收款项。

自我防范小贴士：

- 提醒自己、公司员工和同事，对于不请自来的促销电话要提高警惕。
- 将与您所在企业常有业务往来的公司一一列出。
- 限制有权批准购买和支付账单的员工数量。
- 明确规定帐户和发票的验证、支付和管理流程。
- 联系您所在省份的监管机构，了解您的法律义务。
- 欺诈者会使用与某些较有知名度企业极为相似的名称或徽标，使其发票看起来真实可信。支付任何款项前，应仔细检查发票。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。

网络钓鱼和短信诈骗

时刻留心！信息极易造假！

随着我们在网络世界中停留的时间越来越长，诈骗者在数字领域的骗局也日益创新。

网络钓鱼指的是您收到声称来自合法组织（如金融机构、企业或政府机构）的垃圾电邮。诈骗者会要求您通过电子邮件或点击链接的方式提供或验证个人信息或财务信息，例如您的信用卡号、密码和社会保险号。

顾名思义，短信诈骗通过手机短信进行，但形式与网络钓鱼并无二致。

在短信中，诈骗者会模仿较有公信力的组织机构的语气，使用他们的徽标，并常常敦促您采取行动。此类短信的内容五花八门，但目标只有一个，就是套取您的详细个人信息。

自我防范小贴士：

- 信誉良好的组织机构永远不会在电子邮件或短信中询问您的个人信息。
- 不要理睬来自未知联系人的信息。
- 可疑信息中可能带有病毒，应及时删除。
- 不要回复垃圾邮件（即使是通过回复取消订阅），也不要打开任何附件或点击任何链接。
- 将鼠标悬停在链接上，验证其真伪，仔细检查网址是否准确。
- 在所有设备上更新防病毒软件。
- 切勿使用可疑邮件中提供的电话号码或电子邮件地址 – 应使用已经验证网站上列出的联系信息。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。

税务诈骗

收到了来自CRA的电话或电子邮件?首先查证是否真实!

您收到来自加拿大税务局(CRA)的短信或电子邮件,声称您有权获得额外退税,只需提供详细银行信息即可。请注意,这样的“飞来横财”正是典型的税务诈骗。

还有一类骗局,是告知您有CRA欠款需立即缴纳,否则对方将报警。

无论遇到哪一种情形,如果您接到电话、信件、电邮或短信,声称有CRA欠款,您都可以登陆CRA网站的“My Account”个人帐户或致电1-800-959-8281进行核实。

自我防范小贴士:

CRA绝不会:

- 使用攻击性或恐吓性的语言。
- 威胁将您逮捕或报警。
- 要求您通过预付信用卡或礼品卡(例如iTunes、Home Depot礼品卡等)进行付款。
- 通过Interac电子转帐收发款项。
- 通过短信与您沟通。

来自CRA的电子邮件中:

- 绝不会询问您的财务信息。
- 绝不会包含任何财物信息。

CRA只接受以下付款方式:

- 网上银行。
- 借记卡。
- 预授权借记付款。

如遇疑似欺诈行为,请务必举报。

请阅读第19、20页内容,了解更多信息。

上门欺诈

叮咚!猜猜是谁?诈骗者上门来了!

尽管我们已经步入数字时代,但依然有些陈旧的骗局登门而来,对个人及企业安全造成威胁。走街串巷的销售人员会利用高压销售技巧,诱导您购买或注册您不想要、不需要的产品或服务。

他们的推销言辞往往极具煽动性,鼓动您为慈善组织捐款、抓住投资机会、装修屋宅设施(例如热水器、暖炉和空调)等等。

但很多时候,这些产品或服务根本不见踪影。即便是您获得了这些产品或服务,其质量也令人担忧,与推销言辞中的描述大相径庭。

自我防范小贴士:

- 不要强迫自己立即作出决定 – 应先对商家和产品进行一番调查。
- 让推销人员出示带有照片的身份证件,询问推销人员姓名,了解其代表的公司或慈善机构的名称。
- 详细询问慈善机构如何利用获捐善款,务必请对方出示书面信息。
- 切勿分享任何个人信息或任何账单、财务报表副本。
- 只让您信任的人进家门。
- 投资前,先进行调查。仔细阅读详细条款,不要急于签字。
- 了解您的合法权利。联系您当地的消费者事务办公室 – 大多数省份和地区都依据其消费者保护法案制定了相关指导方针。

如遇疑似欺诈行为,请务必举报。

请阅读第19、20页内容,了解更多信息。

紧急事务骗局

牵挂晚辈的老人们，三思而后行！

紧急事务骗局通常以牵挂晚辈的老人们为作案目标，利用亲情来骗取他们的钱财。

在典型的此类骗局中，老人会接到电话，对方自称是其孙子或孙女。这些所谓的“孙辈”声称自己遇到了麻烦——常见借口包括车祸、入狱、身在海外无法归国——急需用钱。

对方会向您提问，诱导您给出个人信息，还会表示自己觉得很难为情，不想让家里其他人知道实情，所以请您务必保密。

有时，诈骗者会与同伙一起行骗，在电话中一人假扮您的孙辈，另一人则饰演警察或律师。

还有些时候，诈骗者会扮作您的老邻居或您家人的朋友，并称自己遇到了麻烦。

自我防范小贴士：

- 花些时间，查证对方说辞是否属实。诈骗者正是利用您急于帮助亲人的心情来诱您上钩。
- 给孩子的父母或朋友打电话，了解他们的行踪。
- 在电话中提出只有您亲人能够回答的问题，验证对方身份，核实后再采取行动。
- 切勿向您不认识或不信任的人汇款。
- 切勿向致电者透露任何个人信息。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。

购物诈骗

并非所有网上卖家都拥有良好信誉!

在线购物, 是许多人都喜欢的消遣方式。但是, 您在网上看到的许多优惠——无论是价格低廉的设计师手袋, 还是巨幅折扣的电子产品——不过是夺人眼球的“免费午餐”罢了。

诈骗者可以在合法的拍卖网站(如eBay)或在线市场(如Kijiji或Craigslist)上创建帐户, 以极低的价格兜售自己产品, 诱使您消费。

到头来, 即便您真的下了单, 收到的也会是质量低下的货物或拙劣的仿冒品。

还有些时候, 诈骗者会诱导您点击赞助商链接, 继而访问某个看似真实的网站。如果您决定从这一网站购物, 将无法享受合法网站提供的任何保护或服务。

如果某网站或优惠与类似网站或产品相比异常显眼, 很可能有您看不到的问题。

自我防范小贴士:

- 从信誉良好或曾经交易过的卖家或个人处进行购买。
- 所有交易均应通过拍卖网站进行。
- 对于相距遥远的卖家, 或收到评价数量很少或为零的卖家, 要谨慎辨别。
- 在线购物时用信用卡支付, 许多信用卡发行方都提供相关保护措施, 可能会向您退款。
- 谨防包含拼写错误和语法错误的网站。
- 仔细阅读退换货政策(包括细则)。
- 向卖家提问, 并确认商品/服务的交付时间和总计费用。

如遇疑似欺诈行为, 请务必举报。

请阅读第19、20页内容, 了解更多信息。

销售骗局

伪装成买家的诈骗者。

如果您在网上销售商品——无论是个人行为，还是代表商家——都需要小心辨别买家身份，因为其中有些人对您的商品和钱财虎视眈眈。

有时，诈骗者还未见到商品，就表示要购买。您会收到PayPal通知或转账邮件，称买家已进行支付。

但通知或邮件中也会提到，您只有在提供商品物流追踪号后，才可收到货款。当您寄出商品，并输入物流追踪号后，才发现通知邮件根本是伪造的。

还有一些情况下，您可能会收到来自伪造银行转账、假支票或被盗用信用卡的付款。

此外，诈骗者也可能给您发送信息，声称您的PayPal或银行账户有问题，导致买家无法付款，然后要求支付一笔费用，以开设商业帐户，完成交易。诈骗者会提出先帮您垫缴这笔费用，您稍后通过转账或电汇的方式还付即可。如果您相信了这套说辞，这笔“费用”就落入了对方的口袋。

自我防范小贴士：

- 一定要安排在当地安全的公共场所见面交易。
- 对于语法不流利且没有针对性的电子邮件，要提高警惕。
- 留意相距遥远或是未见到商品就同意下单的买家。
- 核实发信人电邮——诈骗者的邮箱地址往往与真实地址非常相似，仅改动一两个字母。
- 不要为了收取钱款而先行付款。

如遇疑似欺诈行为，请务必举报。

请阅读第19、20页内容，了解更多信息。

提高警惕：需要留心之处

学会辨识情况不妥的迹象。

电汇。许多诈骗者会要求您使用汇款服务（例如MoneyGram、Western Union）或加密货币（例如比特币）进行电子汇款。请您牢记，通过这些服务进行转账汇款，就好比转出现金——对方一旦收讫，您几乎不可能追回钱款。

超额支付。如果您是销售商品的卖家——尤其是在线卖家——则应留意买家的付款方式。诈骗者会通过伪造的出纳支票、个人支票或公司支票向您支付高于约定价格的款项，然后会要求您存入支票，再汇回超额支付的部分。一旦银行查出支票是伪造的，就会认为是您企图骗取钱财，从而使您身陷困境。

拼写错误。谨防下列电子邮件、消息或网站：常用单词拼写错误；内容中包含语法错误，导致难以理解；词句的表达方式不正确。还应仔细检查电子邮件和网址，识别可能存在的细微错误或差异。

索取个人信息。诈骗者可能会要求潜在受害者提供个人或财务信息，而这些信息已超出交易或讨论所需的范畴。如果有人要求您提供护照复印件、驾照号、社会保险号或出生日期，请务必留意，如果您不认识对方，则更要谨慎辨别。

不速之电。您可能会接到电话，对方声称您的计算机感染了病毒，您有未付税款，或您的银行帐户涉及欺诈活动。请您牢记，合法组织不会直接来电。遇到此类情况，应挂断电话，并拨打来源可靠（例如电话簿、对方网站，甚至发票和帐户明细）的号码自行联系相关组织。

莫名其妙的社交网络好友请求。在查看对方个人资料或向现实生活中的朋友求证之前，请不要接受不认识人士的好友请求。他们的个人资料页面是不是没什么内容？或者从中无法辨别对方身份？他们是不是抛出了“比友情更进一步”的承诺？这些都是需要警惕的诈骗迹象。您应删除这一好友请求，并屏蔽对方，使其无法再与您联络。

邮寄信件中大奖。您收到一张寄来的抽奖卡，寄件者声称，这张卡已经中奖，或肯定会中奖。奖品多种多样，您可以赢取轿车，外出旅游。如果您没有参加抽奖，请将卡片丢弃。骗子可能已经找上门了！

天上不会掉馅饼。大幅折扣，谁人不爱？但是，过于诱人的折扣和令人难以置信的价格背后，往往暗藏玄机。低廉的价格，通常只会带来廉价甚至仿冒的商品。所谓“免费”，也可能需要您输入信用卡号码，以支付运费。诈骗者无需大费周章，便可坐收巨额利益。

举报诈骗行为

向何处进行举报，取决于您的居住地点，以及所涉及的诈骗类型。

无论是已经受骗，还是诈骗者曾试图行骗，您都应举报。加拿大政府部门可能无法对每一起诈骗活动采取行动，但您可以通过各种方式提供帮助。通过举报诈骗活动，您也许能帮助政府部门警示他人并提醒媒体，尽力阻止诈骗活动继续蔓延。您也应将遇到的任何骗局告知家人和朋友，以示提醒。

根据诈骗类型的不同，您可以向以下机构进行举报：

加拿大反欺诈中心
（Canadian Anti-Fraud Centre）
www.antifraudcentre.ca
1-888-495-8501

加拿大竞争局
（Competition Bureau）
www.competitionbureau.gc.ca
1-800-348-5358

本地诈骗活动

联系您当地的消费者事务办公室

您当地的消费者事务办公室是调查您所在省份或地区诈骗活动的最佳资源。您可以在《加拿大消费者手册》（Canadian Consumer Handbook）中找到各省份和地区消费者事务办公室的名单。

www.consumerhandbook.ca

金融与投资诈骗

请联系加拿大证券管理处（Canadian Securities Administrators）

金融诈骗涉及金融产品与服务（例如退休金、代管基金、财务建议、保险、信用账户或存款账户等）的销售或推广活动。

投资诈骗涉及股票购买、外汇交易、离岸投资、庞氏骗局或优质银行投资理财产品。

您可以向加拿大证券管理处或您当地的证券监管机构报告金融和投资诈骗。

www.securities-administrators.ca

银行和信用卡诈骗

请联系您的银行或金融机构

除向加拿大反欺诈中心举报此类骗局之外，您在收到任何有关您帐户的可疑信件时，还应告知银行或金融机构，他们会指导您如何采取下一步行动。

在联系您的银行或金融机构时，请务必使用电话簿、帐户明细单或银行卡背面的电话号码。

垃圾电邮和短信

请联系垃圾信息举报中心（Spam Reporting Centre）

许多不法分子会通过电子邮件和短信进行诈骗。请浏览www.fightspam.gc.ca网页，查阅加拿大反垃圾信息的相关立法，了解如何举报此类信息。

如收到索取详细个人信息的欺诈性钓鱼邮件或短信，您也可以向银行、金融机构或其他相关组织进行举报。同样，请务必使用信誉良好的官方来源中列出的电话号码或电子邮件地址，切勿使用不明电子邮件中显示的号码或邮件地址。

欺诈、盗窃及其他犯罪活动

请报警

许多可能违反各项消费者保护法(由加拿大竞争局以及其他政府和执法机构强制执行的法律)的诈骗行为,很可能也已经触犯了刑法中的欺诈条款。

如果您是欺诈行为的受害者——也就是说您因为他人的不实或欺骗行为而遭受损失——请考虑联系当地警方,如果涉及金额巨大,更应及时报警。如遇财产被盗,或受到诈骗者的威胁或侵犯,请务必联系警方。

身份盗用

请报警

身份盗用是指出于犯罪目的获取、收集他人的个人信息。

如果您怀疑或已确定自己遭遇了身份盗用或欺诈,或在无意中提供了个人或财务信息,您应该:

- 联系当地警方,进行报案。
- 联系您的银行或金融机构,以及信用卡发行方。
- 联系两家全国信用局(credit bureau),请对方在您的信用报告中设置欺诈警报。
- 如遭遇身份盗用或欺诈,务必举报,请联系加拿大反欺诈中心(Canadian Anti-Fraud Centre)。

根据遇到的具体情况,您还可联系以下机构:

- 您所在省份的商誉促进局(Better Business Bureau)
- 加拿大税务局开设的慈善机构查询热线

www.cra-arc.gc.ca
1-800-267-2384

- 您所在省份的档案办公室
- 信用机构可以在您的账户上设置欺诈警报,这将提醒借款方和债权人,可能发生欺诈行为:

Equifax Canada
1-800-465-7166

TransUnion Canada
1-866-525-0262

您也可以在线阅读《防范诈骗迷你宝典》,网址:
www.competitionbureau.gc.ca

知识就是力量！