社交媒体安全提示

如果您的社交媒体资料是公开的，请注意以下事项：

任何人都可以**查看、保存或截屏您发布的照片**、图像或评论， 包括您的雇主、同事、同学，以及任何可能怀有恶意的人。

请不要使用您的全名及/或您的面部图像作为个人资料照片和身份证明，也不要在个人经历描述中**透露个人身份信息**。

避免张贴任何关于您居住的社区、您经常去的地方、学校、工作地点等内容的图片或视频。因为其他人可以利用这些内容找到您。离开某个地点或活动后再发布相关图片：使用 ***#latergram***，并**关闭地理位置定位功能**。

是否因职业发展、宣传、政治原因等需要开设**公众帐号**？
不妨另设一个专用的**公众帐号**，与分享个人生活的私人帐号分开。

拥有众多粉丝是否对您很重要？您可以**适当减少个人信息的发布数量**，并参阅前文关于公众帐号的建议。

如果您的社交媒体资料是不公开的，请注意以下事项：

您私下认识每一位粉丝吗？**您是否跟所有粉丝都见过面**？如果您对上述任何一个问题的答案为“否”，那么不妨更新您的粉丝列表并定期查看。

在允许某人在社交媒体上关注您或与您成为好友之前，请查看他们的帐号以**确认真假**，并查看你们是否有共同好友。

更多提示：

下载 U of T Campus Safety 应用程序

- 全天候访问实时警报，了解安全相关事件或校园关闭信息
- 与 Campus Safety 实时聊天，用户可与多伦多大学的安保人员实时联系
- 访问 TravelSafer：允许 Campus Safety 在用户进出校园时监控行动路线，直到其到达目的地
- 访问 Mobile Bluelight：激活后，它会将用户在校园中的位置发送给 Campus
- 其他功能（例如 Friend Walk 和支持服务）可在世界各地为用户提供帮助。

国际留学生：

有关通常针对国际留学生的各种类型的欺诈和诈骗的更多信息，请访问加拿大政府的移民网站：

https://www.canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/internet-email-telephone.html

U of T Campus Safety 应用程序可在 Google Play 和 Apple Store 免费下载。

可为您提供帮助的资源：

如果您怀疑自己已成为欺诈目标，建议您向 ***Campus Safety*** 非紧急热线（如下）报告。

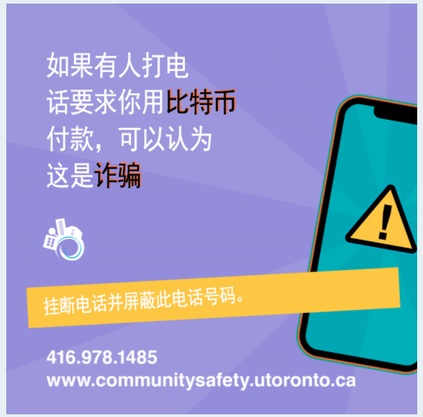
- **UTM Campus Safety** - 905-828-5200
- **UTSC Campus Safety** - 416-287-7398
- **UTSG Campus Safety** - 416-978- 2323

如果发生任何状况令您对自己或他人的安全产生顾虑，您都可以咨询 ***Community Safety Office***。如需获取服务支持，请拨打电话 416-978-1485，或发送电子邮件至 community.safety@utoronto.ca。

UNIVERSITY OF TORONTO | Community Safety Office

多伦多大学反诈信息与支持服务

www.communitysafety.utoronto.ca
community.safety@utoronto.ca
416-978-1485



欺诈类型

欺诈手法 1：“退回寄件人”

1. 受害者会收到快递公司关于包裹的电话留言。对方声称在一家快递公司工作。
2. 受害者会被“转接”给警方，然后被告知截获了一个寄给他们的包裹，其中包含非法物品。
3. 受害者会被告知他们将因参与其中而面临逮捕和驱逐出境，但可以支付罚款以避免入狱或被驱逐出境。

欺诈手法 2：“洗钱”

1. 受害者会接到一个自称为警方工作的人打来的电话。
2. 对方会告知受害者，他们的银行卡已被用于洗钱，银行账户将被冻结。
3. 受害者必须协助调查才能洗清嫌疑，在调查期间应将账户中的资金提取出来并通过比特币存入“安全系统”。
4. 对方会告知受害者，这笔钱将在调查结束时返还。

欺诈手法 3：“性勒索”

1. 受害者会通过社交媒体或约会网站遇到看似无害的人。
2. 施暴者最终会强迫受害者发送暴露的图片、在镜头前裸体或进行性行为。
3. 受害者会被告知，除非向施暴者汇款（或发送更多图像），否则这些图像将在网上与其家人等共享。
4. 在某些情况下，受害者会因为共享图像的威胁而被迫躲藏起来，并联系受害者的家人索要“赎金”。

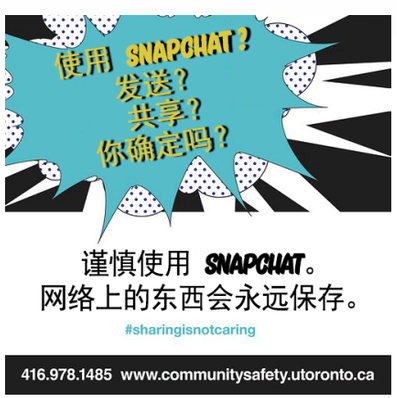
其他情境?

- 冒充 Service Canada 的法律部门打电话/发电子邮件，说有人对您提出指控。
- 冒充 Service Canada 的客服打电话/发电子邮件，说您的社会保险号 (SIN) 已被屏蔽、泄露或暂停。
- 打电话威胁说有一份针对您的逮捕令尚未执行，如果不立即付款则将被执行。
- 打电话威胁说，如果不立即付款，您将失去签证或身份，或被驱逐出境。
- 打电话/发电子邮件说您的电脑感染了病毒。来电者或发件人会提议帮您删除电脑中的病毒。此人会尝试获取您的电脑密码和其他私人信息。
- 接到电话/电子邮件说您获奖了，但您并没有参加过任何比赛。请不要输入任何信息并删除此信息。如果收到信息告诉您“如果不想再收到类似信息，请发送‘STOP’或‘NO’”，请删除此信息。请勿回复。骗子这样做是为了确认这是否是真实的电话号码。

欺诈是什么样的？我该怎样应对？

如果有人联系我试图进行欺诈，我该怎么办?

- 不要轻易相信手机上的来电显示。骗子会设法将来电显示改为“警察”等，而实际上他们是不合法的。
- 加拿大政府官员不会直接联系您并索取金钱来保护您的加拿大身份。
- CRA 或 Service Canada 绝不会要求您通过电子转账、比特币等数字货币，或预付信用卡付款。
- 政府官员不会要求您通过比特币等数字货币将资金转给他们来确保您的资金安全。
- 如果 CRA 给您发放款项，会通过直接存款或邮寄支票的方式放款。
- 加拿大政府不会接受通过西联汇款、Money transfer、预付信用卡或电汇方式向国外的付款。
- CRA 或政府官员绝不会使用攻击性语言，也不会以逮捕或派警察来威胁您。



如果您收到这些类型的电话或联系，可采取以下措施：

- 如果有人索要金钱或个人信息，请提高警惕。
- 不要付款或提供个人信息。如果您有任何怀疑，请向来电者询问员工号码并挂断电话。在网上查找该公司（例如 CRA 或 IRCC），给他们打电话确认来电者提供的员工编号和提出的请求是否合法。
- 致电 Campus Safety (416-978-2323) 请求帮助，以确认来电者的合法性。
- 向 Canadian Anti-Fraud Centre (https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm)、Campus Safety (416-978-2323) 或多伦多警察局 (416-808-2222) 报告。

如果有人威胁要发布或分享您的私密照片怎么办?

- 不要不好意思。 您可以给 Community Safety Office 打电话（416-978-1485）预约，讨论您可以采取哪些措施。
- 也可以向 Campus Safety (416-978-2323) 或多伦多警方 (416-808-2222) 报告。
- 无论您是否认识威胁您的人，都请截取他们的网址/姓名/电子邮件地址/Twitter handle的屏幕截图。
- 保存并复制已发送给您的所有信息。 您在向警方报案时可能需要提供这些信息。
- 不要继续回应或与对方接触。
- 考虑更改您的社交媒体帐号密码，并/或暂时停用帐号。