Grassroots Digital Hub

网络安全提示

1. 保护你的设备

- 锁定你的设备。 给你的手机、笔记本电脑或其他设备设置密码。
  - 这可以在设备丢失或被盗时保护你的信息。
- 备份你的数据。 大多数设备都提供免费备份服务，但存储空间可能有限。
  你可以在 WikiHow 上了解如何进行备份。
  - 备份是设备上所有内容的副本。如果你的设备丢失或损坏，你可以从备份中恢复数据。
  - 备份通常保存在设备以外的地方，一般是在“云端”。
    云端是由 Google 等公司运营的计算机网络。
- 进行软件更新。许多更新都能提高安全性。
- 及时退出登录。使用完应用或网站后，请务必注销，以提高安全性。

2. 注意密码安全

- 使用长密码。使用大小写字母、数字和符号
  - 创建你容易记住的短语，例如：2-H@ppy-Small-Kids&Me
- 尽量为每个账户使用不同的密码。
- 使用密码管理器。这能帮你管理所有密码！
  - 一些浏览器，如 Firefox 和 Chrome，或者操作系统，如 Windows，提供免费的密码管理功能。
- 部分密码管理器提供双重验证（Two-Factor Authentication）。 这意味着登录时需要两个步骤，虽然稍慢一些，但更安全。

3. 注意网络连接安全

- 如果你家中有互联网连接，请使用强密码，以便只有知道密码的人才能访问。
- 如果你使用免费或公共 Wi-Fi：
  - 使用 VPN。有很多免费 VPN，例如 ProtonVPN。
  - VPN 会加密（设为私密）连接，从而保护你的设备免受病毒侵害，并防止你的数据被盗。

4. 掌控你的隐私

- 设置：设备、网站和大多数应用程序都可以保护你的数据，但你必须进行设置。
  - 在设备或应用中查找“设置”或“隐私”（例如 Google、Instagram、ChatGPT）
  - 如需更多帮助，请搜索应用或设备名称以及“如何设置隐私”
- 历史记录：你可以在网页浏览器和 AI 账户中“清除历史记录”。
- Cookies：当网站询问“是否允许 Cookies”时，请选择“仅接受必要的”，或取消勾选“广告”或“定向”。
- 社交媒体：想想你想让谁看到你的社交媒体账号。试图与你建立联系的陌生人可能是收集你数据的机器人。
- 信用卡：避免在网站上保存信用卡信息。

> 你的数据 — 包括你在网上做什么、看什么、买什么的信息 — 非常有价值，但公司却不愿为此付费

5. 让我们一起保持安全

- 点击诱饵（Clickbait）： 如果你看到让你生气或不安的内容，先停下来，深呼吸。这可能是诱导你点击、分享或继续阅读的陷阱。
- 在分享之前
  - 确认你分享的链接是安全的
  - 确认你分享的信息是真实的
  - 清楚说明为什么他人可能会对该链接或内容感兴趣
- 询问亲友
  - 如果你不介意分享他们的信息和照片的话
  - 他们在网络上采取哪些措施来感受到尊重并尊重他人

更多信息请访问

- GetCyberSafe.ca — 加拿大政府提供的网站，包含保护个人身份安全、防范网络钓鱼诈骗等实用提示。
- SecurityPlanner.ConsumerReports.org — 该网站介绍如何保护你的在线信息安全。该工具最初在加拿大创建，目前由一家美国非营利组织运营。

SSHRC CRSH
Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
NSERC CRSNG
We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council.