National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

确保您组织的在线安全

为什么网络安全对社区团体和组织很重要？

本页面提供建议和一些步骤，您可以利用这些来保护您的社区团体或组织免受网络安全威胁。还有一份给个人的单独指南帮助他们在网上保护自己的安全。

这些建议是基于最常见和最严重的威胁来做出的。

- 更新——保持设备上的软件为最新版本，以修补任何安全漏洞。
    - 及时为社区团体或组织的设备进行更新。这包括手机、电脑、WiFi 路由器以及连接到互联网的任何其他设备——包括智能设备。
    - 在可能的情况下尽量使用自动更新。
- 双重身份验证 (2FA) ——通过要求输入密码外加另一个步骤（例如来自手机应用程序的代码）来为您的账户增加额外的安全性。
    - 注：这也称为多重身份验证（MFA）、两步验证（2SV），及许多其他名称。
    - 在您所有的社区团体或组织的账户上启用 2FA。
    - 如果可能的话，尽量使用一种能够防止网络钓鱼的 2FA 形式，这意味着骗子无法诱骗您交出信息。这可以是一把实物安全密钥或者像指纹或扫脸验证之类的东西。
- 严格管理您的在线账户——确保前成员在离开社区团体或组织后不会保留对账户的访问权限。
    - 如果有多人访问同一个账户，请确保他们都使用不同的登录名，并且都启用了 2FA。
    - 保留所有用户账户的列表，并关闭不需要的账户（例如当员工离开时）。
    - 保留一份您提供给成员的所有设备的登记册，并记得在该成员离开组织时将设备收回并恢复出厂设置。您可能还需要更改进入大楼建筑物的门禁密码。
- 检查谁有权访问您的在线账户——您的社区团体或组织中的人员应该只能访问他们需要的内容。
    - 如果一个人的账户被黑客入侵，这些步骤可以限制攻击者可能造成的危害。
    - 定期检查并删除不必要的权限。
    - 如果您有一个“管理员”账户供多人使用，请监视该账户是否存在异常活动。尽量减少使用这类账户，尤其是针对日常任务。
    - 这些规则也适用于管理员对设备（如路由器）的访问。
- 如果您雇用了服务提供商为您提供 IT 服务，请审查您与他们签订的合同。
    - 确保他们有网络安全保护措施来满足您的社区团体或组织的需求。
- 了解您的所有账户和系统如何协同工作——了解这些连接有助于您知道攻击者可以从哪里侵入。
    - 检查您的各个系统之间的连接，例如电子邮件、云存储和财务管理平台。

- 考虑使用虚拟专用网络（VPN）来进一步增强在线安全性。使用 VPN 可以隐藏您的在线活动，防止任何试图追踪您的人看到您的在线活动。如果您的社区团体或组织有任何成员进行远程连接，这尤其有用。

- 让您的员工保持“网络安全意识”——您的社区团体或组织中的人员比您的系统更容易成为被攻击的目标。
    - 对所有员工进行基本的网络安全培训。Own Your Online（自主管理网络安全）网站 Own Your Online |NCSC 提供广泛的建议和技巧，可帮助您确保在线安全以及识别诈骗。
    - 提醒他们这对于他们的个人账户以及他们在您的组织中使用的账户都很重要。
    - 我们也为个人提供了确保自己在线安全的指南。
- 为突发事件制定计划——制定应对计划非常重要，这样可以防止人们在事件发生时惊慌失措。
    - 突发事件应对计划概述了事件发生期间谁做什么。模板可在此处获取 Incident Management |NCSC（突发事件管理 | 国家网络安全中心）
    - 包括一个当电话、电脑或其他系统失灵时应采取什么行动的应对计划。经常更新这个计划。
    - 保留所有必要人员的联系方式，并准备备用联系方式，以防主要联系方式（如电子邮件）无法使用。
    - 将计划同时保存在系统之外的某个地方，以防您无法进入系统访问它。