National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

保障您的組織的網路安全

為什麼網路安全對社區團體及組織至關重要？

本頁提供建議及一些您可以採用的步驟，有助保護您的社區團體或組織免受網路安全威脅。另外亦有一份專門用於個人保護自身上網安全的指南。

我們針對最常見且最嚴重的網路安全威脅提供以下建議。

- 及時更新 – 保持您設備上的軟體為最新版本，以修補任何安全漏洞。
    - 確保及時更新您的社區團體或組織使用的設備。這包括手機、電腦、WiFi 路由器以及所有接入網路的設備，亦包括智能設備。
    - 儘可能啟用自動更新。
- 雙重驗證（2FA） – 透過輸入密碼要求及額外步驟（例如來自手機應用程式的驗證碼），為您的賬戶增加額外的安全保障。
    - 注意：又稱為多重驗證（MFA）、兩步驟驗證（2SV）等衆多不同名稱。
    - 請為您社區團體或組織的所有賬戶啟用雙重驗證。
    - 儘可能嘗試使用有防網路釣魚功能的雙重驗證方式，確保您不會因為被騙而交出驗證資料。這可以是實體安全金鑰，亦或類似指紋或人臉識別的方式。
- 持續追蹤管理您的網路賬戶 – 確保已離開社區團體或組織的前成員不再有權登入賬戶。
    - 如果有多人使用同一賬戶，請確保每個人都使用不同的登入資料，並且均已啟用雙重驗證。
    - 根據賬戶的所有使用者整理一份賬戶清單，並停用任何不再使用的賬戶，例如員工離職時停用其賬戶。
    - 根據您已分配給成員的設備整理一份設備清單，並記得在相關成員離開組織時等收回其設備並恢復出廠設置。您亦可能需要更改進出大樓時使用的門禁密碼。
- 查看哪些人能訪問您的網路賬戶 — 社區團體或組織中的成員的訪問權限應僅限於他們的實際需要。
    - 如果某人的賬戶遭駭客入侵，以下方法可以減低駭客攻擊造成的損害。
    - 定期檢查並移除不必要的權限。
    - 如果您有一個多人共用的「管理員（admin）」賬戶，請監控其是否有異常活動。儘量不要設置此類賬戶，尤其避免將其用於日常工作。
    - 這些規則亦適用於設備（例如路由器）的管理員訪問權限。
- 請審查與 IT 服務提供商的合約 – 如果您雇用他人來提供該服務。
    - 確保其已爲您設置網路安全防護措施，以滿足您社區團體或組織的需求。

- 了解您的所有賬戶和系統如何協同運作 – 理解其中的連結方式有助於您知道攻擊者可能會從何處入侵。
    - 審查您的系統之間的連結方式，例如電郵、雲端儲存和會計平台。
    - 考慮使用虛擬私人網路（VPN）進一步增強網路安全。使用 VPN 可以隱藏您的網路活動，防止他人試圖追蹤您。當您的社區團體或組織的成員有遠端連線需求時，VPN 更能發揮效用。
- 令大家保持「網路安全意識」— 與系統相比，社區團體或組織中的成員往往更容易成為攻擊目標。
    - 為所有員工提供網路安全的基礎培訓。「Own Your Online（自主管理網絡安全）」網站 Own Your Online | NCSC 提供內容廣泛的建議和技巧，助您安全上網並識別詐騙手法。
    - 提醒員工，保持網路安全意識不僅對其個人賬戶至關重要，對於其在組織所使用的賬戶而言同樣重要。
    - 我們亦準備了一份供個人使用的指導手冊，幫助大家安全上網。
- 為突發事件制定計劃 — 提前準備應對計劃十分重要，可以避免事件發生時引起恐慌。
    - 突發事件應對計劃應概述在突發事件中每個人應該負責的事項。此處提供範本：Incident Management | NCSC（突發事件應對管理 | 紐西蘭國家網路安全中心）
    - 其中亦應有相應計劃，說明手機、電腦或其他系統發生故障時的處理方法。及時更新該計劃。
    - 保留所有必要聯絡人的聯絡方式，並保留備用聯絡資料以防主聯絡方式（如電郵）失效。
    - 將計劃存放於系統之外的地方，以避免您需要時無法獲取的問題。