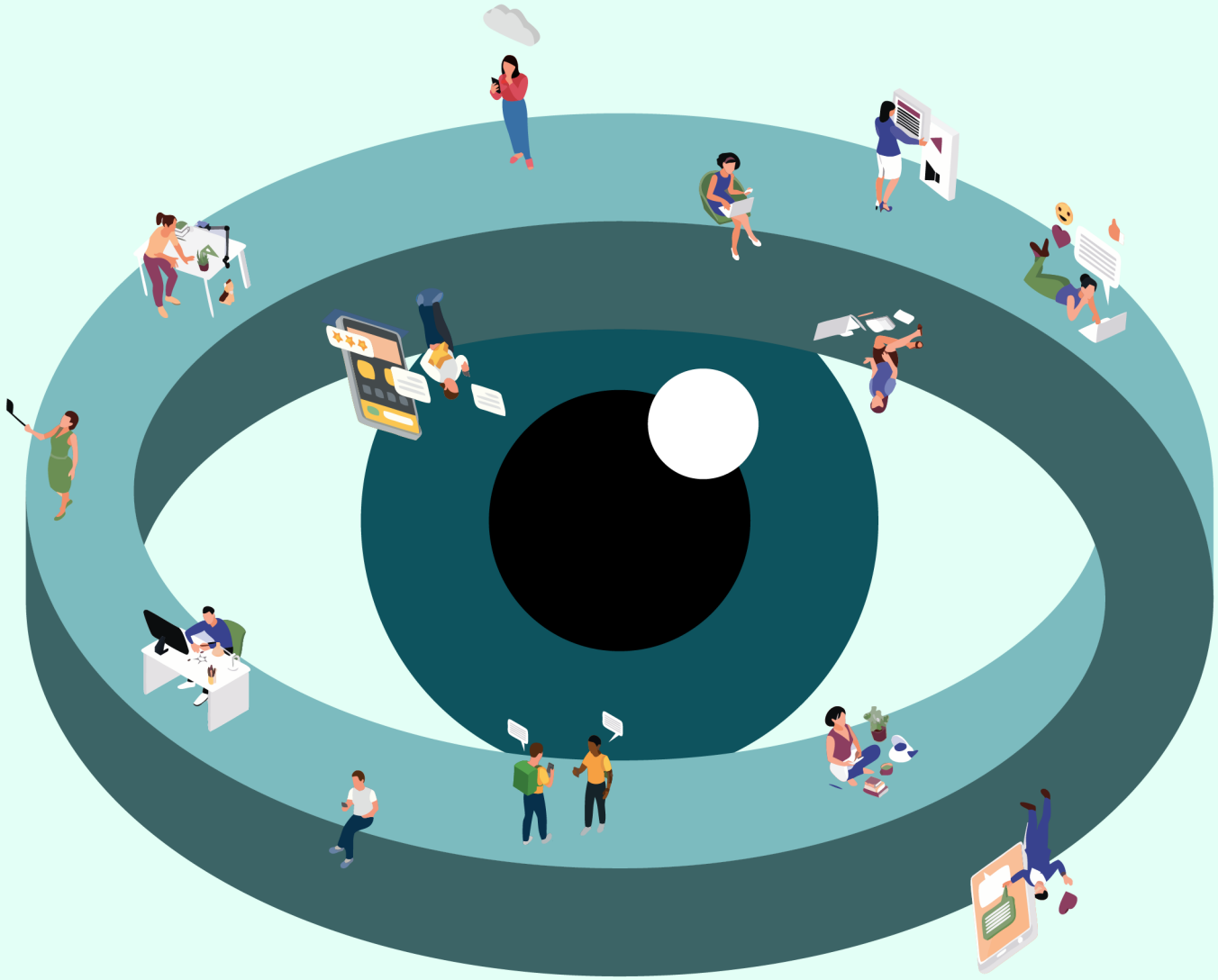
處變不驚

公民社會資訊安全韌性指南



聲明

本手冊之內容僅供教育用途。所有內容均可在網上查閱，並不構成資訊安全、法律或其他事項的專業意見。如有需要，請向相關專業人士諮詢，以獲取具體的行動建議。本手冊內容反映截至撰寫時的法律及技術環境，讀者宜定期查閱最新修訂。

版權



© 2026 韌性創新實驗室 Resilience Innovation Lab

除另有註明外，本手冊採用 Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International（CC BY-NC-SA 4.0，CC「署名－非商業性使用－相同方式共享」4.0 國際）授權條款發佈。

在遵守上述授權條款的前提下，任何人均可複製、分享、傳播及改作本書，惟必須清楚標示作者／來源，提供授權條款連結，並註明是否曾作修改；不得將本書用於商業用途；如改作、轉換或建基於本書創作，須以相同的 CC BY-NC-SA 4.0 授權條款發佈相關作品。

授權條款全文請見：https://creativecommons.org/licenses/by-nc-sa/4.0/

第三方版權材料除另有註明外，不受本書之 CC BY-NC-SA 4.0 授權涵蓋；使用者須就該等材料另行向相關權利持有人取得使用許可。

韌性創新實驗室
Resilience Innovation Lab

https://resilienceinnovationlab.org/
info.ril@proton.me

快 速 參 考

緊急情況清單

懷疑設備被入侵時：

1. 立即斷開網絡連接
2. 移除未知登入裝置
3. 更改所有密碼
4. 啟用封鎖模式（iOS）
5. 考慮重置設備

出入境前：

1. 備份所有重要資料至安全雲端
2. 清除設備敏感資料
3. 準備沒有連上個人資料的備用設備
4. 設定安全聯絡人
5. 確認 VPN 可用

推薦工具一覽

類別	推薦工具
密碼管理	KeePassXC, Bitwarden
雙重驗證	2FAS, Aegis（Android）, Yubico Authenticator
加密電郵	Proton Mail（僅限收件人寄件人同為ProtonMail帳戶）
即時通訊	Signal, Session, Wire, Delta Chat
VPN	Proton VPN, Mullvad VPN, Lantern VPN
檔案加密	Cryptomator, VeraCrypt
安全瀏覽器	Brave, Firefox, DuckduckGo

應對監控技術與方法



概述

面對日益嚴密的監控環境，減少網絡足跡和分隔網絡身份是保護私隱的基礎策略。本章介紹實用的技巧，幫助你降低被追蹤和識別的風險。

1 減少網絡足跡的實務

甚麼是網絡足跡？

類型	例子
主動足跡	社交媒體帖文、電郵、註冊帳戶
被動足跡	瀏覽記錄、IP 位址、裝置序號、設備元數據

基本原則：- 知情原則：了解你提供資料、披露對象、目的
- 必要性原則：只提供完成任務所必需的最少資料

伺服器端追蹤 Server-side Tracking（SST）

為減少網絡行為數據被直接分享予分析與廣告平台，可在傳送訊息或點擊連結前，先清除社群媒體連結追蹤碼。具體做法：在分享或送出前，將網址中問號「?」及其後的所有字元刪除

類型	例子
傳統追蹤	https://youtu.be/Aq5WXmQQooo?si=1Eg_ninop5NwfHs0
SST追蹤	https://youtu.be/Aq5WXmQQooo

電子郵件安全設定

像素偵查原理：

攻擊者在電郵中嵌入隱形追蹤像素

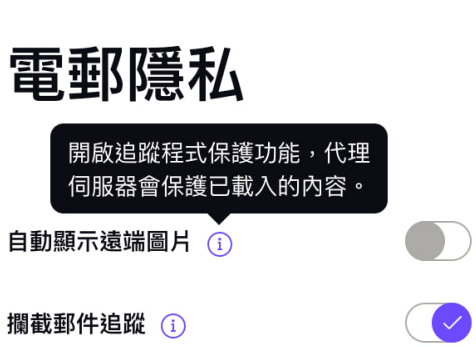
↓

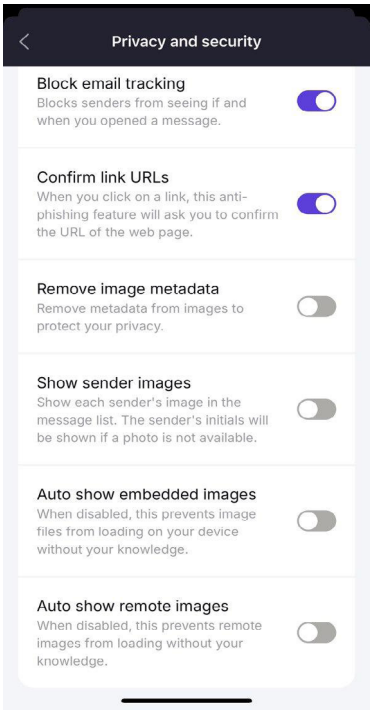
你打開電郵，瀏覽器自動載入遠端圖片

↓

攻擊者伺服器記錄你的：IP 地址、設備資訊、開啟時間、地理位置

電郵服務	設定路徑
Gmail	設定 → 一般設定 → 圖片 → 顯示外部圖片之前詢問
Proton Mail	設定 → 安全和隱私 → 自動顯示遠端圖片 → 關閉
Apple Mail	設定 → 隱私保護 → 保護郵件活動





化名電郵策略

服務	特點
Firefox Relay	可創建多個別名，指向同一收件箱
Proton Mail 別名	可創建多個別名，指向同一收件箱
SimpleLogin	無限別名，與 Proton 整合

2 分拆數位與實體身分

公私分明原則

設備	用途	注意事項
個人手機	銀行、公共服務（稅務、醫療）	使用真實身份
工作手機	敏感工作、研究、倡議活動	使用化名，不與個人生活混用

工作手機設定原則

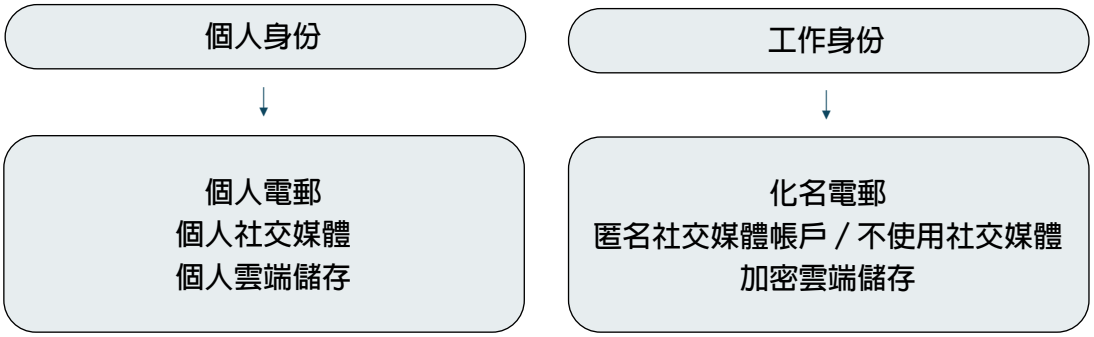
基本要求：

- 使用新的 Apple ID 或 Google 帳戶（不要登入個人帳戶）
- 使用非實名制的 SIM 卡
- 僅使用安全 Wi-Fi/VPN（推薦：Proton VPN、Mullvad VPN）
- 不要在工作手機上處理任何私人事務
- 將可識別個人資訊減到最少

進階設定：

- 關閉所有自動同步功能
- 使用 VPN 連接網絡
- 定期清除瀏覽記錄和緩存

帳戶隔離策略



SIM 卡類型	用途	建議
實名 SIM 卡	個人日常使用	與敏感活動完全分開
非實名 SIM 卡	工作手機上網	在私隱友善地區購買
預付卡	臨時使用	用完即棄

清理習慣

每日清理：

□ 清除瀏覽器緩存和歷史記錄　　□ 刪除不必要的螢幕截圖

□ 檢查並刪除下載資料夾中的臨時檔案

每週清理：

□ 審視相簿中的照片，刪除或加密敏感圖片　　□ 檢查應用程式權限

□ 清除即時通訊應用的媒體緩存

每月清理：

□ 審視社交媒體帖文和標籤　　□ 檢查已登入的設備和活躍工作階段

□ 更新或輪換密碼

3 代號策略

建立有效的化名身份

原則	說明
一致性	同一個化名在相同語境中保持一致
獨立性	不同用途使用不同化名
無關聯性	化名不應與真實身份有明顯關聯

避免的錯誤：

- ☒ 使用真實姓名的變體（如諧音）
- ☒ 使用生日、電話號碼等個人資訊
- ☒ 在多個平台重複使用同一化名
- ☒ 使用可追溯到真實身份的暱稱

身份隔離舉隅

活動類型	設備	帳戶	網絡	身份
日常社交	個人手機	真實帳戶	一般網絡	真實身份
敏感工作	工作手機	化名帳戶	VPN	化名
高風險活動	專用設備	一次性帳戶	Tor	匿名

檢查清單

- ☐ 關閉電郵的自動載入遠端圖片功能
- ☐ 建立至少一個化名電郵帳戶
- ☐ 評估是否需要設置獨立的工作手機
- ☐ 制定定期清理網絡足跡的習慣
- ☐ 審視聯絡人列表，使用代號替代敏感聯絡人的真實姓名
- ☐ 確保不同身份的帳戶之間沒有關聯

RESILIENCE
INNOVATION
LAB