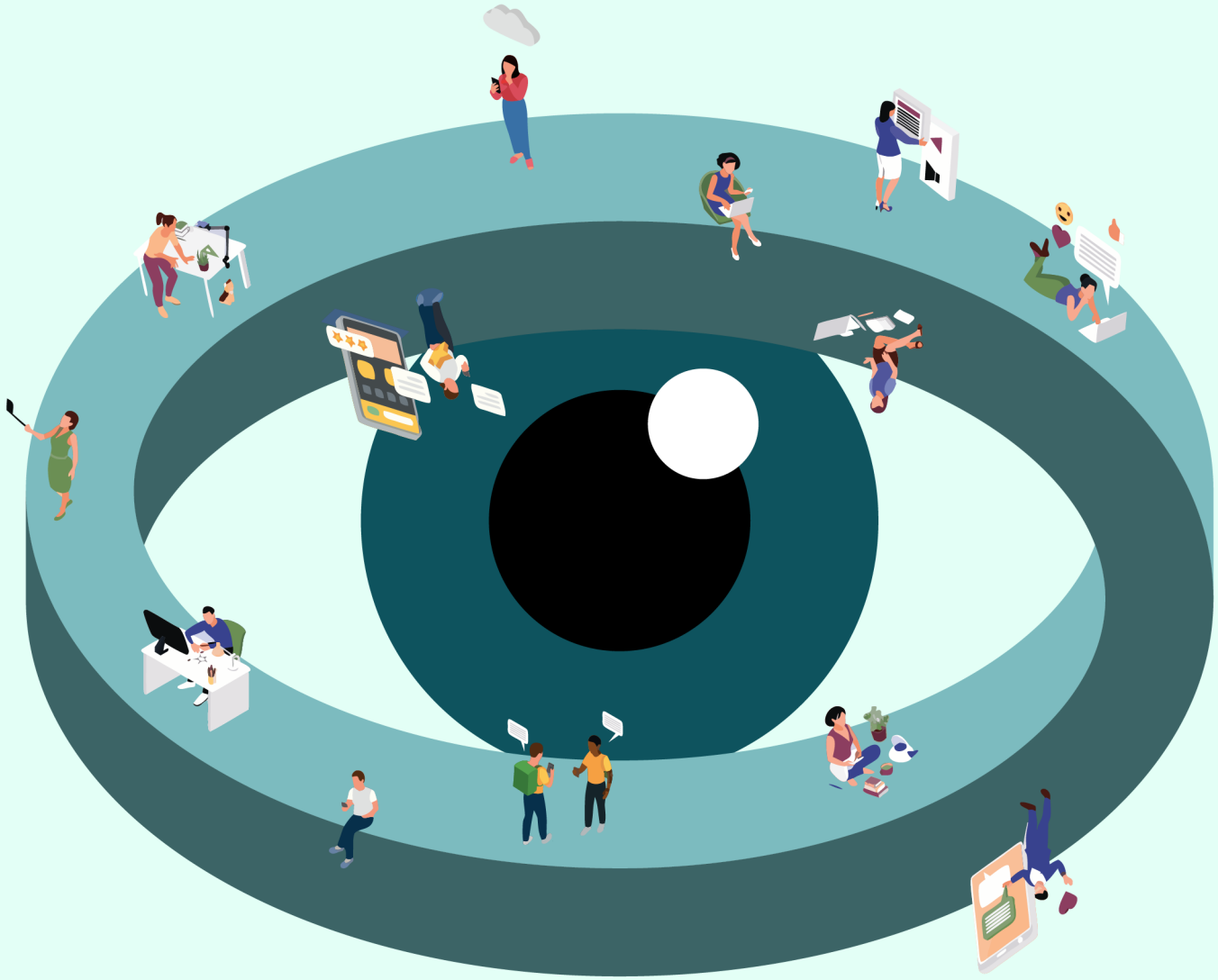
處變不驚

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

出入境安全



概述

跨境旅遊或工作時，電子器材會面臨另一類風險。本章提供出入境時保護資訊安全的完整指南，按「出發前—旅途中—回程後」時間軸編排。

1 出行前準備

三個基本問題

出行前，先問自己：

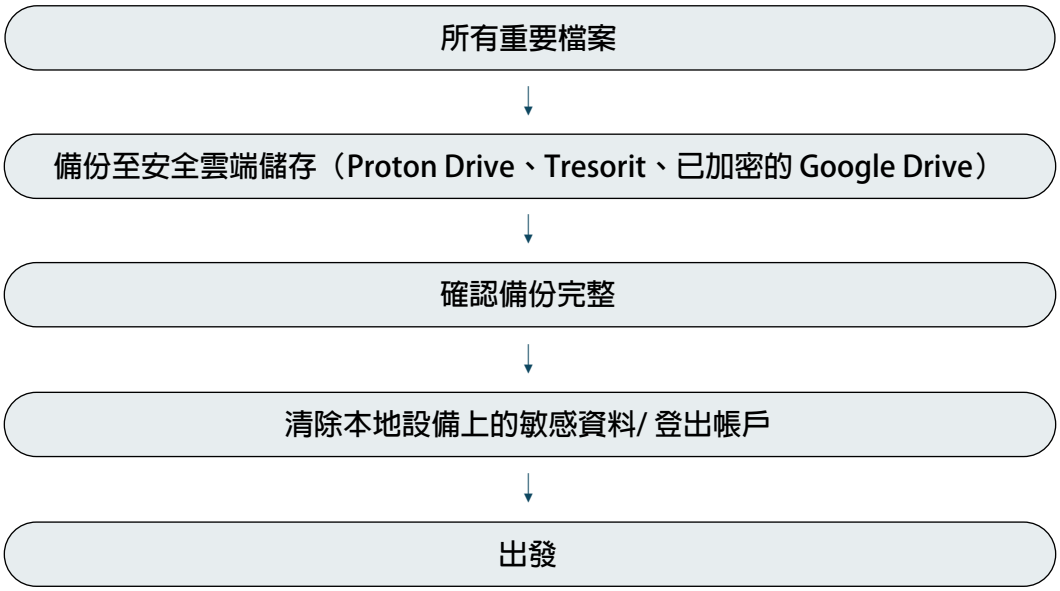
1. 是否需要攜帶存有個人資料的常用設備？
    - 考慮攜帶專用設備而非日常設備
2. 哪些資料是必需的？
    - 只攜帶行程所需的最少資料
3. 如果設備被盜，或被檢查或扣押，後果是甚麼？
    - 評估風險並做好應對準備
    - 2026年起，當局可即場要求提供密碼及解密協助，拒絕遵從有具體法律後果。設備上保存的資料愈少，可降低當場面對的風險。

設備選擇策略

風險級別	建議設備	說明
低風險	日常設備（清理後）	清除敏感資料，加密備份到雲端
中風險	專用筆記型電腦	不儲存敏感資料，只保存必要聯絡人
高風險	即棄手機	用完即棄，不與個人身份關聯

2 設備清理與備份

備份策略



清除敏感資料

類別	項目	方法
通訊記錄	Signal、WhatsApp 對話記錄	刪除對話或清空應用資料
瀏覽記錄	瀏覽器歷史、Cookie	清除所有瀏覽數據
圖片	圖片、螢幕截圖	刪除或移至加密雲端
文件	文件、下載資料	刪除或移至加密雲端

3 安排安全聯絡人

設定應急計劃

項目	範例
報平安時間	每天/ 隔天固定時間聯絡（如每晚9點）
聯繫方式	主要：Signal； 備用：Wire、Delta Chat
暗號	確認安全/ 有風險的代號
失聯應對	逾時未聯絡應採取什麼行動
緊急聯絡人	律師、家人、組織的聯絡方式

4 出行安全注意事項

設備安全： - 切勿讓手機或電腦無人看管 - 務必隨身攜帶所有設備 - 離開房間時將設備帶走或鎖在保險箱 - 自備叉電器 / 流動叉電裝置

通訊安全： - 避免使用酒店 Wi-Fi 進行敏感操作（改用手機數據 + VPN） - 假設在酒店房間內所說的任何話都可能被錄音 - 敏感對話應在室外或使用加密通訊

5 邊境檢查應對

了解你的權利

根據2026年修訂的國安法《實施細則》，在香港，當局有權在特定情況下以國家安全為由檢查電子設備，拒絕配合或提供失實回應可能會帶來法律後果。前往其他司法管轄區時，亦需留意當地對邊境檢查與電子設備的法律授權範圍。

小結：出發前的資料清理，比臨場的法律理據提供更可靠的保護。
設備上保存的資料愈少，可降低當場面對的風險。

降低風險的措施

出發前：

1. 清除或轉移敏感資料
2. 登出所有敏感帳戶
3. 關閉生物識別解鎖
4. 考慮使用專用旅行設備

檢查時：

1. 保持冷靜和禮貌
2. 了解被要求做甚麼
3. 如條件許可，要求聯繫律師——惟臨場等候法律意見的空間有限；**事前準備比臨場應對更為關鍵**
4. 在安全情況下，記錄被查過程

6 回程後處理

設備檢查

- 設備是否有被物理開啟的痕跡？
- 是否有新安裝的應用程式？
- 系統設定是否有變更？
- 是否有異常的登入活動？

懷疑設備被入侵

簡單自我檢查：

- 數據流量異常增加？（設定 → 行動服務 → App 數據使用）
- 電池異常快速耗盡？（設定 → 電池 → 電池用量記錄）
- 在閒置時手機仍然過熱？
- 通訊程式有異常行為？
- 應用程式權限異常？

工具	平台	用途
Knock Knock	macOS	檢測異常啟動項目

應對步驟：

1. 更新系統 — 安裝最新版本
2. 移除未知登入 — 檢查並移除所有活躍工作階段
3. 更改密碼 — 更改所有重要帳戶密碼
4. 啟用封鎖模式 — iOS 用戶啟用封鎖模式
5. 重置設備 — 如有需要，完整重置為原廠設定
6. 不要還原舊備份 — 使用「全新設定」
7. 尋求專業幫助 — 聯絡可信任的資安團隊進行鑑證分析

出入境安全檢查表

出發前

- ☐ 評估是否需要攜帶日常設備
- ☐ 加密備份所有重要資料到安全雲端
- ☐ 清除設備上的敏感資料
- ☐ 設定安全聯絡人和應急預案
- ☐ 確認 VPN 可用

旅途中

- ☐ 隨身攜帶所有設備
- ☐ 使用 VPN 連接網絡
- ☐ 定期向安全聯絡人報平安
- ☐ 避免在酒店房間討論敏感話題
- ☐ 定期檢查帳戶活動

回程後

- ☐ 檢查設備是否有異常
- ☐ 檢查帳戶登入活動
- ☐ 確認安全後從雲端恢復必要資料
- ☐ 如有疑慮，考慮重置設備

RESILIENCE
INNOVATION
LAB