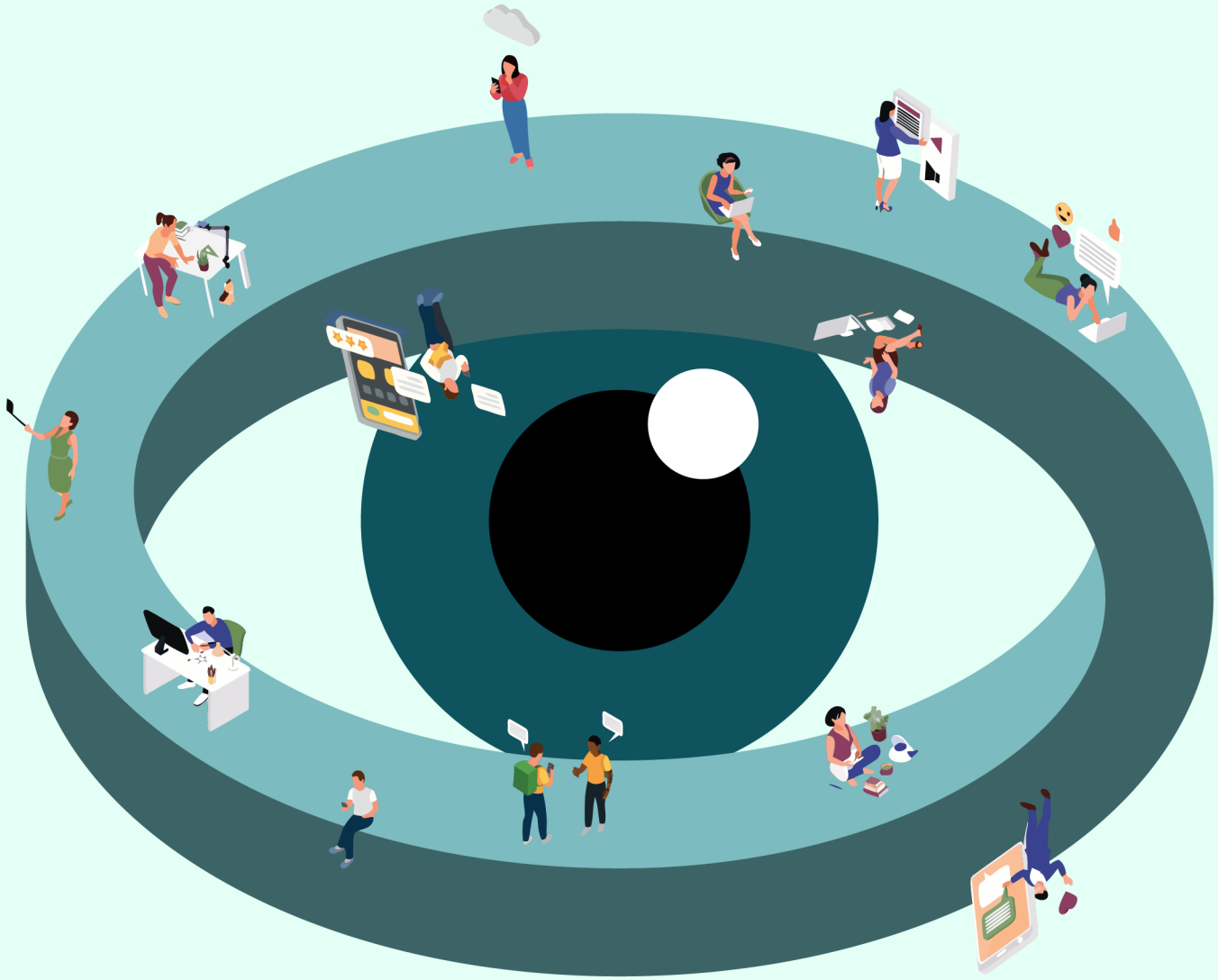
處變不驚

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

通訊安全



概述

安全通訊是保護敏感資訊的關鍵。本章涵蓋加密電郵、通訊應用程式，以及社交媒體與瀏覽器的私隱設定。

1 電郵設定

為何選擇 Proton Mail？

特點	說明
端對端加密	如寄件人及收件人同使用ProtonMail帳戶，電郵內容具有加密（電郵標題除外）
瑞士法律保護	較嚴格的私隱法規
開源	程式碼可供審查
免費版可用	基本功能免費

安裝與設定

1. 連接安全 VPN/ Tor Browser（避免使用香港伺服器）
2. 使用 Proton Mail 應用程式或使用安全瀏覽器訪問 proton.me
3. 使用隨機用戶名，不要包含個人資訊
4. 設定長而強的密碼（與其他帳戶不同）
5. 避免輸入個人信用卡資料，及私人電話或電郵作帳戶恢復資料

基本帳戶設定：

1. 啟用雙重驗證：設定 → 安全 → 雙重驗證 → 開啟
   （使用驗證器應用程式，非SMS驗證）
2. 封鎖遠端內容：設定 → 安全和隱私 → 自動顯示遠端圖片 → 關閉

注意：電郵屬於早期技術，較容易留有元數據(Metadata)。如需要處理敏感通訊，宜改為使用Signal。

Proton Drive 安全分享

- 如非必要，避免以電郵附件形式直接傳送敏感檔案，優先使用設有密碼及過期日的分享連結
- 密碼和分享連結應透過不同通道傳送
- 當檔案已分享完畢時，登入 Proton Drive 手動停用或刪除連結

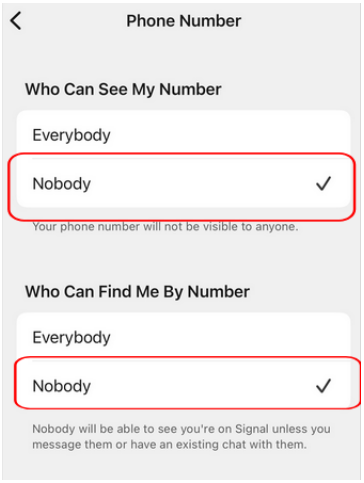
2 Signal 設定

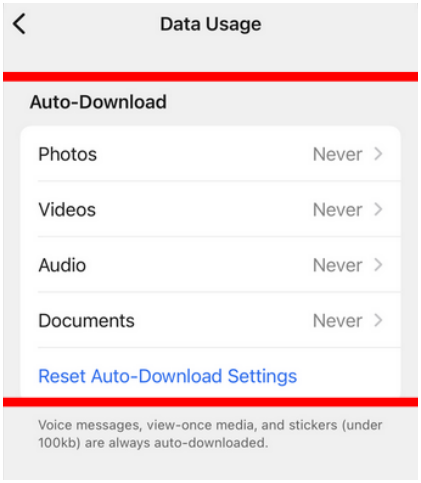
安全設定

設定	路徑	建議
Signal PIN	帳戶 → Signal Pin	設定強 PIN
註冊鎖定	帳戶 → 註冊鎖定 → 開啟	防止號碼被盜用
電話號碼	私隱 → 電話號碼 → 無人	隱藏號碼
訊息自動銷毀	私隱 → 訊息自動銷毀	8小時至1天
螢幕鎖定	私隱 → 螢幕鎖定 → 開啟	逾時1分鐘

使用情境與群組管理

- 將不同風險層級的對話分開
- 在高風險群組中預設較短的「訊息自動銷毀」時限
- 定期檢視舊對話與群組，如無需保留，請整個對話刪除





3 WhatsApp 及 Telegram 注意事項

WhatsApp

應設定	應避免
啟用雙重驗證	在個人檔案中使用真實姓名
使用臨時群組聊天進行短期溝通	發送未加密的敏感檔案
關閉自動下載媒體（圖片、影片）	將聊天同步到雲端（Google Drive、iCloud）

重要提醒：WhatsApp 的元數據（誰與誰通訊、何時通訊）可能被 Meta 收集、分析及訓練AI模型。

Telegram

應設定	應避免
僅使用秘密對話	在普通聊天中分享敏感資訊
在秘密聊天中啟用限時器	在公開群組/ 頻道中分享敏感資訊

重要提醒：Telegram 預設對話並沒有端對端加密，其「秘密對話」(Secret Chat) 的端對端加密方式亦未有公開審計認可，故不會推薦使用。

4 社交媒體私隱設定

通用原則：

- 啟用雙重驗證
- 移除電話號碼
- 限制搜尋範圍
- 謹慎標註用戶
- 注意背景：發布照片前檢查位置資訊和背景細節

5 安全瀏覽器

功能	Brave	Firefox
私隱重點	高	高（需手動調整設定）
廣告/追蹤器封鎖	內建 + 可自訂	需安裝 uBlock Origin
Tor 支援	Android	沒有

瀏覽器安全性設定檢查表：

□ 僅使用 HTTPS

□ DNS over HTTPS（DoH）

□ 自動更新

□ 安裝廣告攔截擴充功能（uBlock Origin）

□ 安裝反追蹤擴充功能（Privacy Badger）





通訊安全檢查表

電郵

- ☐ 設定 Proton Mail 並啟用雙重驗證
- ☐ 關閉自動載入遠端圖片
- ☐ 使用限時郵件功能

即時通訊

- ☐ 安裝並設定 Signal
- ☐ 設定訊息自動銷毀
- ☐ 使用化名和中性頭像
- ☐ 隱藏電話號碼

社交媒體

- ☐ 限制應用程式存取相簿
- ☐ 移除帳戶中的電話號碼
- ☐ 將專頁管理與個人帳戶分離

瀏覽器

- ☐ 安裝安全瀏覽器
- ☐ 啟用 VPN 後再瀏覽
- ☐ 使用無痕模式
- ☐ 瀏覽後清除歷史記錄

RESILIENCE
INNOVATION
LAB