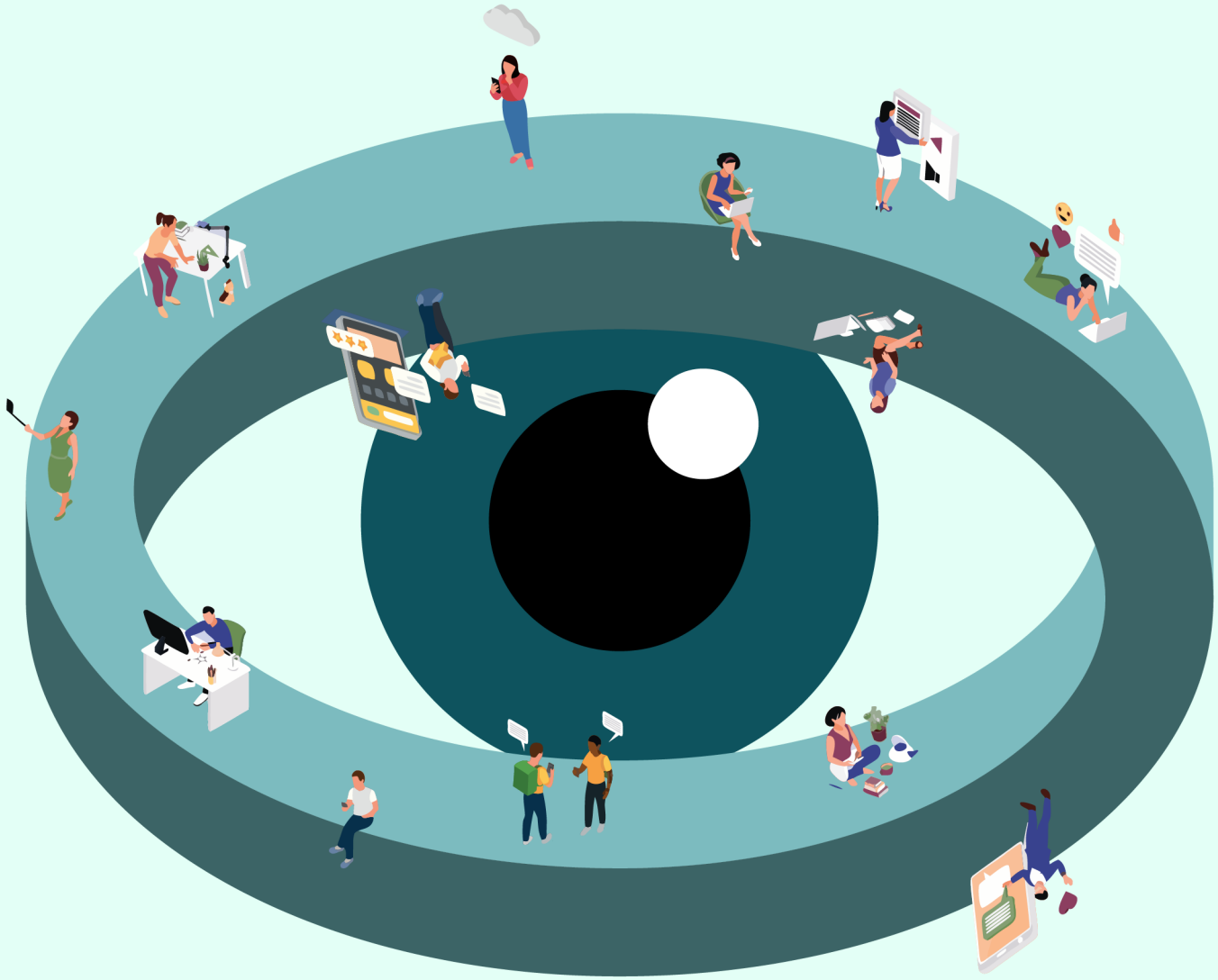
處變不驚

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

設備安全



概述

設備安全是資訊安全的基礎。本章涵蓋從初始設定到加密工具的指南，幫助你建立更安全的設備環境。

1 安裝設定

選擇安全環境

- 切勿將新設備連結至先前的 Apple ID 或 Google 帳戶
- 在已連接 VPN 的環境下進行設定
- 選擇數據儲存於私隱法規嚴格地區的服務（如瑞士、德國）

工作電話設定步驟

iOS系統：註冊Apple ID

1. 預備工作電話註冊用之電話號碼（非香港電訊商註冊號碼），註冊Apple ID用
2. 預備ProtonMail電郵帳戶，註冊Apple ID用。此步驟或需要一個非ProtonMail電郵以作認證
3. 請預先在網上註冊 Apple ID，請參閱：https://account.apple.com/，留意註冊時需設定香港以外地區
4. 填妥Apple 向電郵帳戶及電話號碼發送的認證碼，才能成功註冊 Apple ID

Android系統：註冊Google帳戶

1. 預備註冊帳戶用的電話號碼（非香港電訊商註冊號碼）
2. 預備工作電話用的 ProtonMail帳戶
3. 預備工作電話用的 Google帳戶，或按照操作說明新增帳戶。新增Google帳戶需要電話號碼作認證，建議使用非本地號碼。同時，請在設定時選擇香港以外地區

開機設定：

1. 設定語言或地區時，請選擇香港以外的地區
2. 選擇外觀後，選擇「不使用其他裝置來進行設定」/「手動設定」
3. 設定密碼時請自訂一組由數字、符號及字母組成的密碼，不選用Face ID及Touch ID
4. 如必須連接 Wi-Fi 網路，應確保自己使用可信任的個人熱點
5. 在要求登入Apple ID時，可先略過（點選「稍後再設定」）
6. 在主頁面選擇「系統設定」→ Wi-Fi →點選已連接的網絡→點選「私人Wi-Fi地址」和「限制IP位置追蹤」

可返回App Store下載所需應用程式：

- 密碼管理程式（Bitwarden, KeePassXC, KeePassium等）
- 雙步驟認證程式（2FAS、Authy等）
- VPN（Proton VPN, Mullvad VPN）
- 即時通訊程式 Signal
- 電郵帳戶（ProtonMail）
- 瀏覽器（Brave、Firefox、DuckduckGo）
- 檔案加密程式（Cryptomator）

2 系統安全設定

iPhone 設定

停用生物識別解鎖

為什麼要停用 Face ID / Touch ID？

- 在部分地區，執法人員可要求你用面部或指紋解鎖 - 長密碼加上雙重驗證會享有更強的保護 - 緊急情況下更難被強制解鎖

設定路徑：設定 → Face ID 與密碼 → 關閉 Face ID

停用位置及追蹤

設定	路徑
定位服務	設定 → 私隱與安全性 → 定位服務 → 關閉
廣告追蹤	設定 → 私隱與安全性 → 追蹤 → 停用「允許 App 要求追蹤」

停用高風險功能

- Siri 建議：設定 → Siri 與搜尋 → 關閉相關選項
- iCloud 備份（除非已經加密）：設定 → iCloud → iCloud 備份 → 關閉
- AirDrop：控制中心 → AirDrop → 關閉接收

Android 設定

停用生物識別解鎖

設定 → 安全 → 螢幕鎖定 → 選擇 PIN 或密碼

停用位置及追蹤

設定	路徑
位置	設定 → 位置 → 使用位置 → 關閉
廣告個人化	設定 → Google → 廣告 → 選擇退出廣告個人化

停用高風險功能

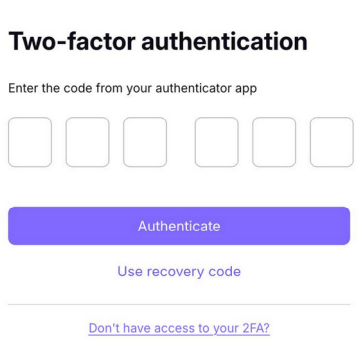
- 鄰近分享：設定 → 已連接的裝置 → 連接偏好設定 → 鄰近分享 → 關閉
- Google 助理：設定 → Google → Google 助理 → 關閉
- 自動同步：設定 → 帳戶 → 關閉自動同步聯絡人、圖片、檔案

3 建立強密碼

特點	說明
長度	至少 16 個字元，建議 18-20 個以上
複雜性	包含大小寫字母、數字、符號
獨特性	每個帳戶使用不同密碼
隨機性	不包含個人資訊或常見詞語

4 雙重驗證（2FA）

優先次序	方式	安全性
1	實體金鑰（YubiKey）	高
2	驗證器應用程式	高
X	簡訊 OTP	可被攔截
X	生物識別	在敏感地區不建議用作唯一驗證





推薦驗證器應用程式

應用程式	平台
2FAS	Android 及 iOS
Aegis Authenticator	僅 Android

5 密碼管理

工具	平台	特點
Bitwarden	全平台	開源、免費版功能完整
Proton Pass	全平台	與 Proton 生態系統整合
KeePassXC	桌面	本地儲存、開源
KeePassium	iOS	與 KeePassXC 通用、本地儲存

6 防禦策略

封鎖模式（iOS）

啟用方法：設定 → 私隱與安全性 → 鎖定模式 → 開啟

功能： - 停用某些網頁功能（減少攻擊面） - 停用非信任來源的訊息附件 - 強化 Wi-Fi、藍牙安全

緊急停用 Face ID

方法：同時按住側邊按鈕 + 任一音量按鈕

這將停用 Face ID，直到手動輸入密碼才能解鎖。

使用場景： - 被攔截檢查前 - 進入高風險場所前 - 任何你擔心被強制解鎖的情況

失竊設備保護（iOS 17.3+）

啟用路徑：設定 → Face ID 與密碼 → 失竊設備保護 → 開啟

7 加密工具

7.1 裝置全磁碟加密

平台	工具	啟用方法
macOS	FileVault	系統偏好設定 → 安全性與私隱 → FileVault
Windows	BitLocker	設定 → 更新與安全性 → 裝置加密
iOS	內建	設定密碼後自動啟用
Android	內建	設定 → 安全 → 加密手機

7.2 Cryptomator — 為雲端硬碟檔案作端對端加密

平台	可用性
Windows 桌面版	免費
macOS 桌面版	免費
iOS	收費
Android	收費

官網：https://cryptomator.org

7.3 Tresorit 或 Proton Drive — 具備端對端加密的雲端硬碟

平台	可用性
Windows 桌面版	免費
macOS 桌面版	免費
iOS	收費
Android	收費

注意：無論使用何種工具，應定期更新程式系統，避免安全漏洞導致入侵。

8 VPN 設定

推薦 VPN：Proton VPN

重要設定：

- 開啟 Kill Switch（斷線時阻截所有流量）
- 工作手機上始終保持 VPN 開啟
- 避免使用香港伺服器
- 追求更高私隱度，可考慮選用 Mullvad VPN（瑞典）

設備安全檢查表

安裝設定

- ☐ 使用新電郵建立新 ID
- ☐ 設定強密碼
- ☐ 啟用雙重驗證（實體金鑰）

系統設定

- ☐ 停用 Face ID / 指紋解鎖
- ☐ 關閉定位服務
- ☐ 停用廣告追蹤
- ☐ 關閉不必要的自動同步

安全工具

- ☐ 安裝密碼管理器
- ☐ 設定雙重驗證（驗證器應用程式或實體金鑰）
- ☐ 啟用全磁碟加密
- ☐ 安裝並設定 VPN

防禦策略

- ☐ 啟用封鎖模式（iOS）
- ☐ 練習緊急停用 Face ID
- ☐ 啟用失竊設備保護

RESILIENCE
INNOVATION
LAB