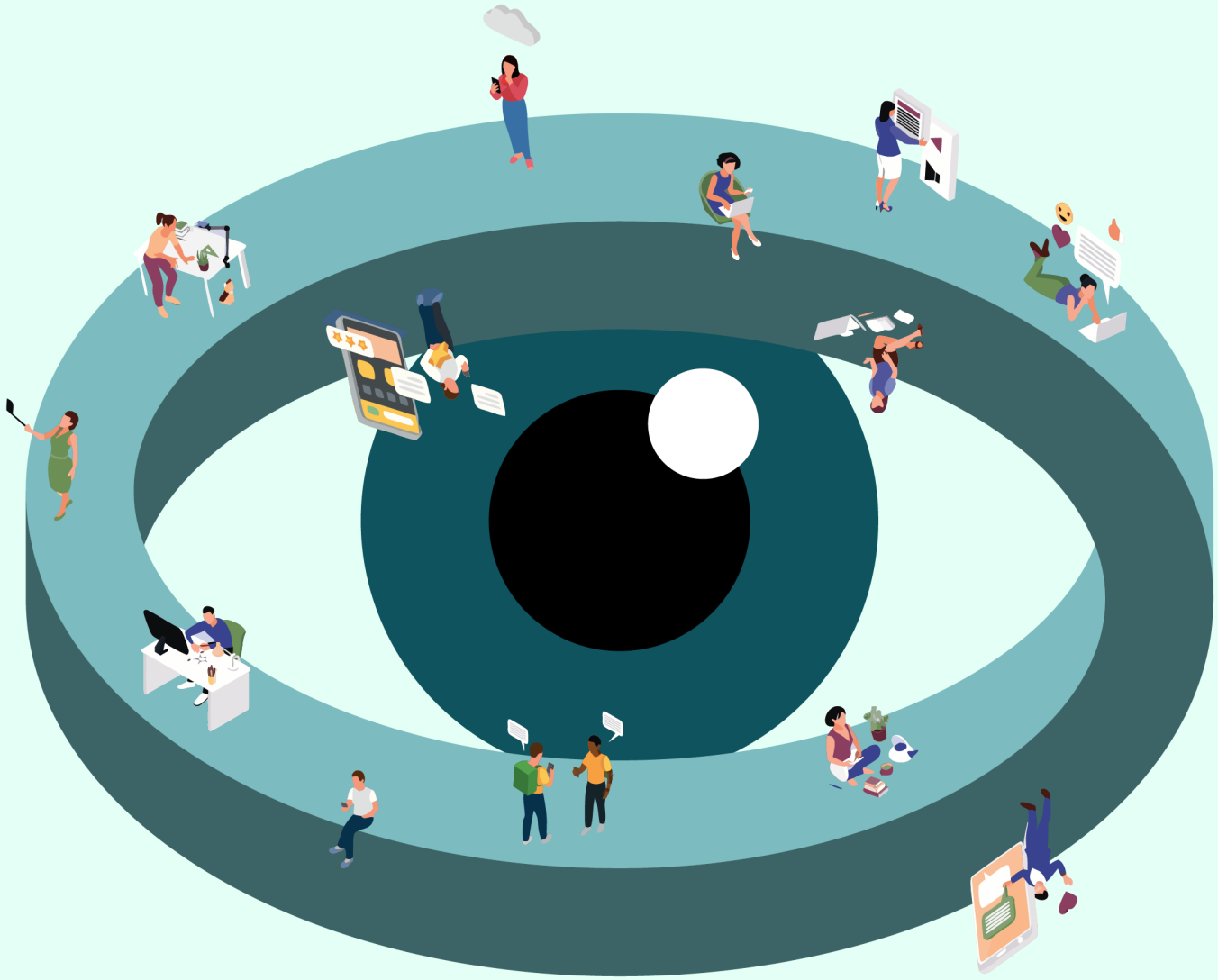
處變不驚

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

韌性創新實驗室
Resilience Innovation Lab

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

前言

隨著全球國家安全體制及法規日益收緊，加上香港在2024年3月起實施《維護國家安全條例》（俗稱「23條」），其域外效力對香港民主及人權倡議者的資訊安全和私隱保護構成迫切威脅。本手冊旨在為香港本地公民社會及離散社群提供實用的資訊安全指引，幫助他們在日益複雜的法律和技術環境中保護自身權益。

本手冊的適用對象包括：

- 公民權利倡議者
- 記者
- 公民社會組織成員
- 學生
- 任何關注資訊安全和私隱、關心社會的香港居民

本手冊推薦的應用程式與工具，均源自團隊成員、用家及測試員的實作經驗，並無任何商業考慮，亦與相關程式和工具的開發商或擁有人毫無利益關係。

本手冊的使用方式靈活多元，讀者可依據自身需求選擇最合適的閱讀方式。若希望系統地建立資訊安全知識，可從第一章開始，依序閱讀各章節，循序漸進地掌握相關概念與實務；若時間有限，或已對某些領域有一定認識，亦可直接翻閱與自身情況相關的章節，針對性地評估目前的安全狀況。此外，每章末均附有自我檢查清單，協助讀者逐項對照，確認各項安全措施是否已切實執行。冀此編排能切合不同讀者在各種處境下的實際需要。

本手冊得以付梓，我們謹此感謝參與撰寫、編輯、校對的團隊成員。我們更要感謝曾參與我們主辦和合辦的「資訊安全工作坊」之朋友、同道。她們認真、坦誠的回饋，實在地幫助我們改進手冊的內容。我們謹願她們在母國或離散社群的努力有所回報。

韌性創新實驗室
2026年6月

目 錄

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

第 1 章

當前香港立法環境下的資訊安全威脅

返回目錄

概述

現行法律框架直接規範我們如何行使網絡自由，並劃定資訊安全的底線。本章重點探討三項法例：第一是《港區國安法》的四類罪行及其域外效力，第二是《國家安全法》第43條的實施細則（內容移除、資料提交、秘密監察），第三是2024年頒布的《維護國家安全條例》（SNSO）及其新增罪行。無論身在香港與否，理解這些法律的內容、檢控門檻與實施情況，都有助於評估自身風險並做出相應調整。章節依「罪行的定義 → 執法權力 → 新法例擴充 → 觀察與應對」的順序編排；讀完本章後，讀者將對當前法律紅線與執法工具有一幅較完整的圖像，並可在後續章節中結合技術與操作建議，制定保護資訊安全與身份的策略。

對於每一個居住或曾居於香港的人來說，自2020年起，理解這些條文不僅是法律層面的需求，更關乎日常生活與言行舉止。因此，以下盡量以條文與案例說明這些法律如何影響言論自由、資訊安全及個人安全，從而協助你在知情下確保自身權益與安全。

1.1 《港區國安法》四大罪行

本節說明《港區國安法》中與網絡言論最相關的四類罪行，以及「域外效力」如何令在境外發表的言論仍可能受香港法律追究。了解罪行的定義與既有案例，有助於判斷哪些網上行為可能被視為觸法。

域外效力（第36條）

第36條訂明：只要被指控的言論、行為或結果在香港境內出現，即使行為不在境內進行，亦屬犯罪。例如，若某些言論被指有意圖「引起境內香港市民對政府憎恨」或對政府機關施政造成干擾，即使發表者不在香港，亦可能被追究。

分裂國家罪（第20條）

四大罪行中，與網上言論最直接相關的是分裂國家罪，以下先看其定義與案例。任何組織、策劃或參與旨在分裂國家、破壞國家統一的行為，不論是否使用武力，均屬犯罪。

案件	案件編號	要點
唐英傑案	HCCC 280/2020	展示「光復香港，時代革命」標語，不需要運用武力，已足夠被裁定為有意圖分裂國家
黃煡聰案	DCCC 210/2023	警方監察「香港獨立黨」在 Facebook、Twitter、Instagram 發表鼓吹獨立的言論，追蹤到長居海外的被告為平台管理員，在他回港探親時將其拘捕檢控；被告其後被裁定罪成

網絡安全啟示：在海外管理社交媒體專頁發表的言論，同樣可能構成分裂國家罪。

顛覆國家政權罪（第22條）

涉及通過武力或其他非法手段推翻政權機關，或嚴重干擾政府機構依法履行職能的行為。

案件	案件編號	要點
47人案（民主派初選案）	HCCC 69 & 70/2022	判詞指被告人協定若當選為立法會議員，將無差別投下反對票，被視為會嚴重干擾政府履行職能的「其他非法手段」

網絡安全啟示：在網上討論或協調政治行動的紀錄，可能成為檢控證據。

恐怖活動罪（第24、27條）

涵蓋以實現政治主張為目的，組織或威脅實施恐怖活動的行為。第27條特別針對宣揚和煽動使用武力行為。

案件	案件編號	要點
港大學生會評議會案	DCCC 917/2021	學生在社交平台直播的會議上發表同情使用武力的意見，被控宣揚恐怖主義。律政司最終改控「煽惑他人有意圖而傷人」罪

網絡安全啟示：被告人不需要有具體的暴力行為，發表同情使用武力的政治言論已可入罪；而直播內容同樣可作為檢控證據。

勾結外國或境外勢力罪（第29條）

涉及與外國或境外勢力串謀，請求對中國或香港進行制裁。

案件	案件編號	要點
黎智英案	HCCC 51/2022	檢控證據大部分來自接受訪問的言論及政論文章

網絡安全啟示：網上發表的言論、接受訪問的內容、管理的應用程式、手機通訊內容，都可能成為「勾結」的證據。

1.2 第43條實施細則（2026年修訂）：執法權力

除「何種行為構成犯罪」外，同樣重要的是了解執法機關以何種權力執行國安法。2026年修訂後的第43條實施細則賦予國安處多項擴大的權力，以下涵蓋五個與網絡自由、資料保護及通訊保密最直接相關的附表。

附表1：裝置存取與解密協助

當局可即場要求指明人士提供密碼、解密方法及其他與裝置或電子資料相關的必要協助。拒絕配合或提供重大失實、誤導性回應，可能觸犯刑事罪行。 修訂同時收緊法律專業保密權（LPP）的程序，增加被捕人法律團隊在搜查或檢取期間爭議物料的程序要求。

資訊安全啟示：要求裝置解密不同於一般監管查問。當事人在查問現場等候法律意見的空間有限，有機會需要即場解鎖提供儲存在設備上的資料。此外，現行法例下，搜查住所無須事先取得法院手令；執法人員在逮捕時往往已備妥搜查令，可即時對住所及設備展開搜查。宜檢視設備是否儲存必須或過多的資料，亦請參考第七章出入境安全。

附表2：行動限制

接受國安調查的人士如不遵從交出護照要求或行動限制，須承擔明確的刑事後果，由過往民事層面升級至刑事責任。

附表4：內容移除

國安處可將視為危害國安的訊息加以限制、停止或刪除，令有關內容不能再在網上傳播。2026年修訂進一步強化當局在通訊鏈不同層面的執法能力，涵蓋出版商、平台、寄存服務及網絡供應商，即使他們並非有關物料的作者或擁有人。

- 在法庭裁定有罪之前，國安處已可向服務供應商作出要求
- 服務供應商包括：社交媒體平台、網站主機公司、網絡商、電訊公司
- 移除內容的決定無需向公眾公布

受影響網站案例：香港監察、支聯會、香港編年史等網站或專頁被封。

附表5：資料要求

當局可強制要求當事人在指定時間及地點答覆問題、提供資料或提交物料。修訂同時引入保密相關限制，可能影響受查人員向內部管理層或法律顧問盡職匯報的能力，令機構在資訊不完整的情況下須作應對決策。

資訊安全啟示：組織紀錄資料（會議紀錄、財務資料、成員名單）都可能被要求提交；而保密限制可能令管理層無法及時掌握完整事實。

案件	案件編號	要點
華人民主書院	—	組織代表接受傳媒訪問時表示，需披露過去七年舉辦過的所有活動資料，包括時間、地點、人物、開支等詳情
支聯會案	WKCC 3633/2021	常委拒絕提交資料被檢控，案件上訴至終審法院得直
J及其他人訴警務處處長案	HCCM 191/2021	國安處要求信託人提交管理帳目、交易記錄、捐贈者資料及受惠者詳情；法庭認為偵測及檢控嚴重罪行的公眾利益較私隱權重要

附表6：秘密監察（截取通訊）

國安處人員可繞過法庭，只需向特首申請命令，便可對特定目標進行監視。監察授權範圍包括：電話勾線、電話短訊、電訊商紀錄的網絡活動、在指定位置設置監察器材。

值得留意： 如當局認為律師或其相關人士會構成危害國安的威脅，
可申請授權監聽律師與客戶的通訊，令法律諮詢保密權利不再是絕對權利。

附表7：物料提交與LPP主張程序（2026年修訂）

國安處可向法庭申請手令，要求組織或團體提交任何與調查案件有關的資料。2026年修訂新設第3部LPP主張程序，當事人須以原訟傳票及誓章提出，並在嚴格時限內以足夠具體方式識別受保密權保障的資料，包括日期、作者、收件人及用途等詳情。

1.3 《維護國家安全條例》（SNSO）

2024年3月生效的《維護國家安全條例》（俗稱「廿三條」）在國安法之外，進一步擴充國家安全相關的刑事規定，並將「境外勢力」「特區居民」等定義寫入法例。

境外勢力定義

「境外勢力」範圍廣泛，包括： - 外國政府或部門 - 境外的政黨或政治組織 - 境外情報組織或情報蒐集機構（不限政府性質，包括私人公司）- 國際組織 - 上述組織的關聯實體或個人

特區居民定義

包括獲發身分證但沒有居留權的人，即在香港工作的外籍人士亦受規管。

新煽動罪（第23條）

煽動罪近年成為香港的「口袋罪」，一些不涉及使用武力的政見表達，都可能被視為具有煽動意圖。

轉變	內容
加重刑罰	舊法例最高刑期兩年，新法例最高七年
降低檢控門檻	明確訂明控方「無需證明煽惑擾亂公共秩序或煽惑暴力的意圖」

相關案例：「快必案」、「羊村案」、「立場新聞案」，以及多宗針對社交平台帖文、YouTube 評論、直播等網上言論的案件。

間諜活動

範圍非常廣泛：

- 管有對境外勢力有直接或間接用處的任何資料或物品
- 將這些資料傳達給任何其他人
- 勾結境外勢力向公眾發佈虛假或具誤導性的事實陳述

網絡安全啟示：一些簡單取得的資料，甚至公開資訊，都有可能構成間諜活動。

境外干預

構成罪行需具備三個元素：

1. 有境外勢力參與（包括「代」境外勢力作出）
2. 使用不當手段
3. 帶來干預效果

「不當手段」包括：明知而作出關鍵失實陳述；威脅對任何人使用暴力或損毀財產；使任何人蒙受財政損失；使任何人名譽受損或受到心理傷害。

「干預效果」包括：影響政府執行政策或任何其他決定；影響立法會議員或法官執行職能；影響他人行使投票權；損害中國或港府與其他地區的關係。

網絡安全啟示：網上批評政府官員的言論、呼籲制裁官員的意見，
都可能被認定為「不當手段」。

1.4 觀察與趨勢

綜觀上述法例與實施情況，可歸納出以下觀察；本節並簡要列出可與後續章節配合的應對方向。

香港的言論自由空間正在逐步收窄：

- 網絡言論的監控將變得更加嚴格
- 可能出現更多對網絡平台的審查和監控配套措施
- 自我審查將越來越普遍

應對建議：

轉變	內容
了解法庭案例	理解哪些言論可能觸犯法律
保護電子資料紀錄	加密敏感資料，定期清理不必要的紀錄
分離身份	將政治活動與個人身份分開
使用安全工具	VPN、加密通訊、匿名瀏覽
預備支援渠道	預先協定內部法律分流程序，避免前線成員在管理層或法律支援介入前，獨自面對當局的即場要求

檢查清單

- □ **了解《港區國安法》四大罪行的定義和案例**
- □ **理解第43條實施細則（2026年修訂）賦予的執法權力**
- □ **認識《維護國家安全條例》的新增罪行**
- □ **評估自己的網上活動是否存在法律風險**
- □ **制定保護電子資料紀錄的策略**

第 2 章
常見網絡安全威脅

返回目錄 | ← 上一章：當前香港立法環境下的資訊安全威脅

概述

在香港，網絡安全威脅來自多個層面：商業網絡攻擊、企業數據收集，以及政府主導的資訊限制。理解這些威脅的性質和運作方式，是建立有效防禦的基礎。

本章按威脅來源分為三部分：先說明一般性的網絡攻擊與國家級黑客活動，再討論企業與應用程式如何收集和利用個人數據，最後檢視政府主導的內容管制及由此衍生的自我審查與資訊獲取限制。讀完本章後，你將能更準確地判斷自己所面對的風險類型，並在後續章節中找到對應的防護建議。

2.1 商業網絡安全威脅與攻擊

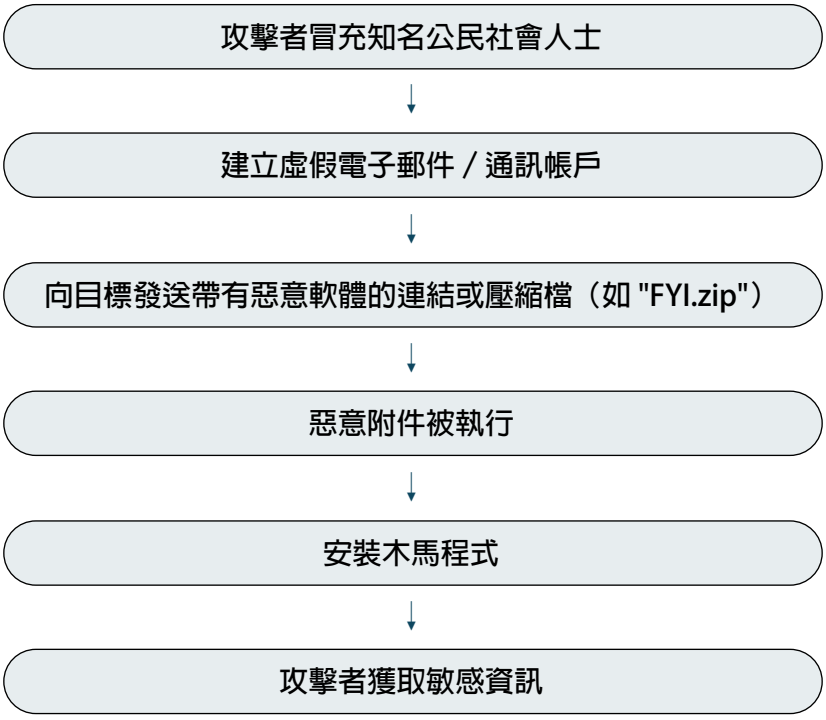
無論是個人帳戶被盜用，還是組織系統被入侵，商業層面的網絡攻擊都是最常見的資訊安全威脅。

常見攻擊類型

攻擊類型	說明
惡意程式	透過下載帶有惡意程式的附件或點擊惡意連結
釣魚訊息	偽裝成可信來源的欺詐性電郵或訊息
黑客活動	針對系統漏洞的非法入侵
中間人攻擊	攔截通訊雙方的數據傳輸
零日攻擊	利用尚未修補的保安漏洞

魚叉式網路釣魚（Spear-phishing）

魚叉式釣魚是針對特定目標的高度定制攻擊，攻擊者會事先研究目標的社交圈與工作習慣，因此比一般釣魚更難識別。



已知目標群體：公民組織、記者、學生組織、研究員

國家級黑客組織

組織名稱	案件編號	攻擊特點
APT31	國家機構支持	針對政治人物、民主運動人士
APT41	國家機構支持	同時進行間諜活動和金融犯罪

防範建議：- 對來自不明來源的電郵保持高度警覺 - 不要開啟可疑附件
- 使用 VirusTotal 等工具檢查可疑檔案 - 啟用雙重驗證保護帳戶

2.2 企業監控與數據私隱威脅

應用程式數據收集

數據收集	私隱風險
硬體型號、作業系統版本	設備指紋識別
IP 地址	位置追蹤、網絡活動分析
GPS 位置	精確定位
網頁搜索詞語	行為分析
通訊元數據（Metadata）	社交網絡行為分析
相簿照片的拍攝地點和日期	行蹤追蹤

中國 AI 應用的數據主權問題

案例：DeepSeek, Qwen, Kimi

- 數據儲存於中國境內
- 受中國《數據安全法》管轄
- 可能被要求向當局提供用戶數據

建議：避免在中國 AI 應用中輸入敏感資訊（詳見第六章）。

社交媒體平台的審查與數據銷售

活動	影響
內容審查	刪除或限制特定內容的可見度
大數據銷售	用戶資料被出售給第三方
AI 數據爬取	用戶內容被用於訓練 AI 模型

2.3 自我審查及資訊獲取限制

政府主導的內容移除

根據《港區國安法》第43條實施細則，當局可要求服務商移除危害國家安全的訊息，或限制任何人接觸該訊息。此類要求無須事先經法庭定罪，且執行細節往往不向公眾披露[1]。身處香港的人士往往需要透過 VPN 才能瀏覽受影響網站。

資訊安全脫鈎趨勢

現象	影響
部分政策文件僅能透過國產軟件程式讀取	資訊獲取受限
軟件生態系統分離	工具選擇受限
跨境數據流動受阻	國際協作困難

1 可參考韌性創新實驗室2025年出版的《維護香港資訊自由：挑戰、機會與出路》。

資安威脅無可避免

即使個人做好安全防護，仍可能受到第三方漏洞或制度性因素影響，例如：

- 第三方保安漏洞：使用的服務或平台被入侵
- 政府網絡受到攻擊：公共服務數據外洩

核心原則： 最弱環節決定整體安全
你的安全程度取決於整個系統中最薄弱的環節。即使你的設備和帳戶安全，
如果你聯繫的人或使用的服務存在漏洞，你的資訊仍可能被洩漏。

網絡安全威脅總覽

威脅來源	威脅類型	主要風險	防範重點
商業攻擊者	釣魚、惡意程式	資料竊取、帳戶入侵	警覺性、防毒軟件、盜版軟件
國家級黑客	釣魚、惡意程式	長期監控、數據竊取	安全通訊、加密
企業	數據收集	私隱洩漏、行為追蹤	權限管理、替代服務
政府	內容審查、數據收集	言論限制、法律風險、監控	VPN、匿名工具

檢查清單

- □ **了解常見的網絡攻擊類型**
- □ **評估自己使用的應用程式的數據收集範圍**
- □ **檢查是否使用了可能將數據傳送到中國的服務**
- □ **測試是否能夠存取常用的資訊來源**
- □ **確認 VPN 工具可用**

第 3 章
應對監控技術與方法

返回目錄 | ←上一章：常見網絡安全威脅

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。

3.1 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

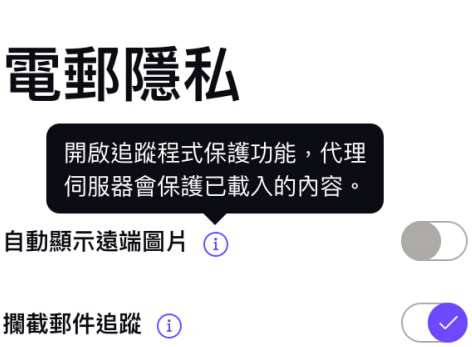
↓

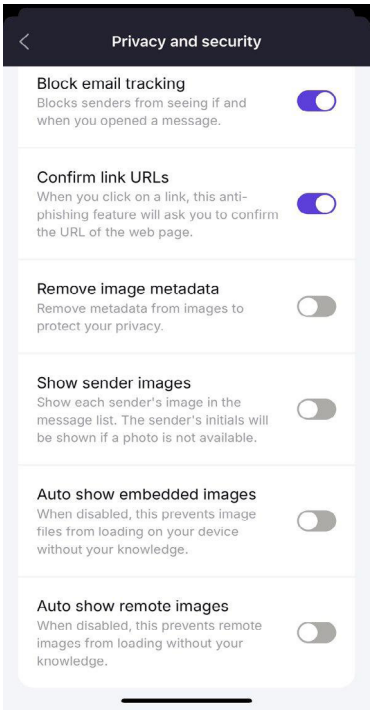
你打開電郵，瀏覽器自動載入遠端圖片

↓

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

3.2 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

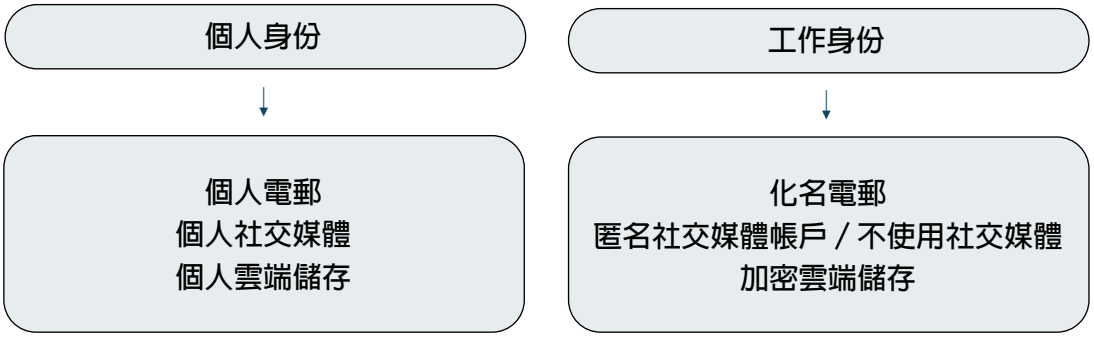
基本要求：

- 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

3.3 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

第 4 章
設備安全

返回目錄 | ←上一章：應對監控技術與方法

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。

4.1 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）

4.2 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

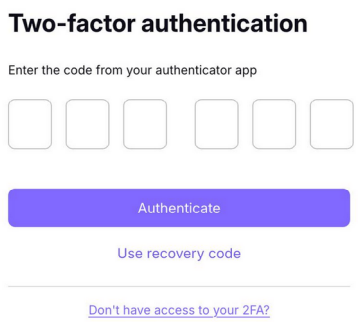
- 鄰近分享：設定 → 已連接的裝置 → 連接偏好設定 → 鄰近分享 → 關閉
- Google 助理：設定 → Google → Google 助理 → 關閉
- 自動同步：設定 → 帳戶 → 關閉自動同步聯絡人、圖片、檔案

4.3 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

4.4 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

4.5 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

4.6 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

4.7 加密工具

4.7.1 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

4.7.2 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

4.7.3 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。

4.8 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

第 5 章
通訊安全

返回目錄 | ←上一章：設備安全

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。

5.1 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

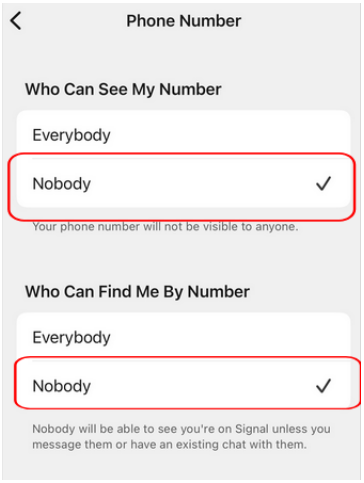
5.2 Signal 設定

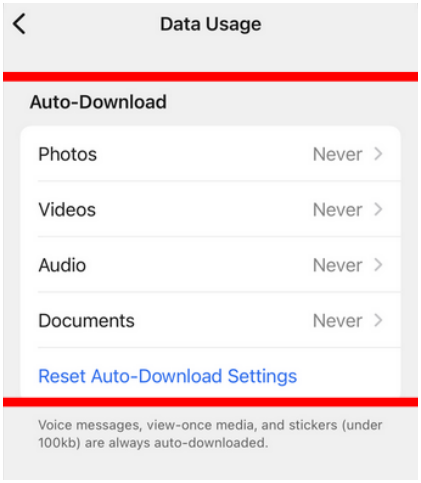
安全設定

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





5.3 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。

5.4 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

5.5 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

第 6 章
人工智能(AI)應用安全

返回目錄 | ←上一章：通訊安全

概述

人工智能（AI）應用程式正在改變我們的工作方式，但同時也帶來新的私隱和安全風險。本章集中討論你「如何與 AI 工具互動」：從資料如何被收集與用於訓練，到輸入時應避免的敏感資訊、私隱友善的替代方案，以及 AI 生成內容的水印與幻覺風險。

6.1 AI 應用的資料收集風險

雲端 AI 服務的數據儲存

問題	說明
數據儲存在哪裡？	可能受不同司法管轄區的法律約束
數據保留多長時間？	可能被長期儲存和分析
數據用於什麼用途？	可能用於訓練 AI 模型
誰可以存取數據？	員工、合作夥伴、政府機構

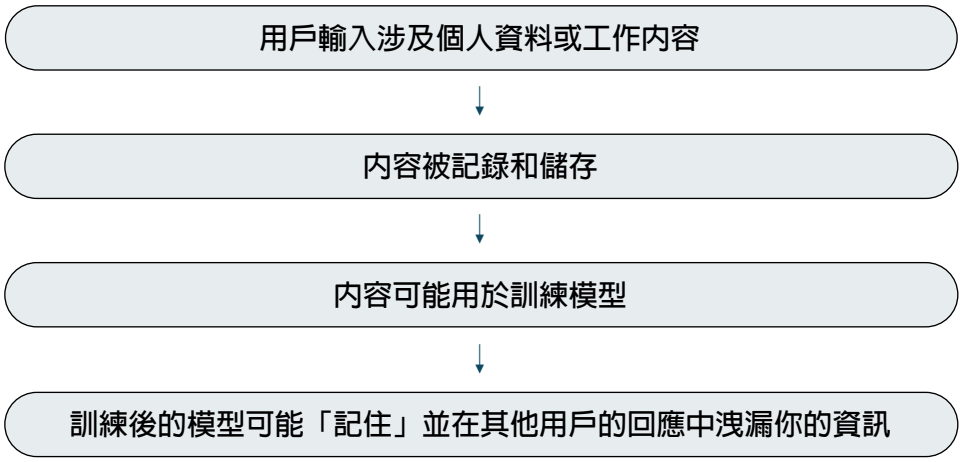
目前多數主流雲端 AI 服務（例如 OpenAI、Microsoft、Google、Meta、Anthropic、Amazon、X、DeepSeek、Moonshot Kimi 等）在其消費者產品中，預設會將用戶聊天輸入與模型輸出用於「訓練與改進系統」。

中國 AI 應用的數據主權問題

案例：DeepSeek

風險	說明
數據儲存	用戶數據儲存於中國境內
法律管轄	受中國《數據安全法》、《網絡安全法》管轄
政府存取	當局可依法要求提供用戶數據
審查機制	內容可能受到審查和過濾

訓練數據回饋風險



重要：在大型語言模型（LLM）時代，「刪除權」與「被遺忘權」幾乎難以落實，輸入內容之前宜深思熟慮，避免輸入敏感內容仍是上策。

6.2 AI 與網絡攻擊：擴充功能與技能外掛的風險

隨著 AI 功能日益普及，許多常用平台已將 AI 工具直接整合至其應用程式或系統層級，包括瀏覽器（Firefox、Brave）、工作平台（Notion）、作業系統（Apple Intelligence、iPhone 及 iWork 套件）等。這類內建 AI 功能的數據處理方式、雲端傳輸範圍及訓練數據政策，往往缺乏透明度，使用前宜主動了解相關設定及條款。除內建功能外，惡意外掛工具可讀取你輸入、存取剪貼簿與瀏覽紀錄，甚至將惡意程式或釣魚內容注入你的工作流程。

建議：

- 使用前查閱平台的 AI 功能條款及數據政策，並按需調整或停用
- 只從可信來源安裝第三方外掛
- 限制授權範圍
- 定期檢視已安裝的擴充與權限
- 避免在處理敏感或機密工作時啟用不明的外掛程式

6.3 使用 AI 時的私隱保護

基本原則

假設你輸入的所有內容都會被：

1. 記錄和儲存
2. 被服務商員工讀取
3. 用於訓練未來的模型
4. 可能被政府機構索取

避免輸入的敏感資訊

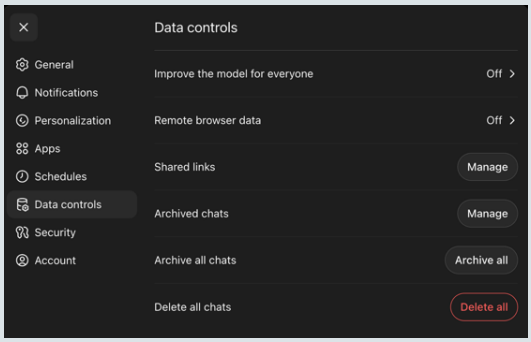
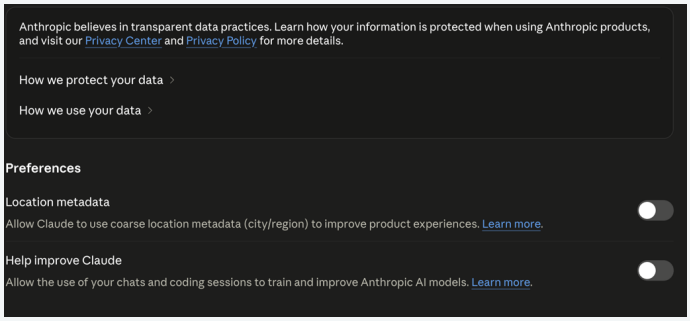
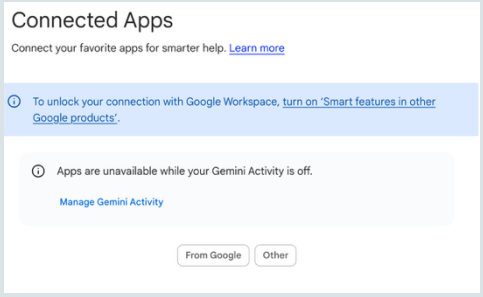
類別	例子
個人身份	姓名、身份證號碼、電話、地址
聯絡人資訊	其他人的姓名、聯絡方式
工作內容	機密文件、內部通訊、未發布的內容
位置資訊	具體地址、行程安排
財務資訊	銀行帳戶、信用卡資訊
政治敏感內容	可能觸犯法例的言論

安全使用 AI 的技巧

模糊化敏感資訊範例：

- 不安全：「幫我寫一封給陳大文的信，關於我們在中環辦公室的會議」
- 較安全：「幫我寫一封正式的會議邀請信」

檢查並關閉訓練選項：

服務	設定路徑
ChatGPT	設定 → Data controls → Chat history & training → 關閉 
Claude	設定 → 私隱 → 改善 Claude模型 → 關閉（停用對話用於訓練） 
Google Gemini	活動控制 → Gemini Apps Activity → 關閉 

6.4 私隱友善的 AI 替代方案

本地運行的大型語言模型（LLM）

AI 模型下載到電腦運行，例如透過 Ollama 運行 Mistral、Gemma 4 等開源模型，數據只會保留在用戶設備。Gemma 提供多種規模版本，包括適合行動裝置運行的小型版本（1B、4B），適合文字處理工作。

類別	說明
優點	數據完全保留在本地；不需要網絡連接；無訓練數據回饋風險；Gemma 4等模型可在一般手機上運行，毋須高端硬件
缺點	部分模型能力可能不及最新雲端版本；設定較複雜

雲端運行的大型語言模型

Confer： https://confer.to/

6.5 AI 生成內容的風險

水印和元數據

類型	說明
文字水印	透過特定的詞語選擇或語法模式識別 AI 生成的文字
圖片水印	隱藏在圖片像素中的識別資訊
元數據	檔案屬性中可能包含創建資訊

AI 幻覺問題

AI 可能生成看似合理但實際上不正確的內容（「幻覺」）：

- 始終驗證 AI 提供的事實資訊
- 不要直接引用 AI 生成的「資料來源」
- 對重要內容進行獨立核實

AI 安全使用檢查表

使用雲端 AI 前

- ☐ **評估內容敏感度**
- ☐ **連接 VPN**
- ☐ **使用匿名帳戶登入**
- ☐ **確認已關閉訓練/數據收集選項**

輸入內容時

- ☐ **移除個人身份資訊**
- ☐ **使用代號代替真實人名**
- ☐ **模糊化位置和時間細節**
- ☐ **避免輸入機密或政治敏感內容**

長期策略

- ☐ **學習使用本地 LLM 工具**
- ☐ **避免使用中國 AI 應用**
- ☐ **定期檢查 AI 服務的私隱政策變更**
- ☐ **審慎使用第三方 AI 外掛**

第 7 章
出入境安全

返回目錄 | ←上一章：人工智能 (AI) 應用安全

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。

7.1 出行前準備

三個基本問題

出行前，先問自己：

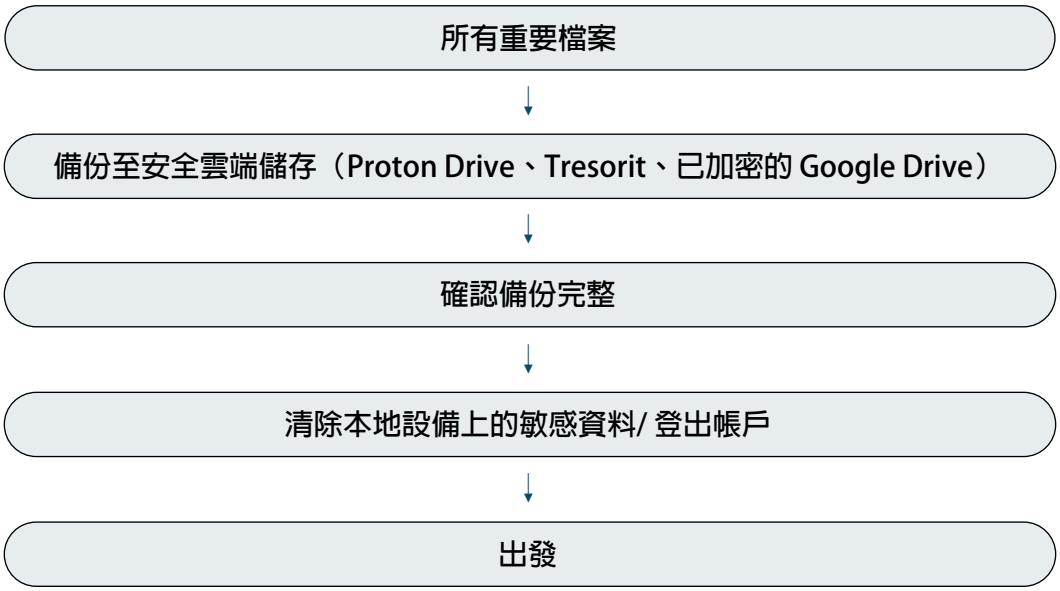
1. 是否需要攜帶存有個人資料的常用設備？
    - 考慮攜帶專用設備而非日常設備
2. 哪些資料是必需的？
    - 只攜帶行程所需的最少資料
3. 如果設備被盜，或被檢查或扣押，後果是甚麼？
    - 評估風險並做好應對準備
    - 2026年起，當局可即場要求提供密碼及解密協助，拒絕遵從有具體法律後果。設備上保存的資料愈少，可降低當場面對的風險。

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

7.2 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

7.3 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

7.4 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

7.5 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

7.6 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

第 8 章
未來挑戰

返回目錄 | ←上一章：出入境安全

概述

香港的網絡監管環境正在不斷收緊。本章分析《保障關鍵基礎設施（電腦系統）條例》的潛在影響，探討 VPN 使用的未來，以及長遠的私隱保護策略。

8.1 《保障關鍵基礎設施（電腦系統）條例》

條例概述

2026年1月，港府開始實施全新法例，加強規管基礎設施營運者的網絡安全。法例涵蓋八種「關鍵基礎設施」(CIs)，賦權執法部門調查及防範網絡安全事故：

類別	例子
能源	電力公司、燃氣公司
資訊科技	數據中心、雲端服務供應商
銀行和金融服務	銀行、證券公司
陸上交通	鐵路、巴士公司
航空交通	機場、航空公司
海運	港口、貨運公司
公共醫療	醫院、診所
通訊和廣播	電訊公司、互聯網服務供應商

潛在風險

風險	說明
後門程式	當局可能以國安為由，要求服務供應商在系統安裝特定程式
監控擴大	直接向營運者取得資訊的做法，繞過傳統司法程序
封網基礎	條例可能成為限制特定網站或服務的法律基礎

8.2 VPN 的未來

VPN 使用建議

因素	建議
公司所在地	選擇私隱法規嚴格的國家
無日誌政策	確認服務商不記錄用戶活動
開源	程式碼可供審查
伺服器位置	多個國家的伺服器選項

推薦服務：Proton VPN（瑞士）、Mullvad VPN（瑞典）

Tor 瀏覽器

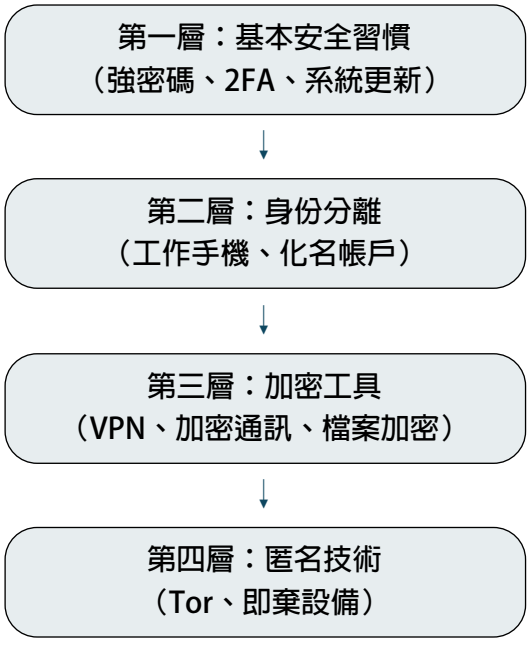
特點	VPN	Tor
速度	較快	較慢
匿名性	依賴服務商	分散式
使用難度	簡單	稍複雜
商業依賴	是	否

使用 Tor 的方法：

- 方法一：從官網下載 Tor Browser
- 方法二：使用 Brave 瀏覽器的「使用 Tor 的私密視窗」（僅 Android 和桌面版）

8.3 長遠私隱策略

建立多層防護



資料儲存策略

考量	本地儲存	雲端儲存
物理安全	設備可能被搜查	不受物理搜查影響
法律風險	本地法律管轄	可能受境外法律保護
可存取性	需要物理存取	隨時隨地可存取
建議	加密後儲存	客戶端加密後上傳

持續學習

推薦資源：

- Security in a Box
- Digital First Aid
- Privacyguides.org
- Electronic Frontier Foundation (EFF)
- Access Now
- Digital Defense
- Civil Society Cyber Shield

檢查清單

- ☐ 了解本地網絡安全相關法律的內容和潛在影響
- ☐ 評估當前 VPN 服務的可靠性
- ☐ 學習使用 Tor 瀏覽器作為備用
- ☐ 為個人及團隊建立多層防護策略
- ☐ 為個人及團隊制定長遠的資料儲存和備份計劃
- ☐ 定期設定提醒，以審視上述安全措施

RESILIENCE
INNOVATION
LAB