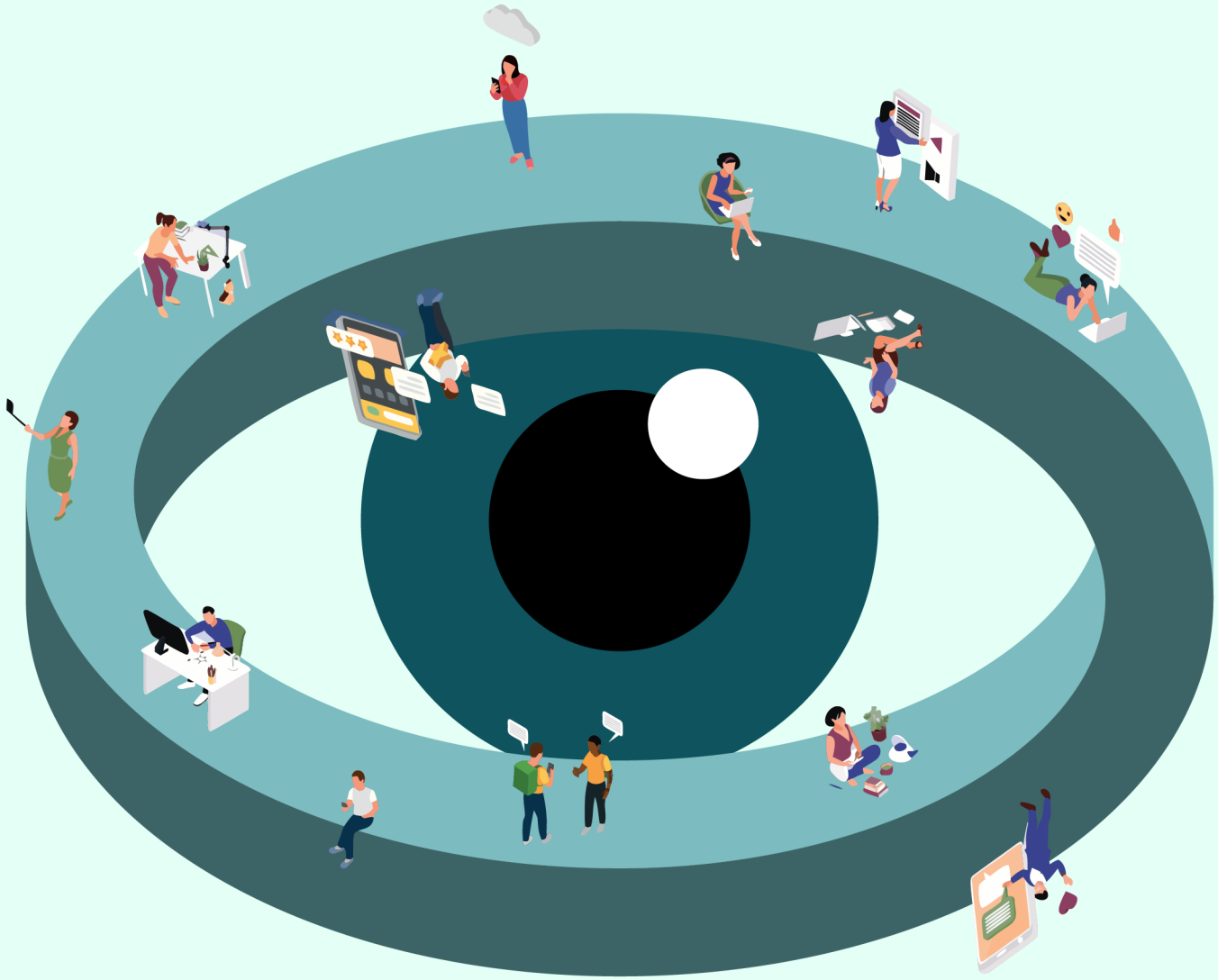
# 處變不驚

## 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 |

# 常見網絡安全威脅



# 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。

# 1 商業網絡安全威脅與攻擊

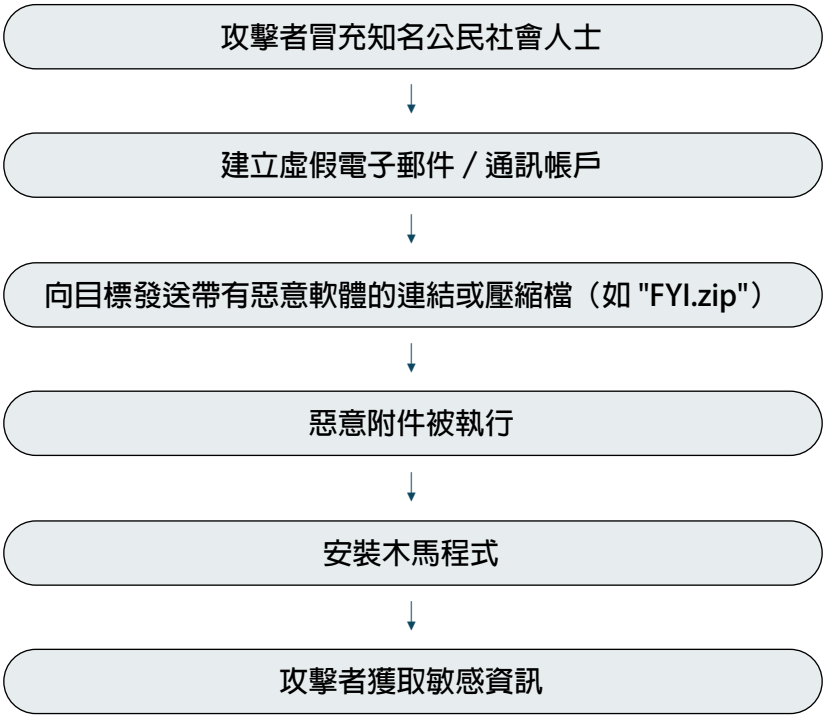
無論是個人帳戶被盜用，還是組織系統被入侵，商業層面的網絡攻擊都是最常見的資訊安全威脅。

## 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 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 |

## 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**

RESILIENCE
INNOVATION
LAB