資訊安全手冊

公海版

1. 基本概念

資訊安全的目標有四：

1. 保密性 (confidentiality)，信息僅在目標方之間共享；
2. 完整性 (integrity)，收到與發送的信息相同；
3. 隱私 (privacy)，存儲和傳輸的信息不能與真實個人識別；及
4. 可用性 (availability)，發送的信息在另一端可靠地被接收。

本指南旨在實用，因此不涉關於原則的細節，而將重點放在實際步驟上。高階措施將以[進階]為前綴標題。

在本指南中有4個虛構人物，Alice，Bob，Eve和Mallory。Bob正試圖向Alice發送一個信息，Eve被動地在聽對話（消極竊聽），而Mallory則在積極地嘗試知道這個消息是什麼（積極竊聽）。

1.1. 資訊安全基本操守

在討論具體要點前，以下規定為必須遵守的第一道防線：

- 不要在不同地方使用相同的用戶名。
- 不要在不同地方使用相同的電子郵件地址。
- 不要使用生物識別技術(如指模)於任何可以存取敏感信息的設備。
- 不要通過真實IP和Proxy/ VPN / TOR登錄相同的帳戶。
- 不要發布任何可通過反向圖像搜索追溯到你身分的照片或圖像。[1]
- 不要在任何網上論壇討論個人喜好或對具體位置的認識，如學校，商店或城鎮。
- 請勿安裝諸如Clean Master，CM瀏覽器(或Cheetah Mobile的任何程式)，騰訊，QQ，WeChat(或任何騰訊程式)，MiFit，MiRemote(或任何小米程式)或任何中國公司製作的軟件。
- 當面對垃圾郵件時，不要理會及予以阻隔。不要嘗試回覆。
- 原則上，不應發布或分享任何不必要的資訊。假定任何在你電腦/手提電話的資訊將永存於互聯網上。

[1] 見： https://images.google.com https://tineye.com https://yandex.ru/images

- 當Bob需要驗證他是否實際上和Alice交談時，不應使用與當前通信方式相同的頻道進行驗證。例1，我是某行動組的新聘人員，有組員用Wire聯繫我，我應該要求該組員用Telegram上用我在申請時提供的Telegram ID與我聯繫確認。例2，有告密者由Wire聯繫我，我應要求告密者在他/她的Twitter帳戶上發布一個特定的句子以識別。

2. 網絡安全

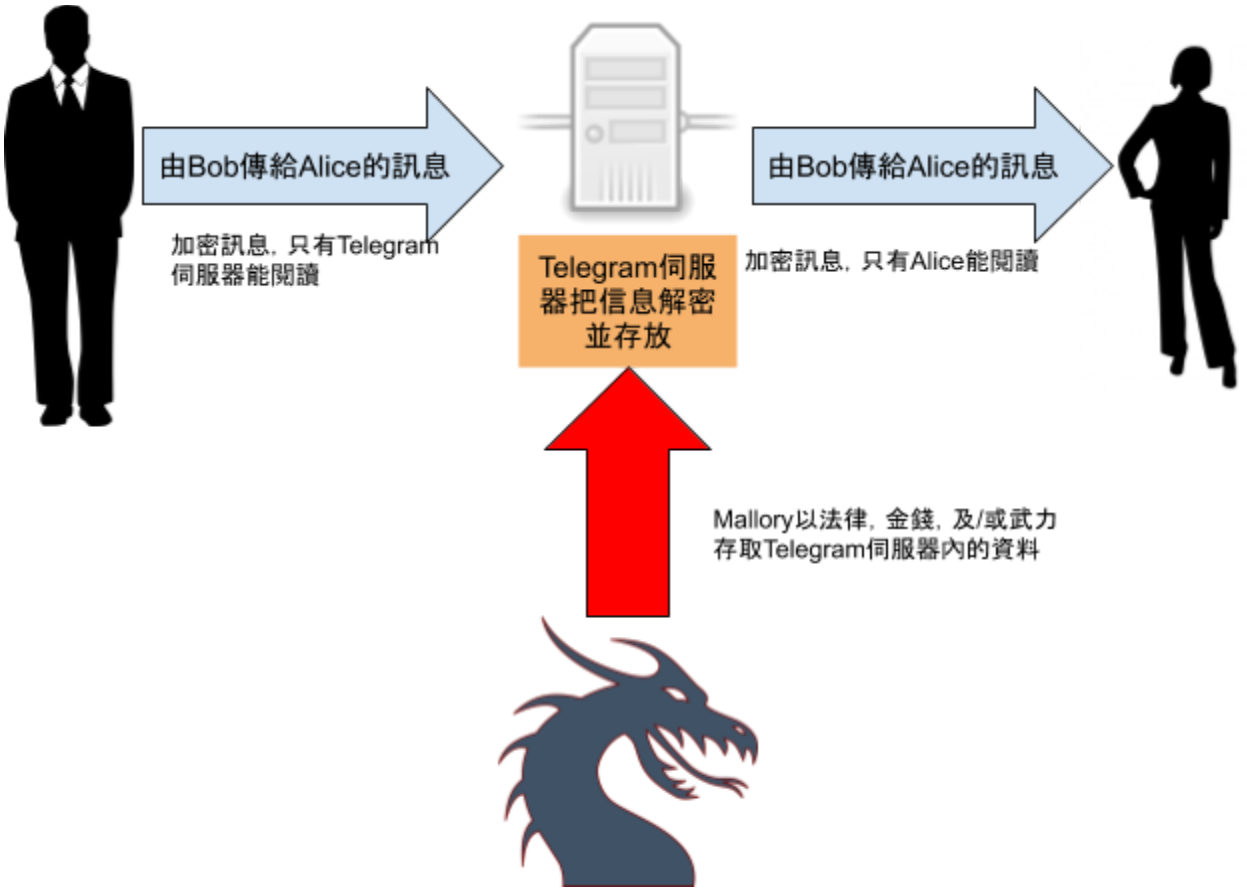
這節會講解如何在不構成太多不便的情況下，保障你的網絡安全至合理程度。大部份設定只需設置一次，便持續生效。部份較麻煩，需要定期設置的方法，會以［進階］標記之，以示之為進階設定。(但這未必切合你的需要)

2.1. 通訊保安(保密性，完整性，通用性)

此小節只涵蓋通訊傳送的保安，即確保A的訊息只送至B，而不是其他人。通訊私隱，即確保其他人不能竊看訊息而得知A和B是有關人士，會在2.2保護身份(個人私隱)講解。

2.1.1. Telegram：非機密的組內通訊

現時香港大部份抗爭群組皆採用Telegram作通訊媒介。但有很多因素使它並不安全。Telegram只預設加密你的電腦/智能電話與Telegram伺服器的通訊。如下圖闡述：



普通人無能力補救來自Telegram伺服器或公司有可能被攻擊的缺陷。故此，只要有足夠的法律權力，財力或軍事實力，任何政府部門都能利用這個缺陷，輕易截取你全部的通訊資料。（當然，是否有國家已經成功攻入Telegram伺服器仍然成疑。）它的點對點加密功能只適用於Secret chat。而且，此功能採用的加密方式屬自家研發，並無其他軟件採用。（加密學其中一個基本安全守則是使用多人都採用，tried and tested的加密方法。）Telegram還有很多保安上及私隱上的問題[2]。所以，我們建議避免使用**Telegram**處理真正敏感資料。

因此，在香港人轉用更好的通訊媒介前的一小段時間，各位必須注意：

請開啟2-step verification(於Setting > privacy and security > active sessions)若你是初次使用此功能，請之後關掉所有active sessions

- 切勿從公用電腦，或其他人的智能手機登入Telegram帳戶
- 電話號碼選項轉至Nobody (Settings > Privacy and Security > Phone Number > Nobody)
- 請啟用電話及電腦的密碼鎖，及設定自動上鎖時間

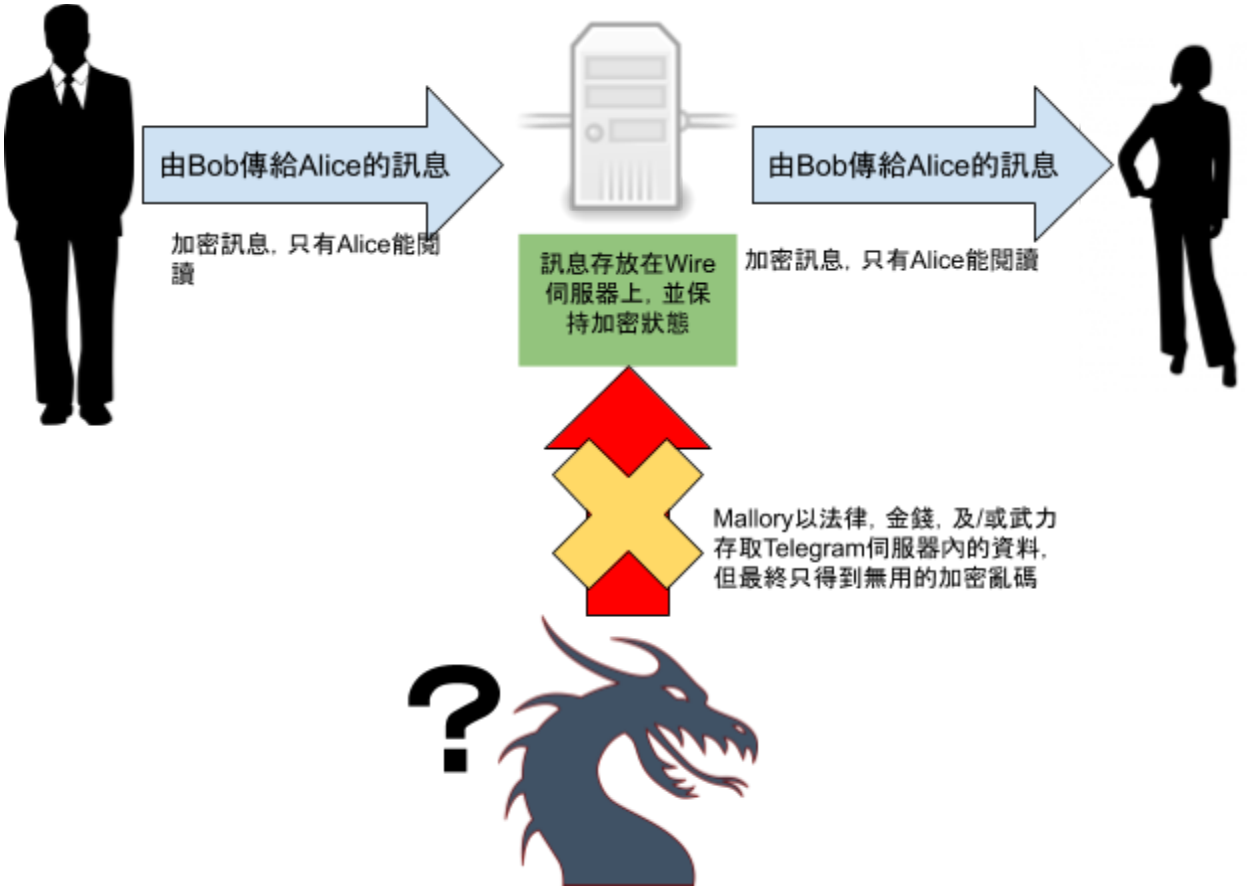
[2] https://oflisback.github.io/telegram-stalking/

- Last Seen選項轉至Nobody (於Settings > Privacy and Security)，以免你與組友的個人資料，隨元數據(metadata)一起外洩。
- 若你必須收發關於行動的敏感資料，而你無安裝Wire，Riot.im或其他更佳的通訊程式，請務必使用secret chat功能 (new message > new secret chat)

2.1.2. Wire： 機密組內通信

Wire 是可以來取代 Telegram 作組內通信的軟件。它已預設將所有通信作端對端加密(end-to-end encryption)，同時支援多人團體對話及端對端加密的跨平台裝置信息記錄同步功能，還可以作加密的多人團體音訊通話。 Wire 的加密法則是建基於廣為採用的 Signal Protocol 加密協議。它不單止用戶端為開源軟件，伺服器也是。Wire 是由 Skype 被微軟收購前的創辦人們所開發，因此通話質素亦非常優異。

下圖將展述為何預設擁有端對端功能是如此重要：



當使用 Wire 時，請注意以下事項：

- 在注冊 Wire 的用戶帳號時，請以網上版的客戶端(而非電話的用戶端)進行注冊。

由此，你便可以使用抗爭群組專用的電郵，而避免使用你的個人流動電話號碼進行注冊。
- 請勿將你的 Wire 帳號連接你的 Spotify 帳號。
- 請對你自己的裝置指紋(設定>裝置)及其他組員的裝置指紋(於對話中>上方的用戶名稱>裝置)進行認證。請你以 **Wire** 以外的媒介與你的組友交換你們的裝置指紋，部門內部的通信建議親身交換。這是因為要進行這些指紋的認証時，是必須要確認對方是你真正想要進行通信的人 — 假冒聲線或寫作風格是非常容易的。

2.1.3. 電郵

由於要將電郵加密是相當困難的，如非必要，請勿使用電郵作組內通信。

如必須使用電郵溝通，請另行申請行動群組專用的電郵地址。請僅記，切勿在你其他的現存帳號中，同時使用相同的帳號名稱及密碼；以及儘量不要使用此群組電郵，作組內通信以外的用途。

2.1.3.2. 即用即棄電郵地址

如你並不需要一個長期使用的電郵，請儘可能使用即用即棄電郵地址。

類似的即用電郵服務包務： <https://www.guerrillamail.com/> 及 <https://trashmail.com/>

2.1.3.2. 建議使用的電郵供應商

- 在三大電郵供應商(Google 的 GMail、Yahoo 的 Yahoo Mail 以及 Microsoft 的 Outlook.com)之中，GMail 理論上是最安全的。Microsoft 已經與中共政府進行行內的秘密交易，透過全面授權中共政府使用 Windows 的原始編碼，以換取 Windows 作業系統能順利於中國國內銷售。因此，假若中共政府向 Microsoft 索取你的電郵資料時，不排除 Microsoft 會把你的資料出賣給中共政府；Yahoo 內部安全總體而言是十分差劣，因此不多評論；而 Google 則因為本地競爭對手百度，至今仍未能成功進入中國市場。
- 如果你需使用一定程度的加密郵件而不希望自行設定煩瑣的 GPG 加密程序，那麼可以嘗試 ProtonMail (由 MIT 麻省理工畢業生營運，伺服器設於瑞士的歐洲核子研究組織(CERN)地庫內)，Mailoo(於法國設立)，Posteo(於德國設立，並使用綠色能源經營)或 TutaNota(於德國設立)。請注意當中的免費版本有一定的使用限制：ProtonMail Free 會以非加密方式，向非 ProtonMail 帳號傳送電郵；而 TutaNota Free 甚至不允許向非 TutaNota 用戶傳送電郵。
- 如你信任 4chan 的 /g/ 及 8chan 的 /tech/ 上一班厭惡政府及愛好開源免費軟件的 Linux 熱衷用家，你可選擇 Cock.li <https://cock.li/>，全世界第一個以陰莖作為

主題的電郵服務。它們的伺服器設於羅馬尼亞，和另外一個不為人知的地方。

2.1.3.3. [進階] 使用 GPG 進行加密 及 認証

請注意，使用 GPG 進行加密，只會對電郵內文有效；你的發信人地址以及收信人地址仍會以明文 (plaintext)方式送出。 因此，使用GPG加密的電郵仍然會給監控者知道你何時及與誰通信。

設定及使用 GPG 加密對日常用家而言是極為複雜及麻煩的過程，甚至連網絡保安專家亦會感到困擾。簡單而言，你需要產生出你一些鑰匙，然後將公開的鑰匙發放出去，同時要保存好自己私人的鑰匙(保存方法會於講述離線保安的章節中詳細講述)，之後你的溝通對象就可以使用帶相應信息的鑰匙，前往信賴網絡(Web of Trust)進行信賴認証及解碼。總括而言，這種加密方式的混亂程度，並不適合普通人作溝通之用。假使你需要對此進行研究，可以參考以下的簡介：

- Windows 用戶：https://www.gpg4win.org/
- Linux 用戶：Linux 發行版的軟件庫內必有收藏，甚至已經預訂安裝。
- Mac 用戶：https://gpgtools.org/

2.1.4. 其他即時網絡通訊軟件，如Signal，Whatsapp，Facebook Messenger，WeChat ，SMS等

無論任何情況，請勿使用以上任何的通訊平台作組內的溝通。原因如下：

- 理論上，Signal的加密是衆多通信平台中世界第一的，但奈何至今Signal仍然使用個人電話號碼作通訊錄基礎，並不支援用戶名，對於非親友通訊其可用性並不高（因為你必不能把個人電話號碼公諸於世給組員）。
- 理論上，Whatsapp 意外地是個相當不錯的平台，因為它預設使用端對端加密功能。然而，其客戶端是非開源的私有平台。 Whatsapp 數年前亦被 Facebook 收購，安全早已成疑。因此，你無法得知你的信息及對話是否真的已經加密，還只是子虛烏有。
- Facebook Messenger 提供了 "Signal protocol" 的加密方式，用戶可在私密對話啟動的情況之下使用。然而，Facebook 是一個龐大的數據收集農場，它們會將你的資料轉售圖利；同時 Facebook 對各政府的對抗態度，並不像 Google 般強硬。
- WeChat 的禁用理由相當明顯；更甚者，請勿安裝 Wechat。
- SMS基本上是完全不安全的，網絡供應商及第三方攻擊者皆可以輕易破解其加密，竊聽甚至假冒發出者名義進行釣魚攻擊（phishing）。俄羅斯已經嘗試過並成功竊聽SMS來盜取Telegram的登入code。

2.1.5. 瀏覽互聯網

2.1.5.1. 運用 HTTPS Everywhere 協助瀏覽已加密(HTTPS)網頁

簡單來說，HTTP 是未加密的網頁連線方式，而 HTTPS 則是已加密的網頁連線方式。只要留意瀏覽器 URL 網址列上的綠色小鎖，便可清楚知道網頁的加密狀態。

若然你希望你的瀏覽器於任何情況下，均自動選用 HTTPS 加密連線方式的話，你可以安裝 EFF 組織的 HTTP Everywhere 附加元件。

- Firefox 桌面版、Firefox 電話版、Chrome 桌面版 及 Opera 用家，可以前往 https://www.eff.org/https-everywhere
- Safari、Chrome 電話版 及 Internet Explorer 用家，則暫時尚未支援。

要注意的是，HTTPS 連線的信任方式只會考究你信任了多少的證書頒發機構。而問題在於有不少的中國公司及香港郵政局均會在瀏覽器及作業系統中得到證書認証。因此，對中共政府特工而言，若果它們真心要對你落手，HTTPS 的保安程度充其量只是一個小麻煩而已。（除非你設置HTTPS certificate pinning，但實在程序煩複。）

2.1.5.2. 運用DNSCrypt/DNS-over-HTTPS（DoH)/DNS-over-TLS（DoT）加密DNS傳輸

在你輸入 "www.google.com" 到瀏覽器前往網站的一瞬間，其實已包含了一系列步 驟。首先，你的電腦會向互聯網查詢到底「誰是 www.google.com?」這個過程稱為 DNS 查詢(DNS Request)。然後 DNS 伺服器會將該網站的 IP 回報給你的電腦， 讓你的電腦能夠找到實際上 "www.google.com" 這名字背後的所屬網站。

這種方式有兩大主要問題：第一，大部分電腦預設使用它們互聯網供應商(ISP)所提供的DNS伺服器；第二，這種DNS查詢方式是未加密的。兩者均意味著，就算你已經使用了HTTPS進行加密，你的ISP(亦即是政府)仍然可以得知你曾經前往過"www.google.com"。

更甚者，如果你使用未加密的 DNS(亦即不能認証的 DNS)的話，任何攻擊者都可以暗地裏偽裝成 DNS 伺服器，並告知你的電腦、電話及其他裝置，然後將你的裝置 導向一個錯誤的 IP 地址。這樣一來，你就會認為你已經順利登入了你的 GMail 甚至是 Telegram，但實質上你其實已經出賣了你的登入資料給攻擊者。

要解決此問題，你可以運用 DNSCrypt/DoH/DoT 加密你的 DNS 傳輸。

- 請跟隨 https://dnscrypt.org 的簡單指示：
    - Windows 用戶，你需要 Simple DNSCrypt
    - macOS 用戶，你需要 DNSCrypt-OSXClient
    - 而 Linux 用戶，請設定 dnscrypt-proxy
- Windows 及 macOS 的客戶端是非常容易，簡單一按enable就可以了。
- 請僅記要從列表中選擇一個 DNS 解析器(DNS Resolver)及伺服器名稱均不是香港或中國的地區。
- Windows 用戶請記得啟用 「DNS 緩存」(DNS Cache)附加功能。

2.1.5.3. 關於代理伺服器(Proxy)及虛擬私人網絡(VPN)的總覽

Proxy 及 VPN 兩者常會給予人一種安全的錯覺。事實上，除非你能選擇一個合適的 Proxy 或 VPN，否則它們其實是不甚安全的。正如任何一間公司，當它們受到政府的全力的網絡攻擊、法律壓力或金錢收買等的狙擊之下，它們往往均會屈服於政府，最終只會失敗收場。

縱使如此，如果你仍要使用 VPN 或 Prozy 的話，請僅記以下數點：

- 請勿在已使用及未使用 VPN 的情況下同時登入相同的帳戶(如電郵或社交平台)。
- 當選擇 VPN 服務時，請考慮：此 VPN 於何地營運?(中國?五眼或九眼聯盟國如美國?還是私隱安全國如瑞士?還是一些東歐的法律黑洞如羅馬尼亞?)
- 服務供應商有否記錄你的傳輸及連線資料?
- 供應商的網站是否受到大量的黑客追蹤?(如受歡迎的“Private Internet Access”)
- 能否使用匿名付款?(例如使用信用卡以外的方式繳費?)
- 它們會否因太受歡迎而出現問題?(如上述的 PIA 或 HideMyAss?)
- 在閱讀 VPN 評價的時候，請選看一些真心有需要優質 VPN 的用家所撰寫的評論(如西方盜版軟件開發者)。TorrentFreak 亦會每年發表一次評論報告，詳情請參照 <https://www.vpnranks.com/best-vpn-reviews/>

2.1.5.4. [進階] 建立你屬於你的虛擬私人網絡(VPN)

精通科技的人們可能會想建立屬於自己的 VPN，但其實這大部份情況下均不是很好的選擇，除非你使用一些大型的虛擬私人伺服器 (VPS)或大型的伺服器租賃供應商。

- 如果你要設定你家中的路由器作為VPN的話，基本上你只是在令你所有的信息傳輸看起來像是從你家中傳送出去的。意味著只有你的實際處身的位置(並非你的家中)和你家中的連接才會使用已加密的傳輸資料。除此以外的所有東西則和正常情況下一模一樣，仍可以被你的互聯網伺服器供應商(ISP)追蹤得 到。
- 如果你正在大學的互聯網服務系統內設定 VPN(不論是以SSH協定為基礎的，還是

其他)，你的一舉一動將會被大學的 IT 部門完全監察。
- 理由同上，如果你要在你的公司內設定 VPN，你的一舉一動均會被公司的 IT 部門所監察。
- VPN這種東西其實只是在你要偽裝身處位置時有所作用(如觀看地區封鎖的 Youtube 或 BBC iPlayer 影片)，它們對於羣組通信這件事上全無幫助。

2.1.6. 安全地收發檔案

收發檔案其實跟收發信息的道理一樣，如果可能的話，請使用安全的通信軟件作為檔案傳送的媒介(如Wire 或 已加密的 Riot.im 對話；在你不能使用這些軟件時，才選擇使用 Telegram 的私密對話收發檔案)。

這些方法這只會令傳遞檔案時變得安全，如果你要令檔案變得難以辨認(或較難辨認)，請閱讀「2.2.5. 隱密地傳送檔案」的篇章；如果你要確保檔案能在傳送後安全地儲存，請閱讀「5. 離線保安」的篇章。

2.2. 保護你的身份(私隱)

這個分類將詳細講述各類幫助你的電子信息及網絡活動分離於現實世界，使人難以從這些地方辨認出你的身份。最理想的目標其實是達至完全匿名，但這幾乎是完全不可能的。因此我們會集中討論如何從最大可能出現的相關攻擊者當中隱藏你的身份，例子包括港共警察、港共政府及受聘的港共思想誘導員(三毛、網絡打手)。至於要從中共政府國家級別的情報網中隱藏起來，則需要 [進階] 或更高級的策略幫助才能成功。

2.2.1. 基本瀏覽器的選擇、設定及使用習慣

選擇

最低限度而言，請使用一個開源及更新頻繁的瀏覽器。這表示你的選擇其實就只有 Mozilla Firefox 或 Chromium。

Google Chrome 雖然是建基於 Chromium 開發，但它卻另加了一些秘密代碼。假如你相信Google的話，它是可以使用的。因為在此情況下，你實際上就有可能已經被NSA所監視；但最少以我們現在的環境而言，目前最大的威脅就只有港共及中共政府，而非美國政府。

要從 Firefox 及 Chromium/Chrome 之間選取作選擇的話，理論上，假設兩者均設定正確，Firefox 相對上較私隱 (privacy)，而 Chromium/Chrome 則比較安全 (security)，請

自行衡量你需要的糖衣毒藥。

另外，Safari 及 Internet Explorer 兩者都很容易被洩密，請避免用之。

至於流動電話上的瀏覽器道理完全相同。如果你在使用 Android 的話，請使用 Firefox 或 Chrome；如果你使用 iOS 的話，你就只能被梱綁在 Safari 之上，因為其他所有的「瀏覽器」都只是披著不同羊皮的 Safari。如果你的 Android 電話內置一些原生的「瀏覽器」軟件(當中包括很多不同的品牌)的話，請你停用它們而轉用 Firefox 或 Chrome。而在電話上 Firefox 比 Chrome 優勝的地方是它支援附加元件，所以你可以如桌面版 Firefox 一樣，安裝所有加強保安及私隱的元件(如 HTTPS Everywhere、 uBlock Origin、Decentraleyes 等等)。

建議設定

- 除慣用的搜尋引擎外，千萬不要轉用其他引擎(例如：若你不抗拒美國政府，可用 Google；否則可用Startpage或DuckDuckGo)。若你發現輸入錯誤網址時，會被帶到奇怪的搜尋網站，請考慮重新設置瀏覽器的偏好設定(Firefox > 於網 址欄輸入“about：support”，之後點擊「重新整理Firefox」
- [Chromium] 設定 > 顯示進階設定 > 隱私權 > 只勾選「保護您和您的裝置不受 危險網站攻擊」
- [Chromium] 設定 > 顯示進階設定 > 隱私權 > 內容設定 > Cookies > 勾選「封 鎖第三方 Cookie和網站資料」。如果你是初次設定，請繼續：所有Cookie 和網 站資料 > 清除資料
- [Chromium] 設定 > 顯示進階設定 > 系統(最底) > 取消勾選「Google Chrome/Chromium關閉時繼續執行背景應用程式」
- [Firefox]選項 > 個人隱私 > 歷史 > 使用自訂的設定 > 接受第三方 Cookie..永 不。

使用習慣

- 請永遠不要將瀏覽器的瀏覽記錄，密碼及 Cookie 同步到並非你所擁有的電腦上。因為這類瀏覽器的個人資訊基本上會毫無加密地保留在這些電腦之內。
- 每次當你見到「錯誤 HTTPS 憑證」的警告時，請馬上離開該網站。因為這有可能代表網站的管理人極其怠惰，或代表某些人正嘗試攔截你的瀏覽傳輸。
- 如果你的公司或組織要求在你的裝置上運行一些需要安裝額外 HTTPS 憑證的「網絡設定工具」的話，(你可以向你的 IT 職員詢問)，或者如果他們要求你手動下載一些憑證才能連接到WIFI 網絡的話，那麼大概 Eve 及 Mallory 均可以 看到你所有已加密的傳輸。
- 如非必要，請不要在瀏覽器內安裝附加元件及擴充元件。因為當愈多的第三方代

碼在瀏覽器上運行，那就代表 Mallory 能從更多的方位進行攻擊。
- 請學習分辨網絡上的釣魚網站。只要你將滑鼠指在超連結上，然後仔細閱讀瀏覽器下方實際上的連結網址，便能方辨真偽。例如一封從 customerserver@hsbc-bank.com.hk寄來的電郵其實並非來自 HSBC 的；一條指向「recovery.facebook-accounts.com」的連結其實並不是指向 Facebook 的(現時是指向至一個俄羅斯的網站)。

2.2.2. 用uBlock Origin阻截廣告及追蹤程式

我們推薦使用uBlock Origin作瀏覽器的阻截器。即使Adblock Plus曾經廣受歡迎，它現已被視作出賣用家的程式，因只要商家付出一定金額， Adblock Plus 便會放生某些廣告。

- 從瀏覽器的附加元件商店(add-on store)下載及安裝uBlock Origin(不是uBlock)
- 點擊右上方的uBlock Origin圖標，然後點擊齒輪，進入「設定」
- 「第三方過濾規則列表」> 生效。“EasyList”， “EasyPrivacy”， “Malware domains”， “CHN： EasyList China”
- (隨你喜歡)若你不想社交媒體追踪你的活動，而且你不信任「讚好」及「分 享」，你可以生效“Fanboy’s Annoyance List”和“CHN: CJX’s Annoyance List”
- 向上轆 > 應用 > 立即更新 (update now)

2.2.3. 使用 ClearURLS, Decentraleyes, 及 Privacy Badger 阻截追蹤

Decentraleyes 能加快讀取所有網站的 JavaScript 函式庫(JavaScript library)，同時阻礙 Google 或 Amazon 等的內容傳遞網絡記錄及追蹤你的傳輸。

ClearURLs 能改寫redirect URL，避免開啓連結時被追蹤去向。Firefox / Chrome

Privacy Badger 能補漏 uBlock Origin人手編寫的第三方過濾列表所沒有編入的第三方追蹤。

2.2.4. 線上帳號

2.2.4.1. 論壇及其他化名帳號

以下我會直接講述重點：

- 請勿在你希望有關連的帳號上使用相同的帳號名稱或密碼。假設你在論壇上以電郵地址 <alice@gmail.com> 注冊論壇帳號，你的帳號名稱為 "Alice" ，而你的

Facebook 帳號亦同時以電郵地址 <alice@gmail.com> 注冊。那麼任何人均可從你的論壇帳號找到你真實的 Facebook 帳號。

- 請勿使用論壇帳戶提及任何有關個人喜好，對於學校、商店等特定位置的認知，以及任何與你的現實身份有關連，而你不願意被人得知的東西。
- 請勿上載任何能夠以圖片搜尋便能追蹤到你的照片或圖片。[3]
- 如果你使用 VPN 或 代理伺服器(Proxy)，請勿在你使用及停用這些功能的情況下，同時登入相同的帳號。

2.2.4.2. 直屬個人帳號 (銀行、校友網站、Facebook、LinkedIn、Snapchat、Instagram、Tinder、 Grindr 等帳號)

- 請勿上載任何非必要的的東西至社交網絡，因為理論上所有東西一旦上傳至互聯網，其實就永遠會存留在互聯網之上，不論你之後有否將原圖刪除。
- 請將你的群組會員身份完全分離於你的直屬個人帳號之外。
- 請不要胡亂將陌生人加為好友。
- 當接收到濫發信息時，請忽略或封鎖它們。請勿作任何回覆。
- 用Grindr約炮的同性戀者要小心：Grindr已被中國公司收購。

2.2.5. 隱密地傳送檔案

純文字格式是最隱密的格式。如你必須使用其他格式，請繼續閱讀。

2.2.5.1. 數據（data）與元數據（metadata）

數據的私隱度取決於你的行為。如Word檔內寫有你的姓名和地址，則任何辦法亦不能保持隱密。

元數據則較為有趣。它指一些並非檔案內裏的資料，例如：Mallory可以得知Bob建立了一個pdf檔，及Alice影了一幅相，還知道當時他們所處的準確位置，及他們何時寄出及收到這些檔案。Linux用家可利用 Metadata Anonymisation Toolkit 2 (MAT2) 消除上述的蹤跡。若你是其他作業系統的用家，如Windows或macOS，則請繼續閱讀。

2.2.5.2. Microsoft Office， iWork 和 OfficeSuite 檔

所有辦公室軟件皆會泄漏能辨別個人身份的元數據，如非必要，應避免使用。可以的話，請用羣組限定的Google帳戶內的Google Docs。

但若你必須使用，請勿於Microsoft Office登入你的Microsoft帳戶。請在Office用戶名 稱及簡稱(initials)留白 (於File > Settings > User Name and Initials)。每次傳送檔案前 ，請

[3] 見：https://images.google.com https://tineye.com https://yandex.ru/images

先消毒 (sanitize)檔案 ：

- 單靠變更「作者」及「上次存檔者」(按右鍵>內容/詳細資料頁面上)並不穩妥。
- [Microsoft Office] 如欲使用自Office 2007內置的Office Inspector，請查看此文章，以取得詳細說明。它能移除姓名及更多私人資料。
- [iWork (如Pages等)] 當你想移除資料，可從Finder內的Get Info移除，但這不保證足夠。

2.2.5.3. 圖片與照片

- 圖片內的每項特徵都是獨特，而且可溯。故此，請按照常理，照片不應包括你的樣貌，常穿的衣服，獨特地標，常佩戴的手錶，電話機殼，常穿的鞋，及任何可以對比出你的身高的背景事物。
- JPEG與TIFF格式的圖片不只包含影像，還有相當份量被稱為EXIF的元數據。當中包括拍攝時間，相機/電話型號，圖片的地理位置定位，快門速度，甚至整張圖片的壓縮版。關於最後一點，諷刺的是，有人用Photoshop模糊樣貌，但EXIF內卻有整張未經修改的圖片。
- 移除EXIF的方法：
    - [Windows]於圖片檔上按右鍵>內容>詳細資料>移除檔案屬性和個人資訊
    - [macOS]使用ImageOptim開源軟件，於<https://imageoptim.com/mac>取得。
    - [Linux] 使用MAT，或jpegoptim：
        - $ jpegoptim --strip-all file.jpeg

2.2.5.4. 專案檔(平面設計、影像處理等的媒體檔案)

所有於 Adobe Creative Suite 以及所有專業的音訊、影像處理等軟件均喜愛將詮釋資料(Metadata)附加於你的檔案之內。姓名是其中一樣你不會希望被記錄在內的東西，但不幸的是有很多版本的不同軟件均無法使有單一而有效的方法來消除這些資料。

所以，我們首先就應避免將姓名加到軟件之內。同時，請勿在安裝軟件時登入任何與 Adobe　或你所使用的軟件相關的個人帳號，並請確認你電腦的登入帳號名稱並非只有你一人使用，那麼別人就不能從你的帳號名稱尋找到你的真實身份。

2.2.5.5. 釋出 PDF 檔案

由於PDF 檔案 會包含可怕的「作者」(Author)及「創建者」(Created By)名稱，它實際上是個人資料的地雷。這些資料一般而言只能透過收費軟件 Adobe Acrobat 才能夠移除。幸運的是，我們活於這個充滿著開源軟件及免費軟件黑客的世界，他們已經解構了整個 PDF 背後的規格。

因此，只要下載Zaro編寫的 PDF Metadata Editor，一個開源並適用於所有作業系統平台(包括 Windows、macOS 及 Linux)的軟件，使用它來開啟 PDF 檔案即可刪除所有你不喜愛的東西。 （源碼：https://github.com/zaro/pdf-metadata-editor）

2.2.5.6. 釋出音訊檔案

很多音訊格式包括 MP3、AAC、Ogg Vorbis 以及 Opus 等，均會在儲存音訊的同時記錄你的詮釋資料(Metadata)。很多時候這是非常有用的，因為「演出者名稱」、「唱片名稱」以及「音軌編號」等均會包括在內。然而，當你想製作音訊檔案作組內用途的時候(例如錄音或混音)，請僅記，不要將任何能夠辨識身份的名字釋出到音訊檔之內，例如將你的姓名加到「演出者名稱」的標籤之上。

2.2.5.7. 壓縮檔案(Zip、Rar、7z、Tar 等)

- 如果你壓縮整個資料夾的話，Windows 系統釋出的 thumbs.db 檔案內有可能會包含從你上一次刪除該 db 檔案後，資料夾內所有舊圖片的縮小剪影。
- 千萬不要依靠 Zip 及 Rar 的密碼加密功能，因為要將它們破解實在容易得可笑。而且 Zip 的環境下，只會有一部份的檔案是有加密，所以並不安全。
- 7z 是 比較上優勝的，但當面對現代 CPU 的破解威力時，它仍顯得微不足道。如果你需要運用密碼來保護檔案，請使用正規的加密軟件，如 GPG。

2.2.5.8. [進階] 讓人不能以你的文筆風格辨認出你的身份

司法語言學[4]是一門憑藉某人所使用的措辭，包括詞語、文句以及語法等的風格，來辨認出某人真實身份的科學。我不清楚對中文而言這種方法是否複雜進階；但以英文來說，即使你使用匿名發文，要用這種方法來識辨你的身份其實仍然是頗為容易。

要避免此事發生，可以使用 Anonymouth 這個協助你堆砌語法及文筆風格的軟件。

2.2.6. [進階] 避免留下任何的網絡瀏覽指紋：戴頭盔防止意外

現時的情況下，我們並不需要用這種戴頭盔方法的，而且最好永遠也不需要用到。以下是一系列的指引，教你如何於廣大的互聯網群體中隱藏自己而不留痕跡。

- 善用Firefox containers：Multi-Account Containers及Temporary Containers
- 停用所有的附加元件，例如 Flash 及 Java。
- 使用 uMatrix(Firefox、Chrome及Opera)或 NoScript(Firefox)，預設停用所有的 Javascript，有需要的時候才將要用的 Javascript 加入白名單。

[4] https://en.wikipedia.org/wiki/Forensic_linguistics

- 使用 Secret Agent 將你的 HTTP header 變得隨機
- 使用 Cookie AutoDelete自動刪除所有 Cookies
- 使用 Canvas Defender 將你的帆布指紋 (Canvas Fingerprint)變得隨機

2.2.7. [進階] 使用 Tor 隱藏行蹤

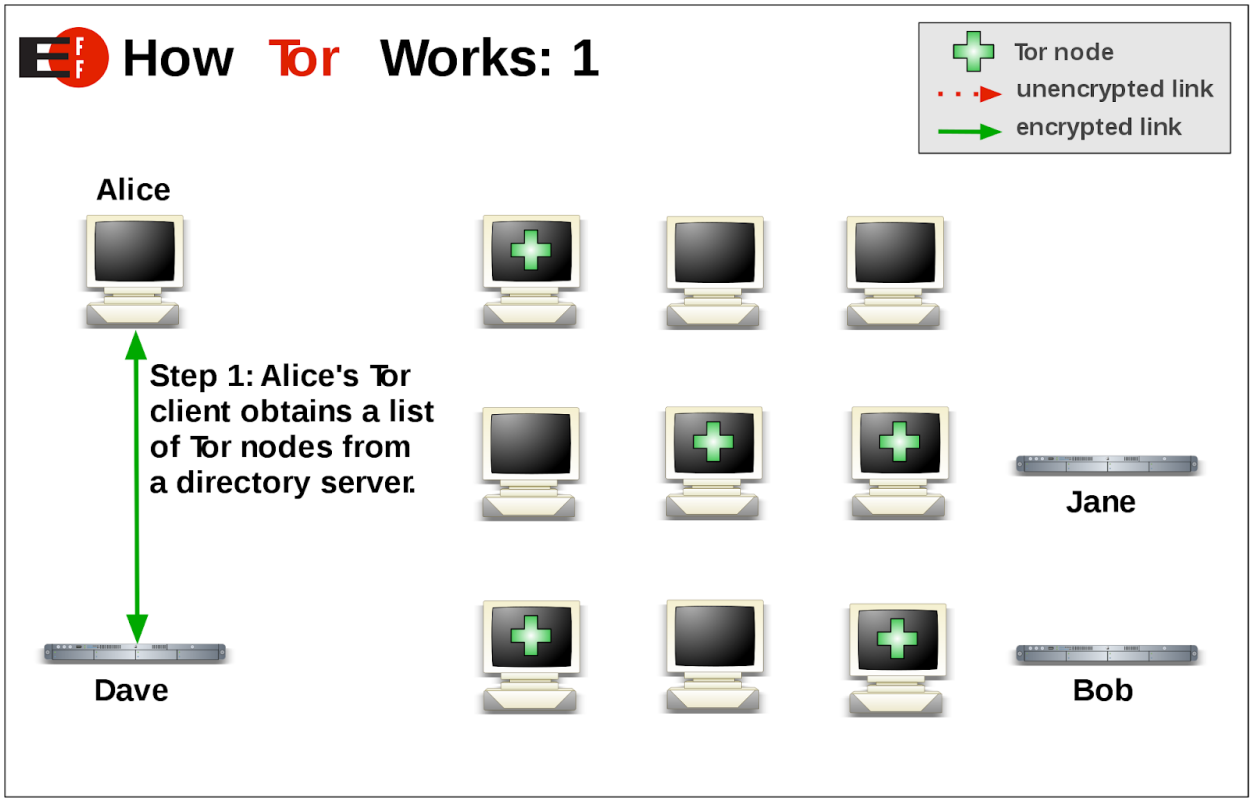
Tor 的原理就如洋蔥一樣，它會將你的互聯網傳輸信息進行三次加密，然後再轉送去三部不同的電腦。每一個的轉遞站(hop)都只能夠剝開信息中最表層的密碼，在這個方法下，途中便無人能夠得知整條信息了。

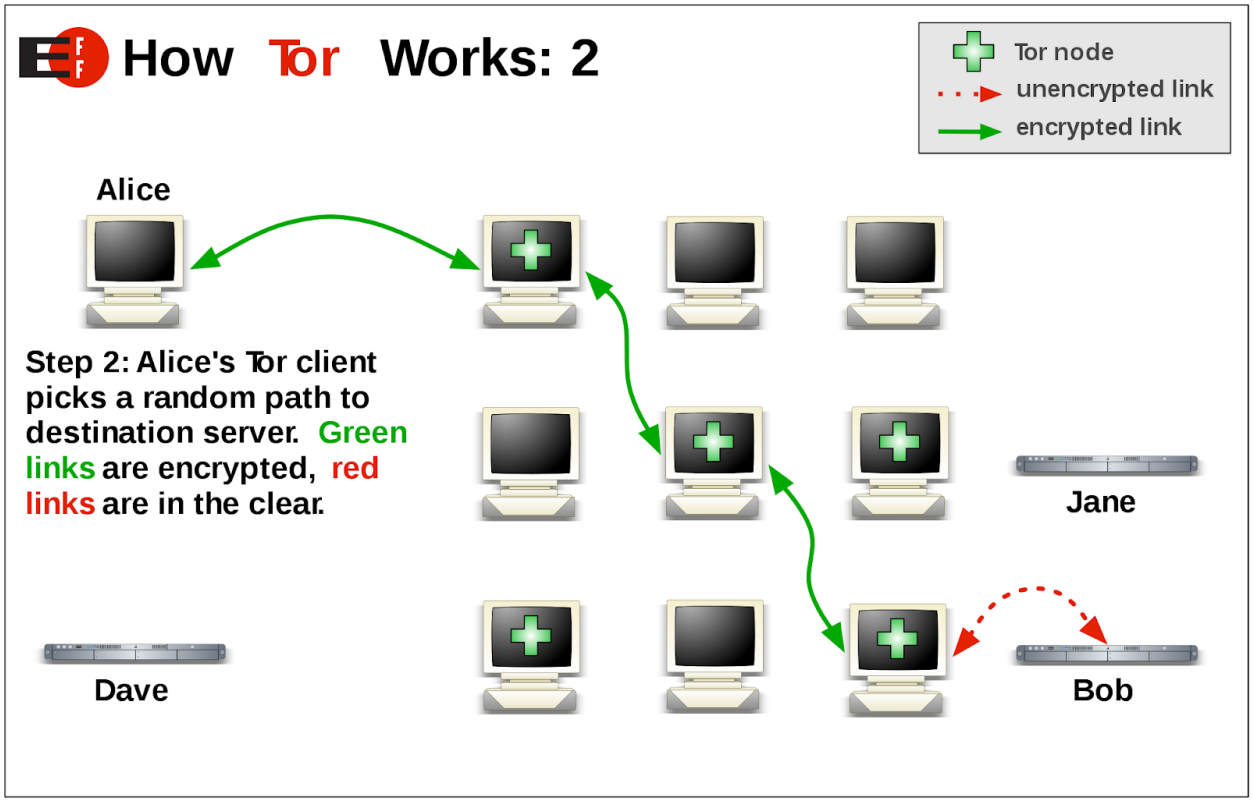
Alice >>>> Eva >>> Evelyn >> Evey > Bob

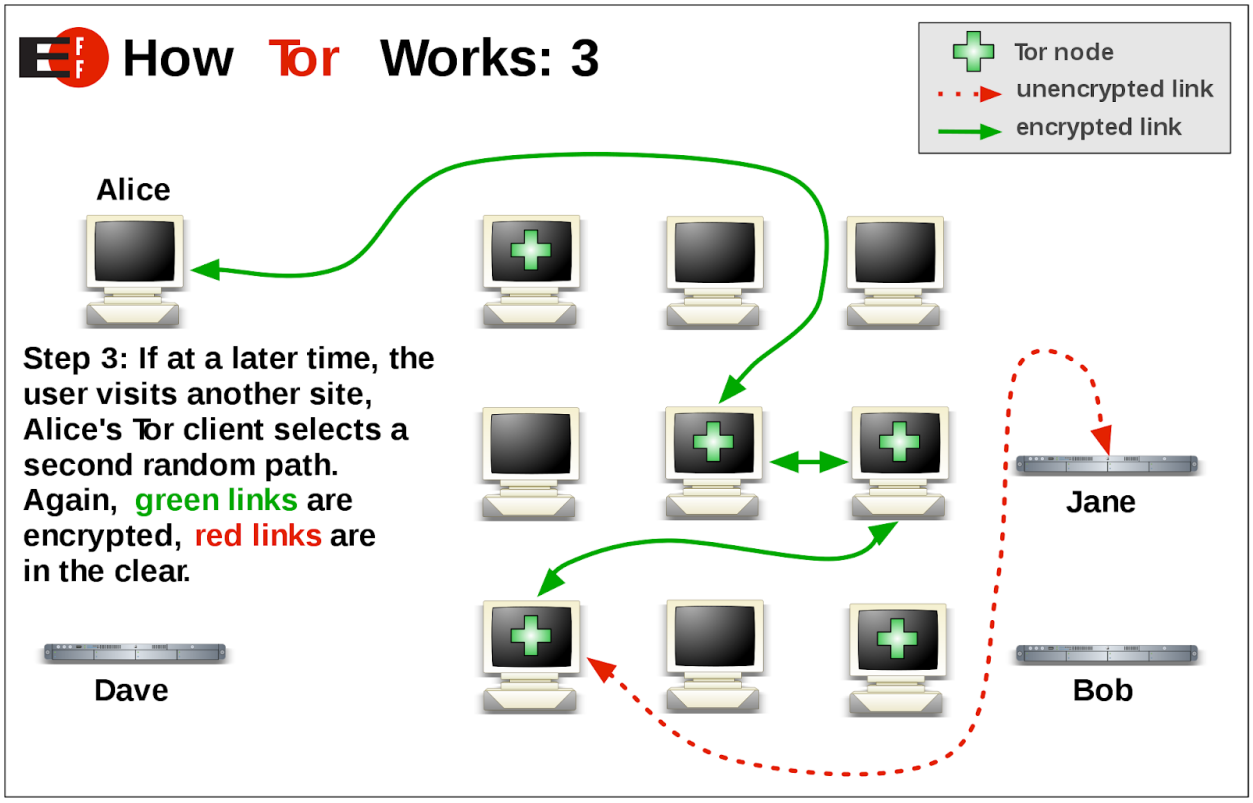
在這裡，Eva 從 Alice 得到一個信息，Eva 便可解密信息的最表層，然後該信息會提示她轉交信息給 Evelyn。Evelyn 從 Eva 得到一個信息，然後就會再解密一次，並提示她將信息轉交給 Evey。Evey得到從Evelyn而來的信息，再解密最後一次，便會傳送給Bob。

在此情況下，Eva 最多只能夠得知 Alice 正嘗試將一個加密信息傳遞給某人； Evelyn 則會知道某人正使用 Tor 網絡；而 Evey 會知道有人與 Bob 正進行通信。如果 Alice 與 Bob 之間的通信本身是用HTTPS 加密的話，那麼 Evey 就不能夠得知信息的內容了。

要描述當中的原理，亦可以參考以下 Tor Project 的解釋圖：


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob



然而，假如美國國家安全局(NSA)覺得你是一個值得追蹤的目標的話，它們確實是有足夠資源去追蹤你的。它們可以很容易就能搜查世界各地它們所控制的電腦，包括 Eva 、Evelyn 及 Evey，對她們而然都不過是一樣的婊子。另外，我們現在仍未得知中 共政府是否有同樣的能力去進行追查。

如果你要使用 Tor，請勿自行設置它。除非你已經使用過或對此十分熟悉，否則你必定會把它搞亂。相對地，請下載並使用 Tor Browser Bundle，它已經幫你設定所有你需要的東西。

注意：千萬不要在你使用 Tor 的時候登入你的私人帳戶。使用 Tor 來瀏覽你的個人 Facebook 是極度愚蠢的行為，千萬要小心。

2.2.8. [進階] 暗網(Dark Web)

暗網，簡而言之，是互聯網中無法從正常途徑進入或讀取的一部份。你不可能使用搜尋器找到任何的暗網網站；你亦無法使用你的常用瀏覽器瀏覽暗網。要瀏覽暗網網站，首先要先將自己置身於暗網之中。

在暗網中你能夠找到包羅萬有的東西，包括賭搏、書籍、數學解迷的論壇、非法色情圖片、黑市交易、毒品、罪行告密、盜版及假卡、軍火槍械，以至恐佈組織均盡在其中。

除非你很清楚自己在做什麼，否則請遠離以上的網站。

我只會列出一些受歡迎的網站出來，請仔細閱讀它們官方網站，學習如何進入其實際的網站。如果你走進去的話，大概你會發現它們其實很無聊的，除非你真的要在裡頭尋找你需要的東西，此時你就需要用用你的常識及小心注意一切了。

- Tor Onion Services：你需要運行 Tor 來進入它們的網站 (有限列表)
- I2P(The Invisible Internet Project)：一個存在於正常互聯網世界以外，匿名、端對端加密、保密及隔離的網絡。在 I2P 內，使用 Torrent 是允許的，而 你可以使用它瀏覽網站、聊天、寫Blog、儲存及收發檔案。它就像一個屬於它自己的互聯網，而且有很多有趣的材料可以在當中找到。
- Freenet：匿名的檔案發佈系統，就像雲端一樣，但無人知道這朵雲的位置何在。裡面有一大堆的非法色情圖片，瀏覽時請自行注意。
- IPFS：次世代的發佈網絡。你可想像它是一個沒有伺服器的互聯網，任何人均可以是一個伺服器，而且沒有人知道何者才是真正的伺服器。網絡正在高速開發中。

3. 流動電話保安

3.1. 總括建議

電話是可怕的東西。電話同時是兩台電腦：一部份是使用 Android 或 iOS 系統的電腦；另一部份是無線電組件。因為無線電組件是一個黑盒，所以沒有人能實際地知道到底它正運件哪些軟件。就算你將你的電話完全關掉，基於現今大多無線電話皆裝有不能拆除的電芯，無線電組件乃有可能廿四小時運行並向無線電收發站傳送某人想索取的資料。

就算你的 Wi-Fi 及其他所有東西均關掉，你所在的實際位置仍然很容易就可以以三角測量的方式被無線電收發站計算出來。而且，由於你的無線電晶片可以以一星期 7日 24小時無間斷地運行，假設一部電話的位置必然能夠在 7 日 24 小時被你的電訊公司 記錄並查找得到；而你的相機鏡頭及麥克風亦有可能長期開啟，那麼你每日隨身攜帶的東西其實就是一個完美的監控裝置。

因此，請儘量不要使用流動電話作任何行動組內的機密工作。

當出席公眾示威、遊行、或任何同好集會，請你將流動電話留於家中。事前請安排一位好友(沒有出席同好活動的好友)於活動結束後的特定時間內於他通電；若然你未能致電給

他，你的朋友則應意識到你已經失蹤或已被拘捕，繼而向其他行動組內成員發出警示信息。

你應避免使用任何生物識別功能(指紋、面部及聲音等)進行電話解鎖。請僅記，警察只要使用一些基本工具複製這些你的特徵，很容易就可以解鎖；而且因為香港身份證的關係，政府必然已經擁有你的指紋。

3.1.1. 電話通話 及 SMS

請假設所有的電話通話及 SMS 信息均可能被攔截。

SMS 是極度不安全的，它的傳輸從不加密。要讀取大氣電波內流動中的 SMS 只要使用非常廉價的裝置就很容易可以辦得到。寄件人可以隨意將寄件的電話號碼篡改為任何他想要的東西。

不論有線(家居及辦公室)或無線(流動電話)，電話通信同樣地不安全。任何一個陌生均可運用名為 IMSI-catcher 的廉價裝置偷聽你所有的對話內容，並追蹤你的準確所在地。

請自行考慮任何已加密的即時通信方式取代 SMS：即使是 Whatsapp 仍然會比未加密的 SMS 優勝。而如果你要進行通話，請考慮：

- 使用 Wire 或 Telegram secret chat 作個人通話及團體通話。
- 如果兩者均知道對方的電話號碼，亦可使用 Signal(建議)或 Whatsapp(較 差)。

3.2. iOS： 最佳用法

- 不要安裝微信，任何一類「垃圾清理工具」，QQ，及任何騰訊(Tencent)及獵豹移動(Cheetah Mobile) 所開發的程式。
- 不要用生物辨識程式，例如TouchID等等。
- 選用6位數字的PIN。設定PIN，你的電話便自動加密。
- 電話PIN不應與信用卡的PIN相同。
- PIN不應是英文字母形狀，或任何簡單，明顯的圖形。
- 若你的iPhone已越獄(jailbreak)，等於你完全允許任何得到你電話的人任意使用你的電話。如非必要，切勿越獄。
- 保持iOS更新。

3.3. Android： 最佳用法

- 切勿安裝微信、Clean Master、QQ、或其他中國軟件。
- 不要用生物辨識程式。
- 選用6位數字或以上的PIN。
- 電話PIN不應與信用卡的PIN相同。
- PIN不應是英文字母形狀，或任何簡單，明顯的圖形。
- 加密你的資料分區 (data partition) 。設定位置因製造商而異。於市面上的Android，則於設定(Settings) > 保安(Security) > 加密電話(Encrypt phone)
- 若你解鎖你的啟動程式(bootloader)及/或取得系統最高權限(即Root機)，等於你完全允許任何得到你電話的人任意使用你的電話。如非必要，切勿解鎖你的啟動程式及/或Root機。
- 考慮以Firefox或Chrome代替三星Samsung/索尼Sony/小米等瀏覽器。若使用Firefox，請如電腦版Firefox般，安裝附加完件 HTTPS Everywhere 、Decentraleyes及uBlock。
- 當Mallory試圖以IMSI-Catcher測度你的位置，及用無線電竊聽電話通話時，而 你又想收到警告，請安裝Android IMSI-Catcher Detector （注意：Project被重寫中，舊版並不能偵察近年新一代的IMSI-Catcher）
- 保持Android更新。

4. 連線保安

4.1. 防火牆

- Windows或macOS的用戶，請確保內置的防火牆正在運作。
    - [Windows] 控制台 > 系統及安全性 > Windows防火牆
    - [macOS] 系統偏好設定 > 安全性與隱私 > 防火牆
- 前往選項，確認無垃圾程式能穿過防火牆。若你發現某些程式，是你沒有安裝的，且防火牆允許通過，應阻止它穿過防火牆，並解除安裝。
- 至於Linux用家，請檢視正監聽的端口，以確認無不必要的伺服器在運作。
    - $ sudo lsof -i -n or $ sudo netstat -ntulp
    - 另外，以iptables設置防火牆。Ufw及gufw是很好的使用者介面(front-end)。

4.2. 無線上網保安

- 應盡避免無線上網。
- 避免使用藍芽耳機，因其他人極容易竊聽你的談話內容。
- 避免使用公用無線網絡，包括PCCW或麥當勞的熱點。手機不要自動連接它 們。
- 較新版iOS及Android都有隨機化MAC地址的設定，務必開啓。
- 配置你的無線路由器至WPA2(個人版)安全系統(不是WEP)，AES加密(不是 TKIP)，關閉WPS(非常重要)，及使用一個安全的密碼(關於「密碼」，請閱附錄)

4.3. 有線上網

- 當心鍵盤記錄器。
    - 硬件上的physical security能凌駕於任何軟件加密，所以每次使用電腦是都請望清楚有否被人改動。見下圖：

圖中並非USB安全套，此乃鍵盤記錄器，會盜錄一切鍵盤敲擊。

- 若面對的敵人是國家級，請以相片記錄主機板及每一個插口，並以紙質封條作機箱被開啓的指針
    - 基本上，平民是無可能抵擋整個國家的資訊攻擊資源的。若平民真的認為自己是敵對國家積極監控（national level targeted surveillance）的對象，請申請政治庇護。

5. 離線保安

5.1. Microsoft Windows

- 請勿用生物識別系統(面貌，指紋，語音解鎖，如Microsoft Hello)登入。
- Windows 8及之後的系統毫不保障私隱，Windows 10則更糟。如必須使用，請到開始>設定>變更電腦設定>隱私權關閉所有選項。 Windows 10 已預設將所有你輸入的資料傳送往Microsoft。
- 請將所有有關羣組的敏感資料儲存在VeraCrypt隱藏加密庫 (hidden container)內。請詳閱Veracrypt的初用指南，惟請在第四步選擇 “Hidden VeraCrypt Volume” 。在外層加密庫 (outer volume) 先儲存一些個人資料，如銀行戶口資料，普通帳戶密碼，甚至一些令人尷尬但合法的色情影片，隱藏加密庫 (hidden volume) 則儲存羣組的敏感資料。
- VeraCrypt全機加密（Full-Disk Encryption）。系統(system)>加密系統分割區(Encrypt System Partition/Drive)，之後請依照指示繼續。
- 基於Windows對Bitlocker的擁有權，我們不鼓勵用它加密資料。Microsoft已將整個Windows的原碼交予中國政府，故此，千萬不要使用BitLocker。
- 務必安裝防毒軟件。Windows內置的Microsoft Security Essentials已經足夠，甚至比坊間售賣的更好。
- 盡可能使用自由開源的軟件 (free and open-source software)。請參閱免費且公開的軟件推介（free and open source software, FOSS）。
- 請確保Windows及所有軟件保持更新

5.2. macOS

- 請將所有有關羣組的敏感資料儲存在VeraCrypt隱藏加密庫 (hidden container)內。請詳閱Veracrypt的初用指南，惟請在第四步選擇 “Hidden VeraCrypt Volume” 。在外層加密庫 (outer volume) 先儲存一些個人資料，如銀行戶口資料，普通帳戶密碼，甚至一些令人尷尬但合法的色情影片，隱藏加密庫 (hidden volume) 則儲存羣組的敏感資料。
- MacOS用家只能靠蘋果自家的FileVault作全機加密。可惜FileVault的源碼並非 開放，這少不免會引致麻煩。縱使沒有保安專家信任它，但很抱歉，它是唯一選擇。
- VeraCrypt全機加密(Full-Disk Encryption)。系統(system)>加密系統分割區(Encrypt System Partition/Drive)，之後請依照指示繼續。

- 務必安裝防毒軟件。現時，Mac機已受到愈來愈多惡意程式攻擊，蘋果電腦在保安上表現得十分差勁。
- 盡可能使用自由開源的軟件 (free and open-source software) 。請參閱免費且公開的軟件推介。
- 請確保macOS及所有軟件保持更新

5.3. GNU/Linux

- 盡量由軟件庫 (software repository) 內安裝所需程式
- 請將所有有關羣組的敏感資料儲存在VeraCrypt隱藏加密庫 (hidden container) 內。請詳閱Veracrypt的初用指南，惟請在第四步選擇 “Hidden VeraCrypt Volume” 。在外層加密庫 (outer volume) 先儲存一些個人資料，如銀行戶口資料，普通帳戶密碼，甚至一些令人尷尬但合法的色情影片，隱藏加密庫 (hidden volume) 則儲存羣組的敏感資料。
- 以LUKS作前端(frontend)，進行dm-crypt全機加密。Ubuntu，Debian及Fedora都能趁安裝期間，輕易執行這些工作。若想親手加密，請細閱ArchWiki有關加密(disk encryption)的文章。
- 設置一個執行rkhunter的cronjob

5.4. 其它作業系統

- OpenBSD 乃為最安全的作業系統
- 由 Terry A. Davis 所編寫的 TempleOS 可能更為安全。 Davis 為一名精神分裂的自閉人士，據稱能以 TempleOS 的隨機數字生成器與神溝通。

“Yeah， I killed a CIA nigger with my car in 1999. Score one for the good guys.”

- Terry A. Davis

Appendix I. 論密碼

只要密碼脆弱，再好的加密運算方式、再好的資訊安全指引，亦只能作廢。

選擇密碼：常見錯誤

- 不同的帳戶，用一樣的密碼

- 不同的帳戶，用一樣的密碼為本，再加不同的數字或字母於尾
- 密碼中用到個人名字、生日、電話號碼、足球隊名、卡通角色名字等元素
- 誤以為「h0nGk0Ng-43v3r!」比「hong kong forever」難破解
- 誤以為「!#@HongKong%$#」比「hong kong」難破解
- 誤以為「Hong Kong hOnG kOnG HoNg KoNg」比「hong kong」難破解

寄存密碼：常見錯誤

- 把密碼寫在紙張上
- 把密碼存入非自由軟件密碼庫內(意即：切勿使用1Password，LastPass，Keeper，及Enpass)
- 把密碼告訴給任何另一人

如何選擇密碼

好的密碼，世上有二：

- 每個網站、用戶、帳號獨有的密碼，由專有密碼庫軟件運算出，並以密碼庫軟件收藏
- 兩個「總密碼」，一個用來解開密碼庫，一個用來解開加了密的硬碟

要依賴人腦記憶的，只有這兩個「總密碼」。

這兩個總密碼該用Diceware方法運算。現時已有網站及手機apps能輕易地「一鍵運算」Diceware式密碼。Diceware的好處是它並不是一連串亂碼（e.g. 73na%$g8*），而是幾個人腦可以理解的字（e.g. uninvited quantum football zoology from dribble）。以下會首先講解手動步驟，約無興趣可略過：

1. 找一棵六面骰子
2. 下載Diceware字表(原祖英文字表，EFF公佈的簡易英文字表)
3. 字表中每一行有多少個數目字，就擲多少次骰子(e.g.　用原祖字表者，則擲骰五次，用EFF字表者，則擲四次)
4. 如是者，從字表中找到「總密碼」的第一個字(e.g.　若擲到　“1-1-1-1”，那麼在EFF字表中，便是 “acid”)，把這字寫在另一張紙上。
5. 重複以上步驟至少四次，「總密碼」越多Diceware產生的字，則越安全。
6. 事成!
7. 牢記你的Diceware「總密碼」，並銷毀寫有「總密碼」的紙張(用火燒成灰，加水，再沖入廁所)。Diceware字表並不需銷毀。

若不想用傳統紙筆方法，可見以下：

- Diceware Android app： Diceware
- 以下網站其一：https://www.dmuth.org/diceware/或 https://www.rempe.us/diceware/
- 坊間的軟件密碼庫已有Diceware generator，或名為 “passphrase” ，以下推介的KeepassXC為其中一個。

如何存放密碼

至今只有一款可信用的軟件密碼庫：

- Windows 用戶可採用 KeePass 2 或 KeePassXC
- Linux 及 macOS 用戶可採用 KeePassXC
    - KeePassXC安裝後，在瀏覽器用KeePassXC-Browser把兩者連結
- Android 用戶可採用 Keepass2Android
- iOS 用戶可採用 MiniKeePass

KeePass　密碼庫不只能給你安全地存放密碼，更能自動運算出給每個網站、每個帳戶獨有的密碼。

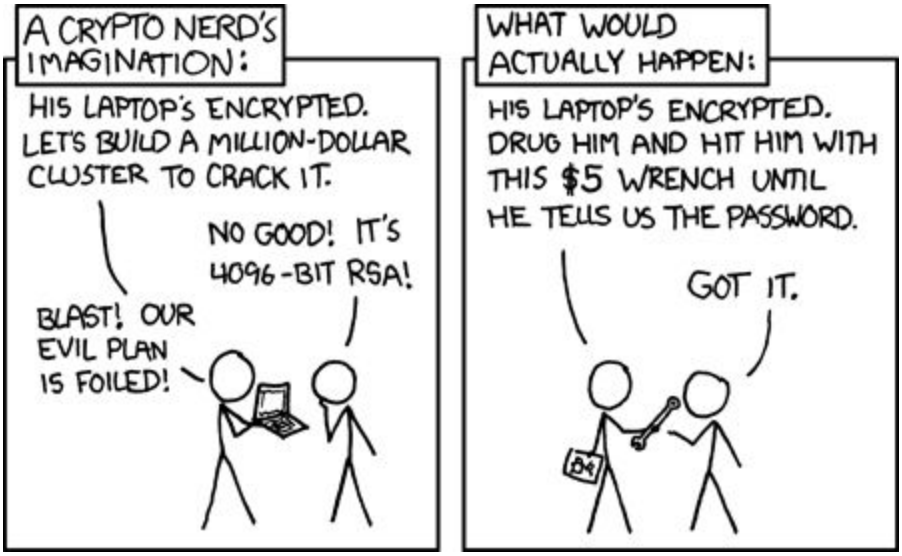
密碼外再多一重保安：雙重認證（two-factor authentication, 2FA）

萬一密碼外泄，只要你已開啓2FA，並且2FA的裝置沒有被攻陷，那麼用戶資料仍然會受保護。

支持2FA的網絡服務名單：https://twofactorauth.org/

注意：若可以，請勿使用以SMS作基礎的2FA，因為SMS是完全不安全的。

論密碼保安與人事保安



再好的密碼，只要知道密碼的人沒有做好人事保安，密碼泄漏只會是遲早的問題。

Appendix II. 警察抄家應變措施

按住電腦的開關制，完全地關掉電腦，並拔掉濕電插蘇。若有時間(極無可能)，關掉手提電話，否則，至少按制把電話鎖上。當警察上門抄家，你是沒有時間做任何其他應變的。

假設你已經依照本指引把你的手機及電腦硬碟加了密，把它們關掉是唯一能夠令到加密起作用的方法：只要電子產品處於開機(或手提電腦蓋上後的準備)狀態，硬碟的資料是被解了密，並寄存於RAM內的。

不要對警察說任何一字，不要承認或否認在你的電子產品裏有對警察「有趣」的資料或檔案，保持緘默。

你是沒有時間去把你的電腦或電話躲起來的，更莫論「摧毀硬碟」。用微波爐加熱光碟或用電鑽鑽入硬碟都為電影情節-對摧毀資料是毫無作用的。

總結：完全折斷電源，保持緘默，搵律師。