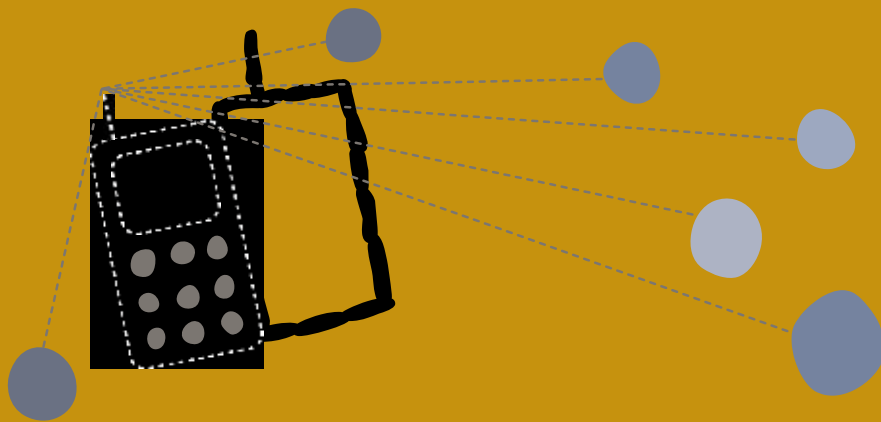


網絡和手機之 安全及隱私



諸如手機和網絡這些新科技是非常強大的宣傳工具，但是使用這些科技來傳達敏感信息會為你、你的聯繫人、朋友和同事帶來風險，此卡的目的為幫助你使用手機及網絡時安全地獲得以及保護資訊。

什麼是數位安全和隱私？

資訊權利和數位安全遭到破壞的跡象可能包括：

- 密密碼在你不知情的情況下被更改了
- 私人信息似乎被收件人以外的人讀過
- 網站在某些國家無法瀏覽
- 官員透露私人信件的資訊，包括數據、名字或者主題。
- 行動電話被監測。

我有必要關心嗎？

如果上述情況會損害你的項目，或者暴露或迫害你或者你的聯繫人，那麼你就應該留意。這些攻擊隱私的知識和電腦軟件在互聯網上都能找到，如果攻擊者有足夠的權限侵入你國家的網絡或者是手機基礎設施，進行攻擊所需的科技是十分簡單的，除了政府機構，網絡服務提供者（ISPs），和手機公司有權限進入這些基礎設施，你的公司同事、鄰居和網吧營運者也可能具有這些權限。

本卡包含哪些安全議題？

本張卡片主要針對網絡工具和行動電話的安全，然而，還有許多其他的科技能使你受到審查、監視和迫害，儘管這些科技不在此卡討論範圍內，重要和基礎的防護措施包括經常更新電腦操作系統、使用並更新可信賴的反病毒軟件和經常性地備份文件。如果你有理由相信你的電腦或者數據儲存裝置，包括你的備份，有遺失、被盜或者被沒收充公的風險時，又或者你的組織可能遭到網絡監視的時候（或者此情形普遍存在於你所在的地區），那麼你需要Tactical Tech（戰略科技組織）的安全工具包。

網絡宣傳工具

當使用如博客，Facebook和Twitter這些網絡工具來動員或者協調活動時，別忘了你儲存在這些平台上的資訊在某種程度上已成為這些工具營運者的財產，許多平台工具會洩露超過你所預計的訊息量。

當你在線上平台儲存敏感的資訊，請閱讀它們的隱私政策或者用戶協議，記住，即使是最開放的政策和條款裡，你的訊息也是在平台工具管理者的直接控制下，你的資訊可能在未經你授權也未告知你的情況下，被洩露、銷售、以及轉移，即使你注銷你的帳戶，許多平台和工具並不會刪除你發表過的內容或者你提供的私人訊息。最後，除非你有特別的理由必須使用大型商業平台服務，例如它易於瀏覽使用，或者因為這些大型平台吸引一些低調的用戶，否則盡量使用一些支持人權及資訊權的平台工具：例如用Blip.tv代替YouTube；和用riseup.net代替Gmail，如果你有技術等資源，你也可以營運自己的網絡服務。

如果你用大型商業平台，小心保護你自己，避免懷有惡意的人士從這些服務平台上挖掘你的私人資訊，尤其是諸如Facebook和Myspace的社交網站，對這些平台的隱私保護政策要有深入的理解，並仔細考慮哪些資訊是你可能會在不經意的情況下洩露，例如你的真實姓名、住址、旅行目的地，和即將舉辦的活動或會議的相關細節。如被監測一段時間，這些訊息可以大致描繪出你的日常生活和工作模式的。

一個有用的方法是在一個網絡平台上註冊使用多個帳戶，這樣你能將不同的帳戶和個人資料用於不同的項目，你也可以建立一個監控自己的監控帳戶，如果你能夠用不同的渠道去了解哪些關於你的資訊是公開的，你的帳戶隱私就能得到更好的保護，例如通過網絡搜尋引擎搜索，或者透過有特殊權限的人。

密碼

絕大多數網絡工具以及平台使用一個密碼來保護你的帳戶，如果一個惡意人士或組織知道了你的密碼，那麼無論你多麼信任網絡管理員，或是多麼小心的保護你的隱私：你都將立刻失去你的隱密性和匿名性。

比較不為人知的盜取密碼的方法包括：惡意人士在你用來登錄安全網站的電腦上安裝惡性軟件，或者在你登錄不安全的網站時監測你的網絡連結。

為了防止受到第一類密碼盜取攻擊，建議使用你自己的電腦，或使用你信任的人維護的電腦，確保電腦的操作系統和反惡性軟件是最新的。為了防止第二類密碼盜取攻擊，使用安全連結上網，絕大多數的網絡郵件服務，社交網絡平台，博客，地圖和視頻平台都提供安全連接，叫HTTPS，你可以在瀏覽器的地址欄裡檢查地址是否以”https://”開始(而不僅僅是”http://”)，然而除了當你輸入你的密碼，許多網絡工具並不使用HTTPS去保護任何資訊，這樣的結果是如果有人長時間監控你的網絡連結，他們即得知你在那個網站上儲存的資訊，所以最好的防衛就是找在所有網頁裡都使用https的網絡工具。

規避审查

你可以使用安全網絡代理主機，審查規避工具或者匿名軟件諸如Tor，在你瀏覽的網站中隱藏你的身份，或繞過互聯網過濾器，這些工具在你需要進入被審查的網站時很有效，例如為了蒐集資料瀏覽網站，或者為了上網絡平台如Facebook。

在網上匿名

當你不想洩露你瀏覽過什麼網頁的時候，像Tor這樣的匿名軟件很有用。Tor讓你的網絡連結在幾台隨機的自願電腦之間跳躍，以防止你的ISP或者政府級的觀察員知道你在網絡上做什麼，然而除非你透過HTTPS網頁連結，不要用Tor在不安全的網站上發送或者接收敏感信息，否則那些你連結的自願電腦有機會監控你所傳輸的內容，Tor基本上是安全的，但是它的缺點是會讓你上網的速度變慢。

行動電話

行動電話在世界各地被普及地使用，但他們往往儲存大量需要保密的資訊，除了通信錄，手機還記錄了通話記錄、日曆、短訊和電子郵件。

想想儲存在你手機裡包含哪些資訊，尤其因為手機極易被沒收，如果你正從事敏感的爭權工作，如爭取人權，你可能不需要在手機的通信錄裡儲存你所有的聯繫人，你也應該隨時刪除手機和SIM卡上的資訊因為短訊是容易被搜索和過濾的，所以在發短訊時避免寫入敏感關鍵詞。只要手機是開機狀態，就可以被用來追蹤你所在的方位，參加敏感聚會的人在出發前應該關掉手機並拿出電池，直到他們返回時再安裝電池，將手機開機。行動電話的通信業者保有所有通話呼叫的細節：在何時何地與誰通話等資訊，這些資訊記錄可能被保存幾年，如果政府官員要求這些業者提供相關電信資訊，電信業者可能負有法律責任必須提供這些資訊。

行動：辨識安全風險

使用以下問題進行你的安全風險評估，幫助你決定使用何種方法來降低風險。

1. **我經手敏感資訊。**知道你所處理的資訊是否可能導致他人對你的監控是非常重要的，你是否在從事一些可能被政府、警察、軍隊或是私人企業視為敏感或干擾性的活動？如果是，除非你執行一些安全的措施，你可能置自己和他人於危險。
2. **我和需要保護身份的人共事。**也許你正在收集一些私人隱私的資訊，例如有關家庭暴力的資料，或是強迫勞動又或者有關強奸的資訊。如果他人向你提供的資訊會置他們於險地，則你必須採取防護措施以確保資訊的保密性。
3. **我在網上和處理敏感信息的人交流。**即使你覺得你沒有安全顧慮，如果你在網上和有這些安全顧慮和風險的人進行交流，那麼你就可能成為他們對手的目標對象，這是因為他們可以利用你而得到他人的私人資訊。
4. **我在敏感網站上瀏覽或發佈訊息。**也許你向人權組織網站提供訊息，或者發表文章公開反對那些你認為不尊重人權的團體，其實僅僅是瀏覽敏感網站都有可能使你成為目標。

互聯網安全和隱私資源

更多資訊和下載安全工具

1. **Security in-a-box** 是由Tactical Tech和Front Line所共同製作，滿足人權運動和捍衛者的電子安全和隱私需要。 <http://security.ngoinabox.org/>
2. **電子安全和人權捍衛者的隱私**是由Front Line所提供的可用於評估和處理電子安全的威脅。 <http://bit.ly/1aCkSs> (frontlinedefenders.org)
3. **Mobiles in-a-box**有整個部分是針對手機安全和隱私保護。
<http://mobiles.tacticaltech.org/security>
4. **使用Wordpress和Tor的匿名博客**。Global Voices編製了這個指引來支持人權擁護者，幫助他們揭示真相和在線上表達他們的看法，最重要的是避免隨發聲而來的風險。[http://advocacy.globalvoicesonline.org/projects/guide /](http://advocacy.globalvoicesonline.org/projects/guide/)
5. **匿名在線和規避審查**。Tor的設計為增強在線活動的隱秘性，它也可以用來避開網絡過濾搜尋，你可以電腦上下載後使用它，或者把電腦連結USB來運行。 [http:// www.torproject.org/](http://www.torproject.org/)