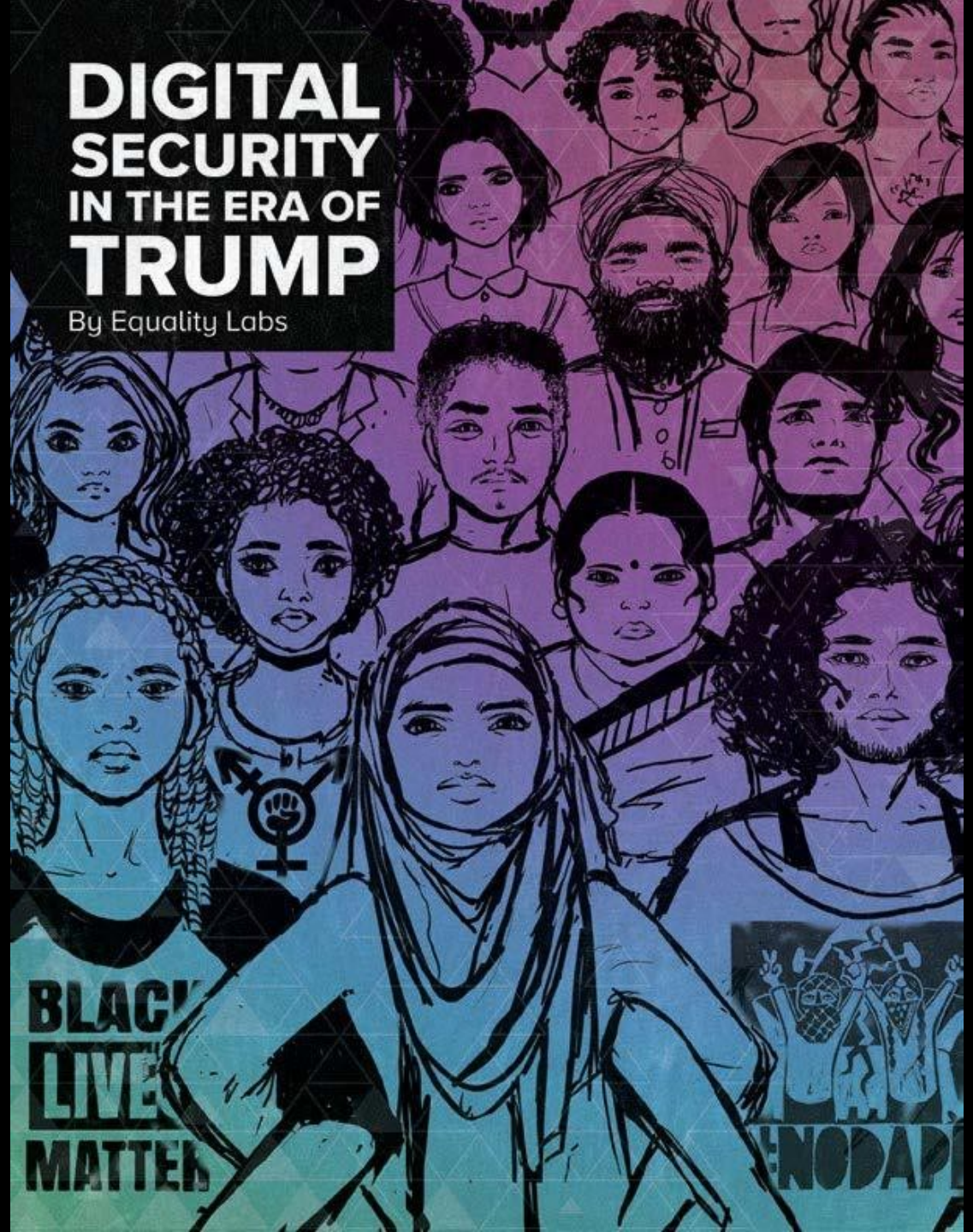
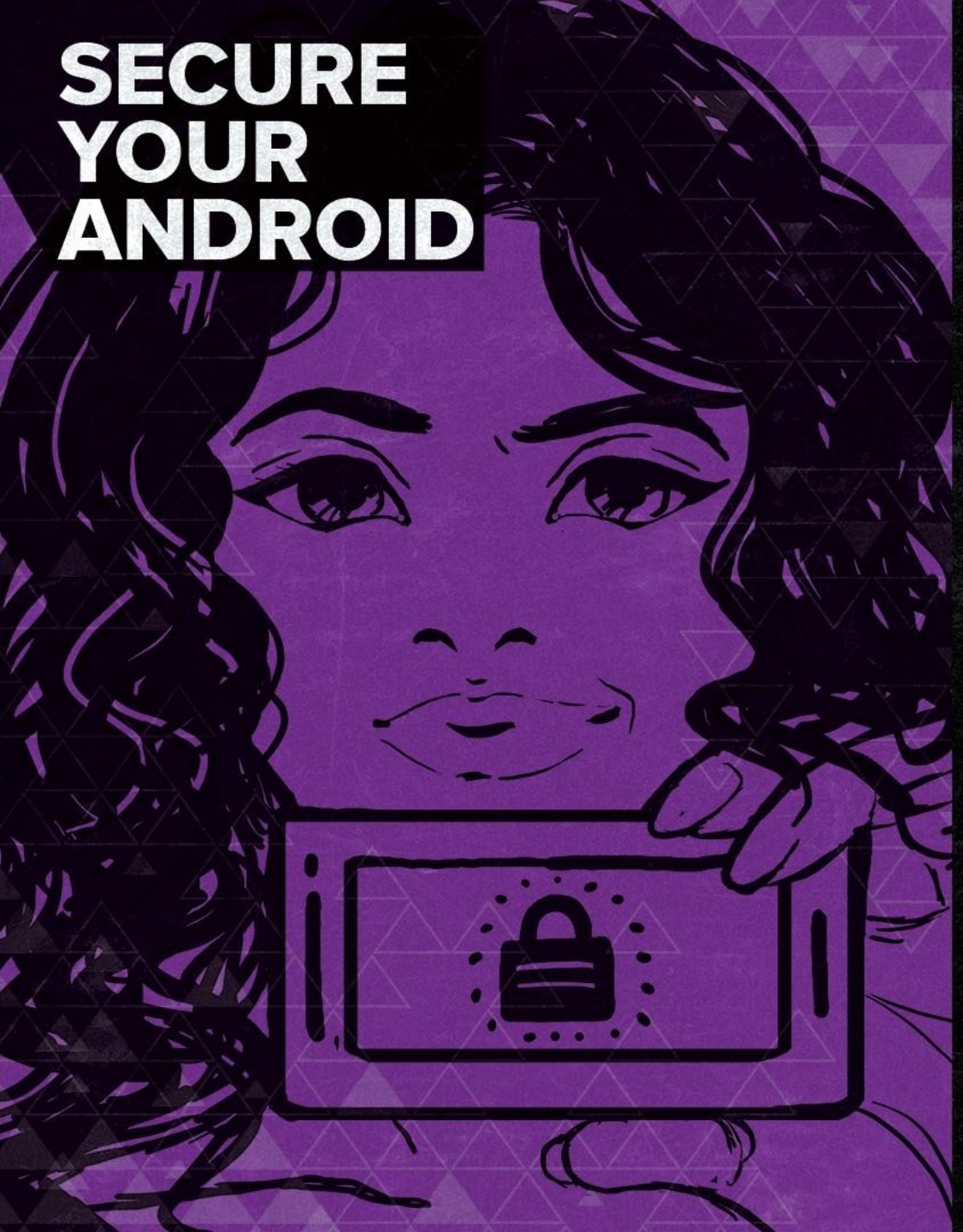

UNDOCUMENTED AND UNAFRAID
IMMIGRANTS ARE WELCO
END MASS Surveillence!
EQUALITY LABS

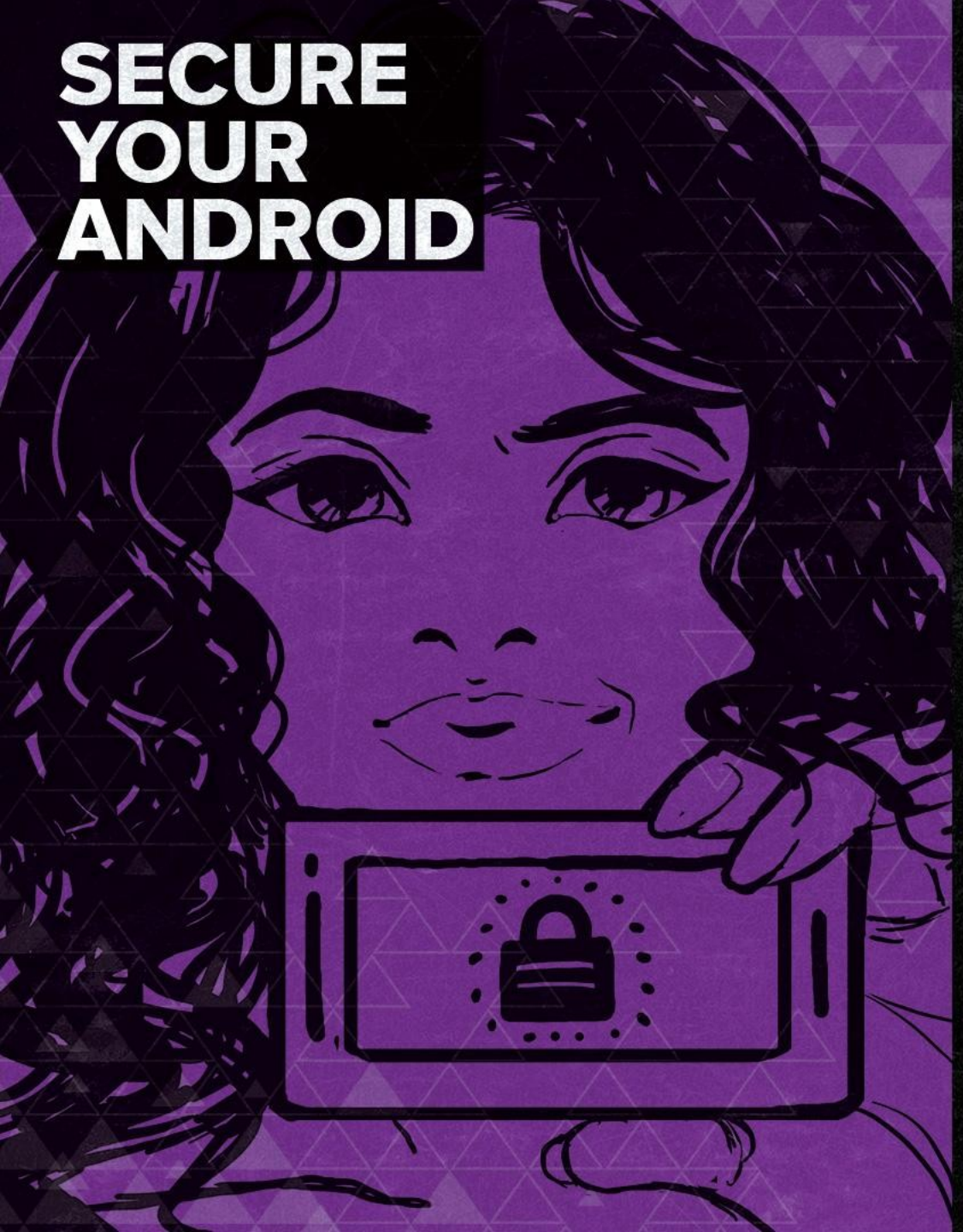

DIGITAL
SECURITY
IN THE ERA OF
TRUMP
By Equality Labs



✓ 使用 PIN 密碼，不要使用觸控指紋辨識。

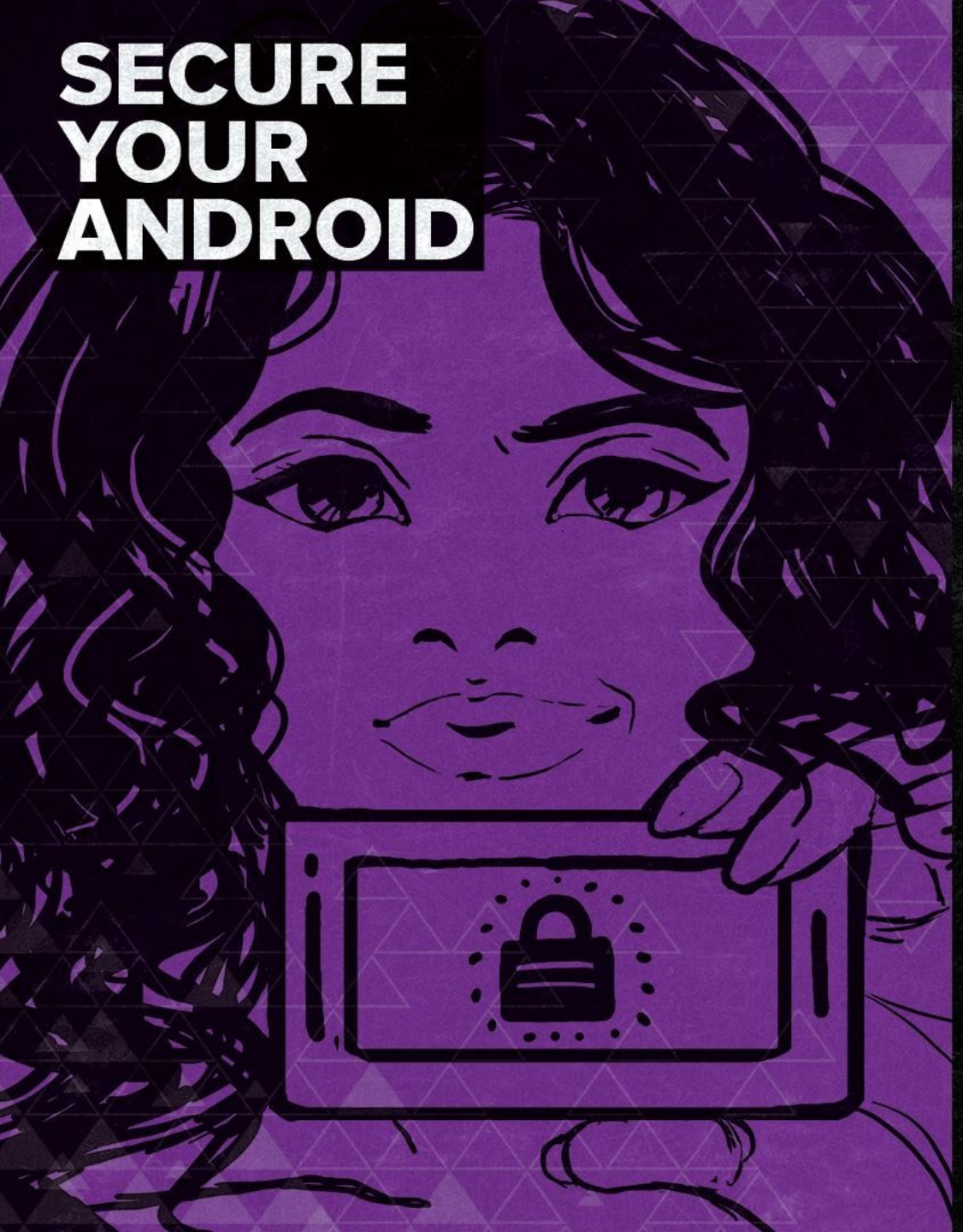
指紋辨識可以被破解，確保讓 PIN 夠複雜故最少有 8 個字元。這個部份的設定請到安卓手機下：

設定 **Settings** →
個人 **Personal** →
安全 **Security** →
螢幕上鎖 **Screen Lock** 進行。



✓ 加密並備份手機

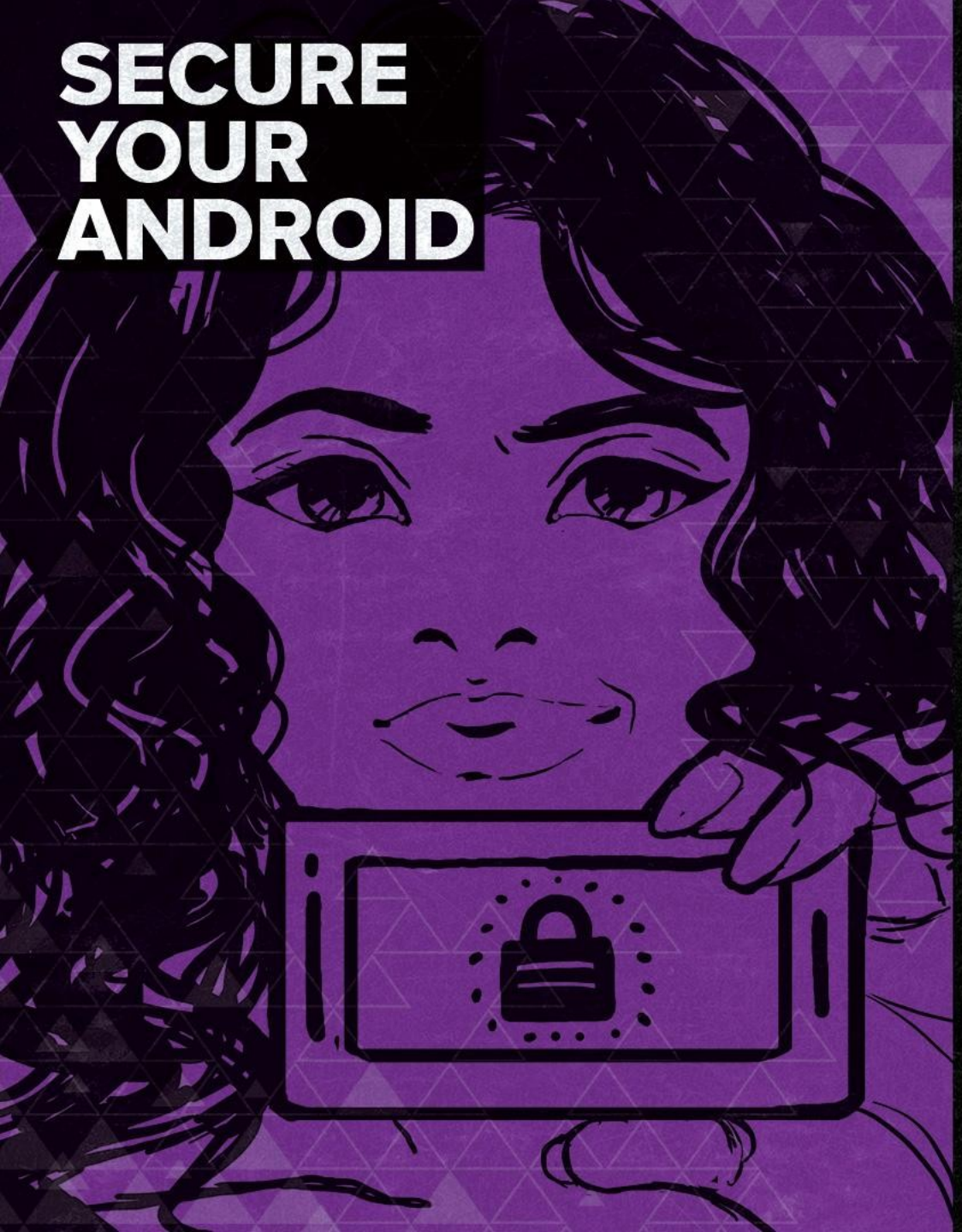
新版本的安卓自動提供此功能，若使用 Android 4.0 以上的版本，你的手機應已將加密功能開啟。 可在設定 **Settings** → 個人 **Personal** → 安全 **Security** → 加密 **Encryption** 檢查相關設定，如果還未加密請依照以下步驟為手機加密。 進行加密之前，先確認相關資料已作備份，手機電池有足夠電力或是接上電源線。



✓ 當手機不用時，將其設為螢幕自動上鎖

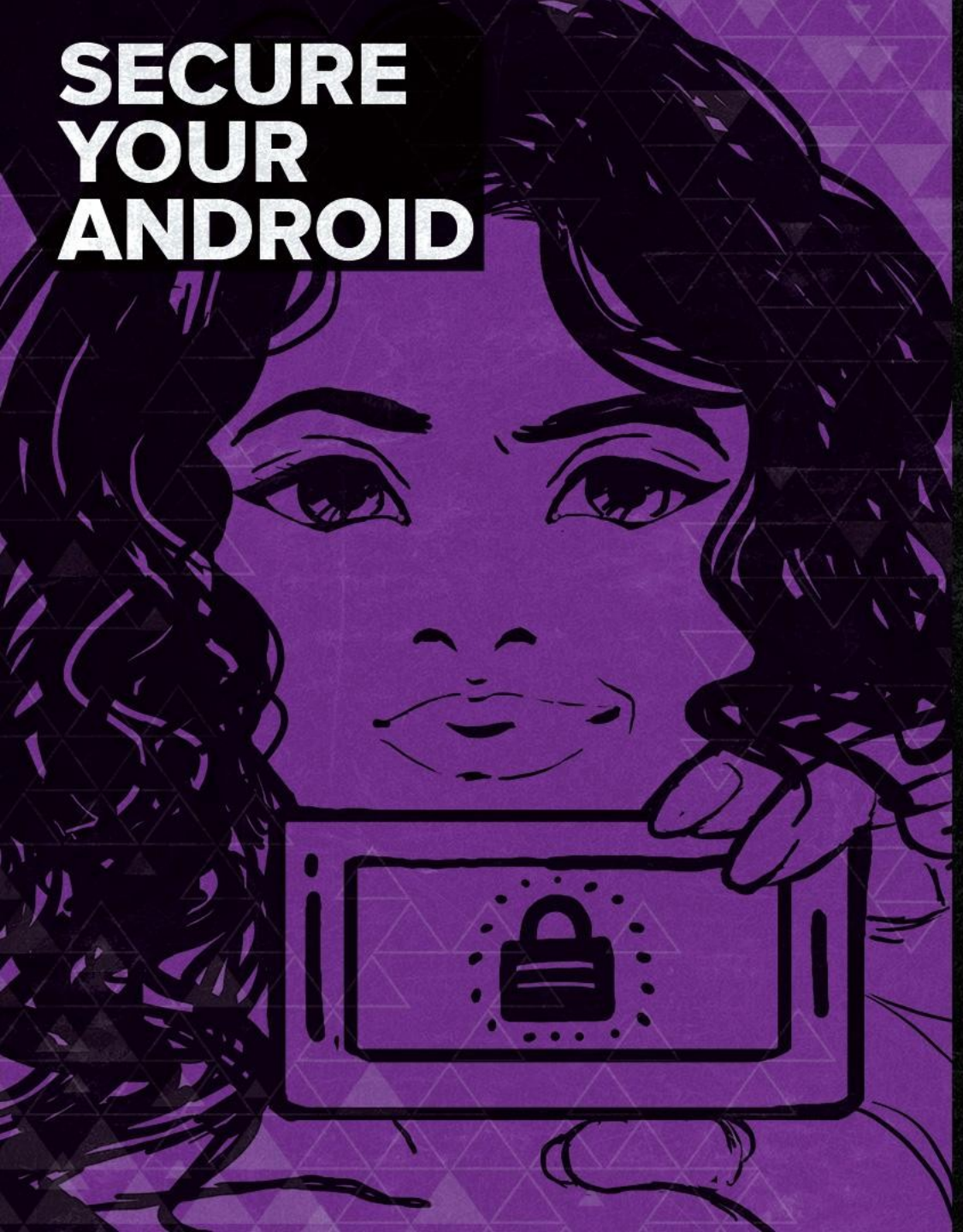
我們建議你挑選一個合適的時間間隔，一般大約是 30 秒到 1 分鐘之間如無動作，則讓手機會自行鎖上螢幕。

安卓手機此設定變更是在： 設定 **Settings** → 個人 **Personal** → 安全 **Security** → 螢幕上鎖 **Screen Lock**。



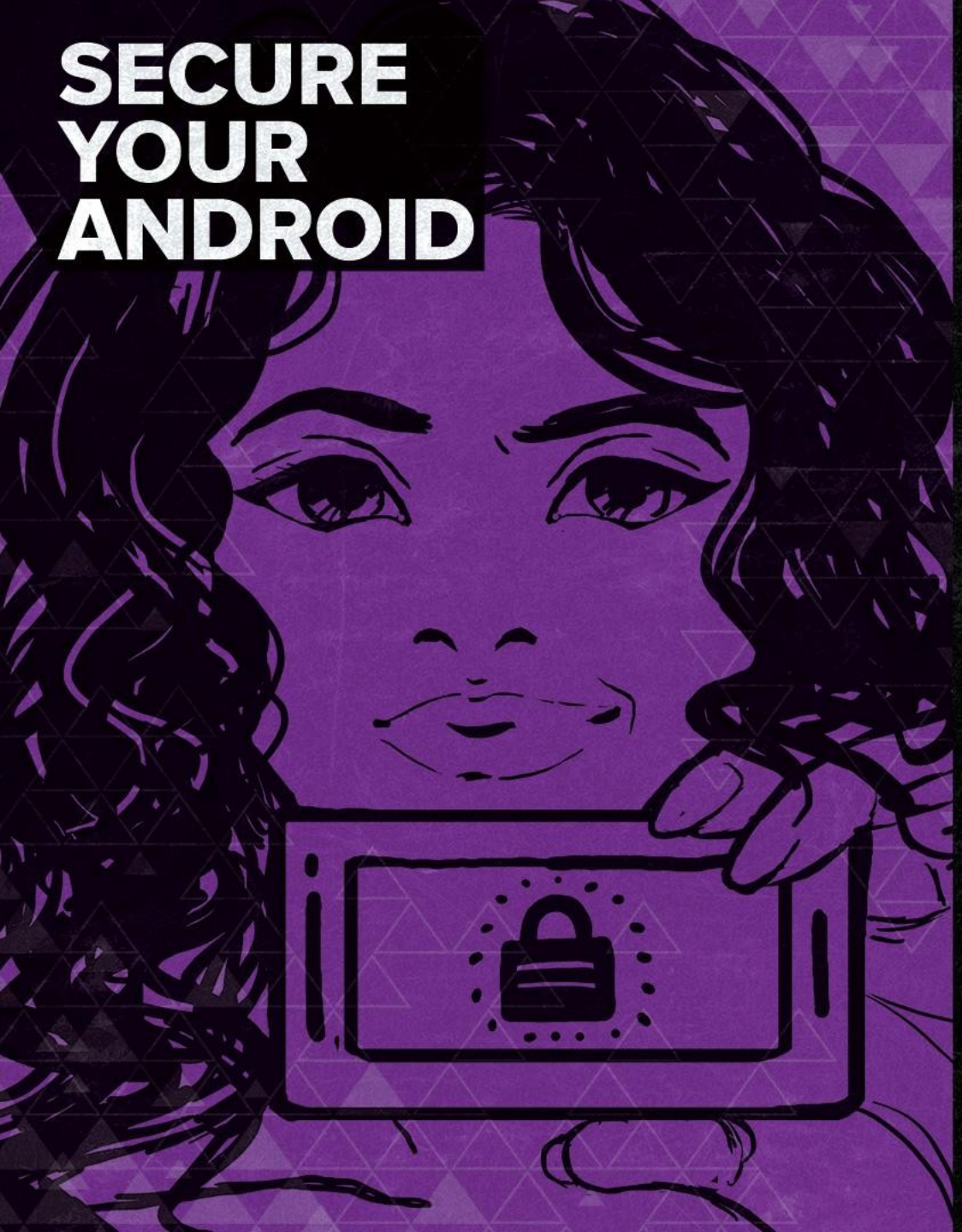
✓ 經常清理手機訊息串

手機的簡訊設定中可以找到選項來清除舊訊息。如果手機遭到沒收，你可能會被脅迫要打開它，而從手機簡訊記錄可能會曝露敏感資訊。



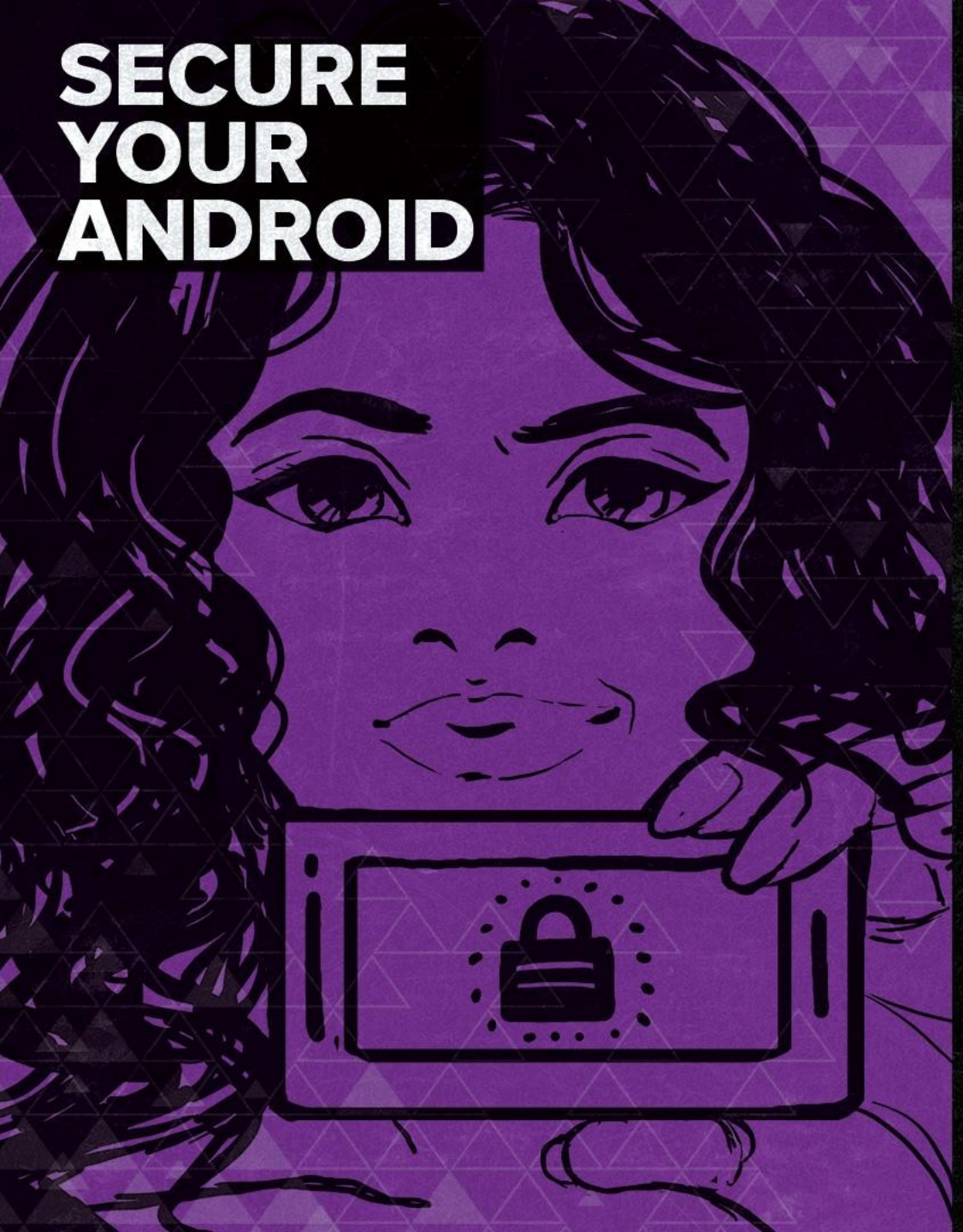
✓ 更新安卓手機系統與軟體

這類更新包括重要的安全漏洞修復。如果沒有更新系統，可能會讓你的手機處於脆弱的危險中。相關步驟請到 設定 **Settings** → 關於手機 **About Phone** → 更新 **Updates** → 檢查更新 **Check for updates.**



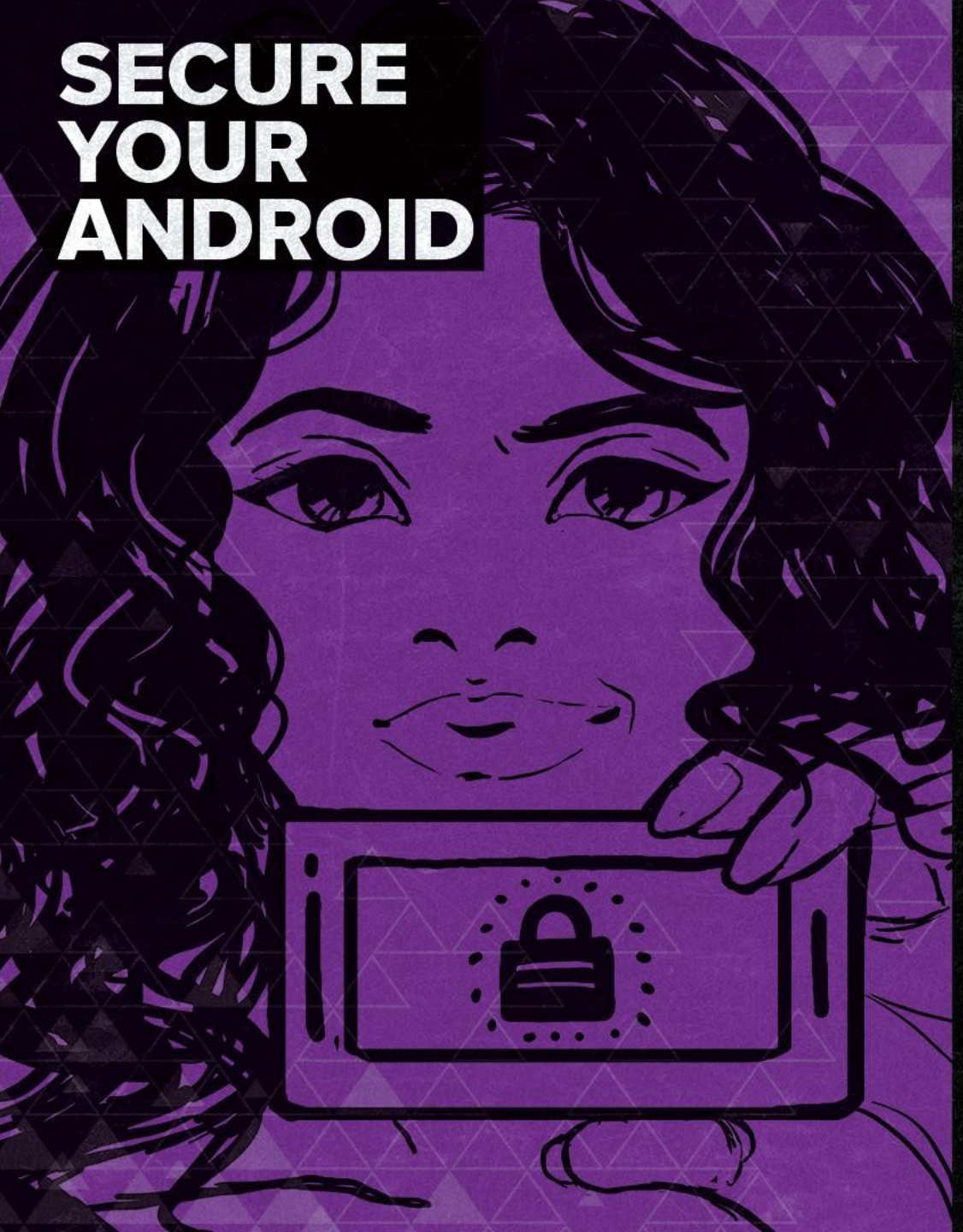
✓ 加入應用程式上鎖軟體

為了多一層防護， 我們推薦在安卓系統下可用 **Applock** ，在 Google Play 商店可找到這個軟體。



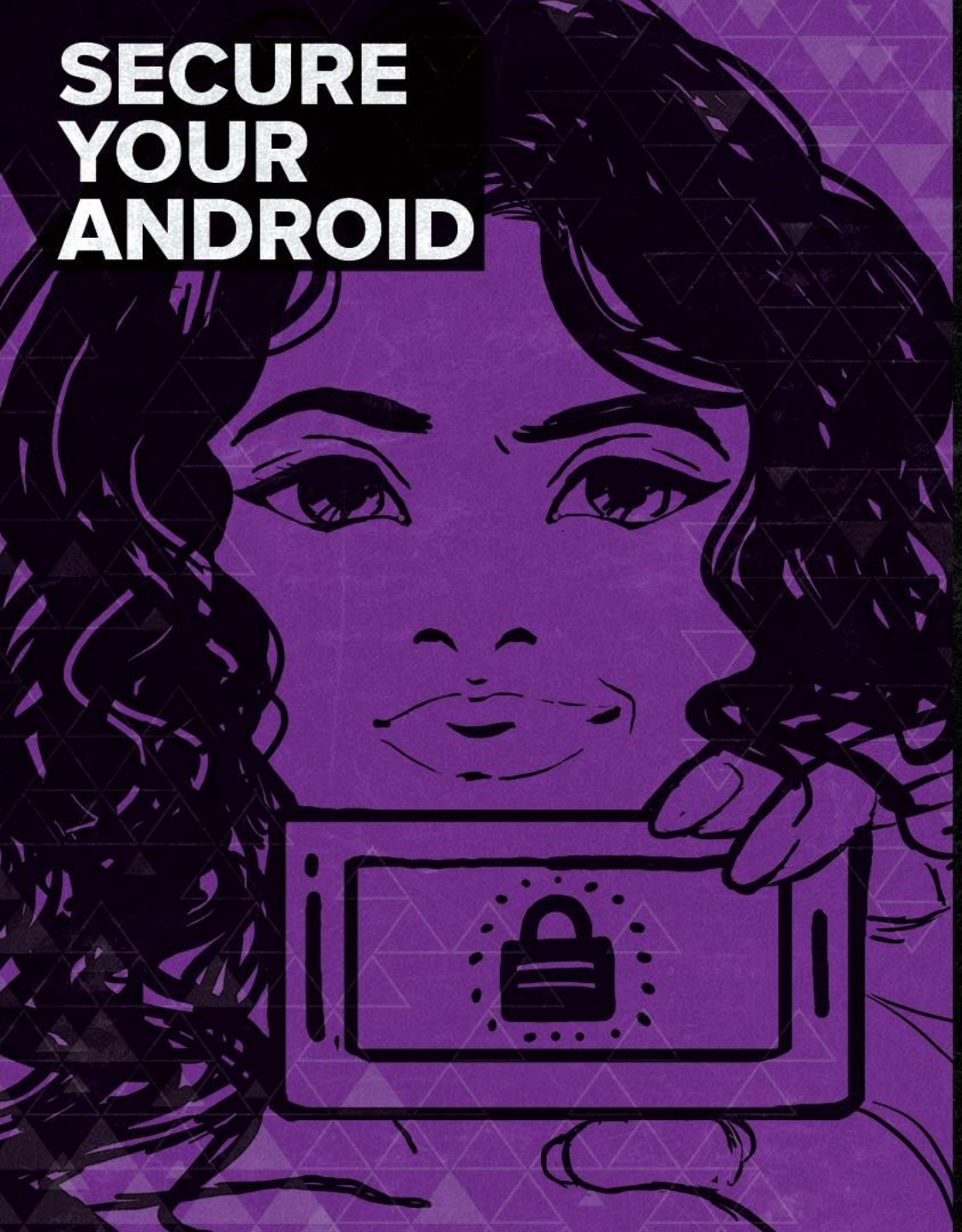
✓ 除非真有必要，否則請關閉地理位置功能

到設定 **Settings** → 個人 **Personal** → 地理位置 **Location** 關閉此定位功能。 這樣讓它不會在背景下默認啟動，降低所在位置被追踪的風險，也可節省電池減少個人資料在不知道的狀況下被應用程式或電信系統業者取得。然而，仍可能透過訊號基地台三角測量法來推測出手機持有者所在位置，故仍請小心留意。



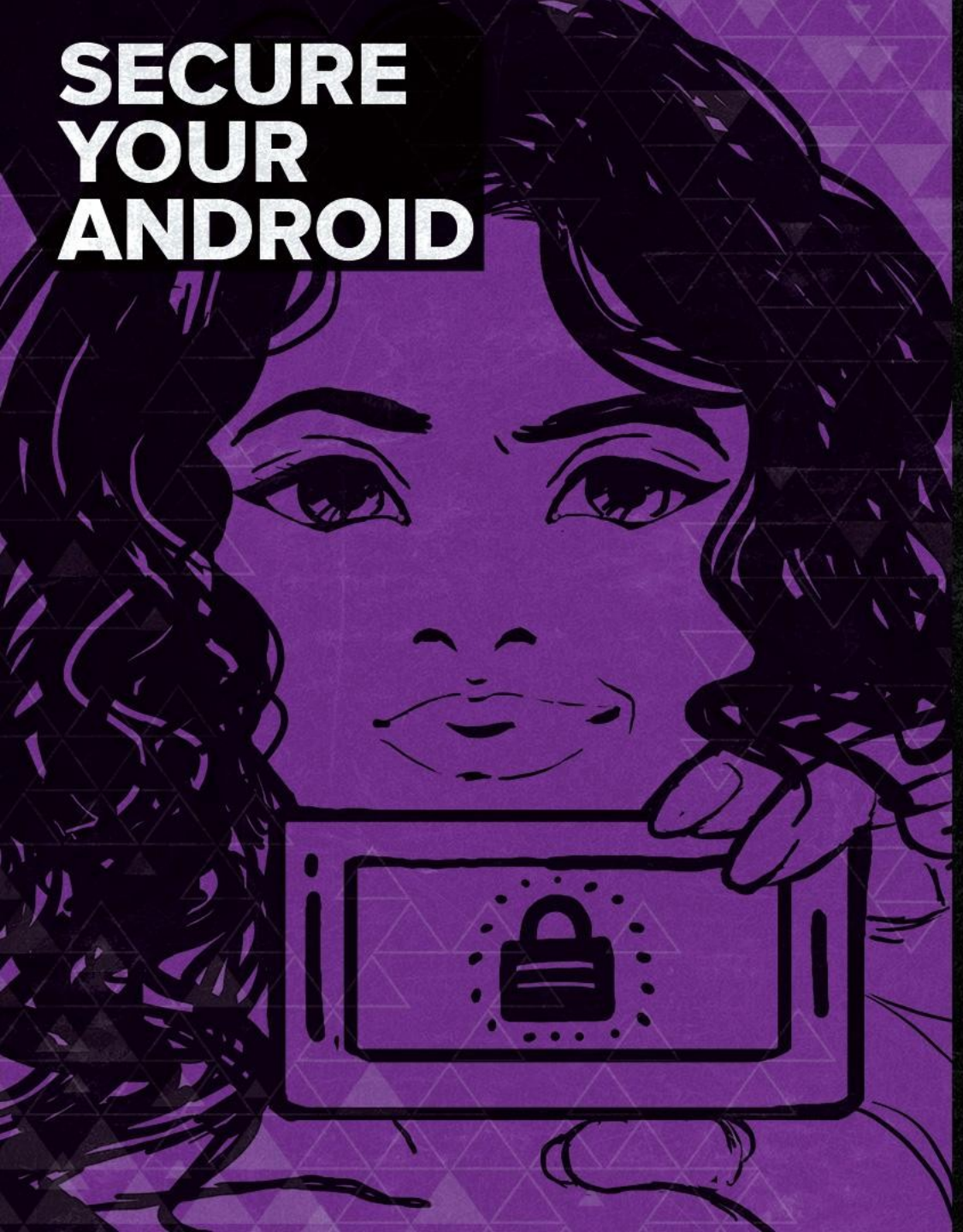
✓ 手機上安裝 VYPRVPN/ORBOT/ORFOX 等應用程式以保護連網

這些軟體可讓用戶匿名化網路流量資訊並躲開網路連線服務業者的過濾檢查。 Google Play 商店可找到這些軟體，進一步了解請到 https://www.goldenfrog.com/vyprvpn



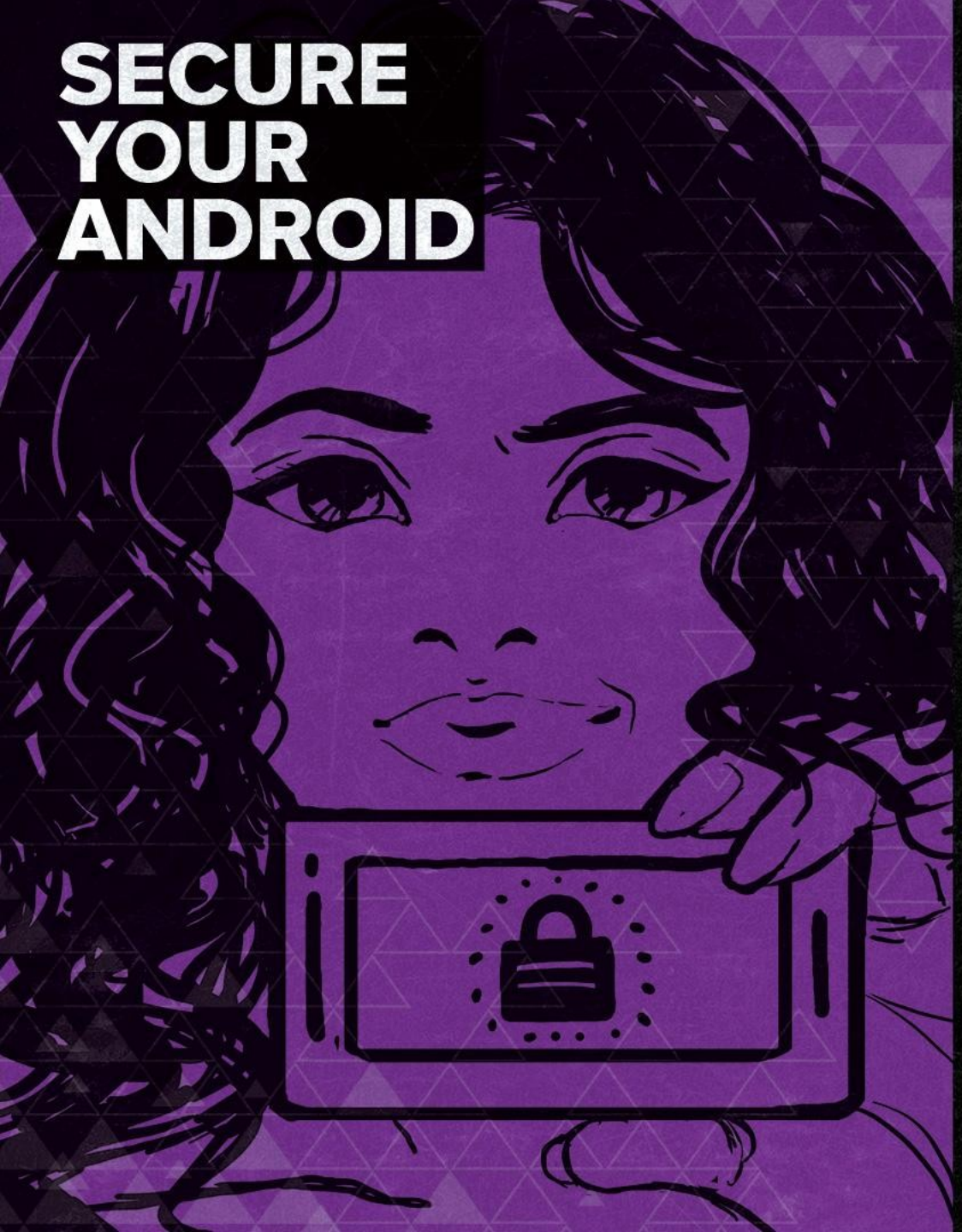
✓ 改用 DUCKDUCKGO 為上網瀏覽器與搜尋引擎

Duckduckgo 不會追踪用戶個人資料。使用者可以放心自己的瀏網資訊不會被作成私人企業或政府描繪記錄的個人樣貌圖譜。這個應用程式可以在 Google Play 商店下載。進一步了解請見：
https://gogoduck.com



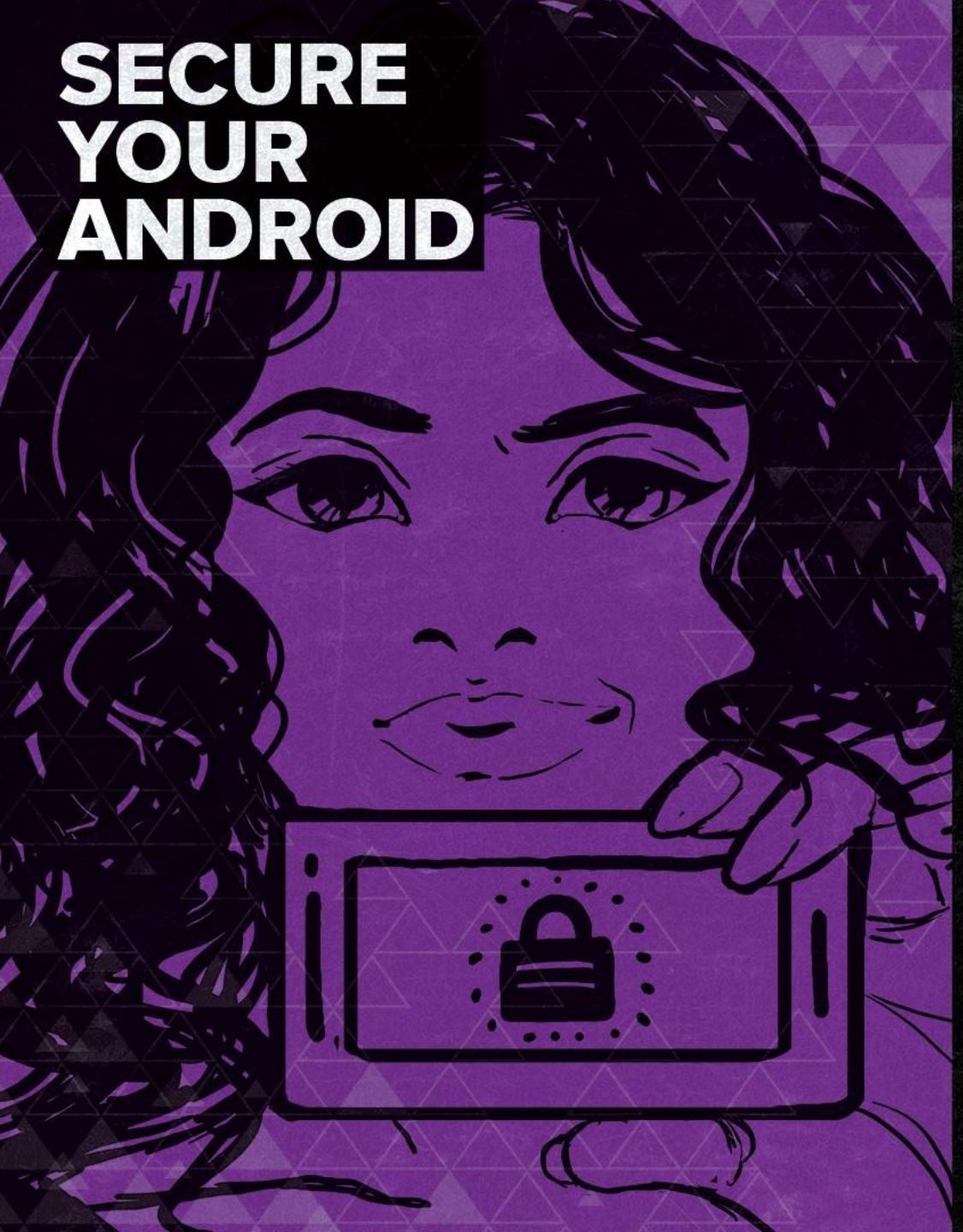
✓ 改用 TALKY

來取代 skype, google hangouts 等語音通話軟體。 **Talky 提供端點對端點加密**且適用於 android, iOS 及各種電腦平台。利用這個軟體，用戶只要輸入名稱並利用產生的網址連結來邀請通話者加入，即建立一個電話會議！ 網址請見 **https://talky.io/**



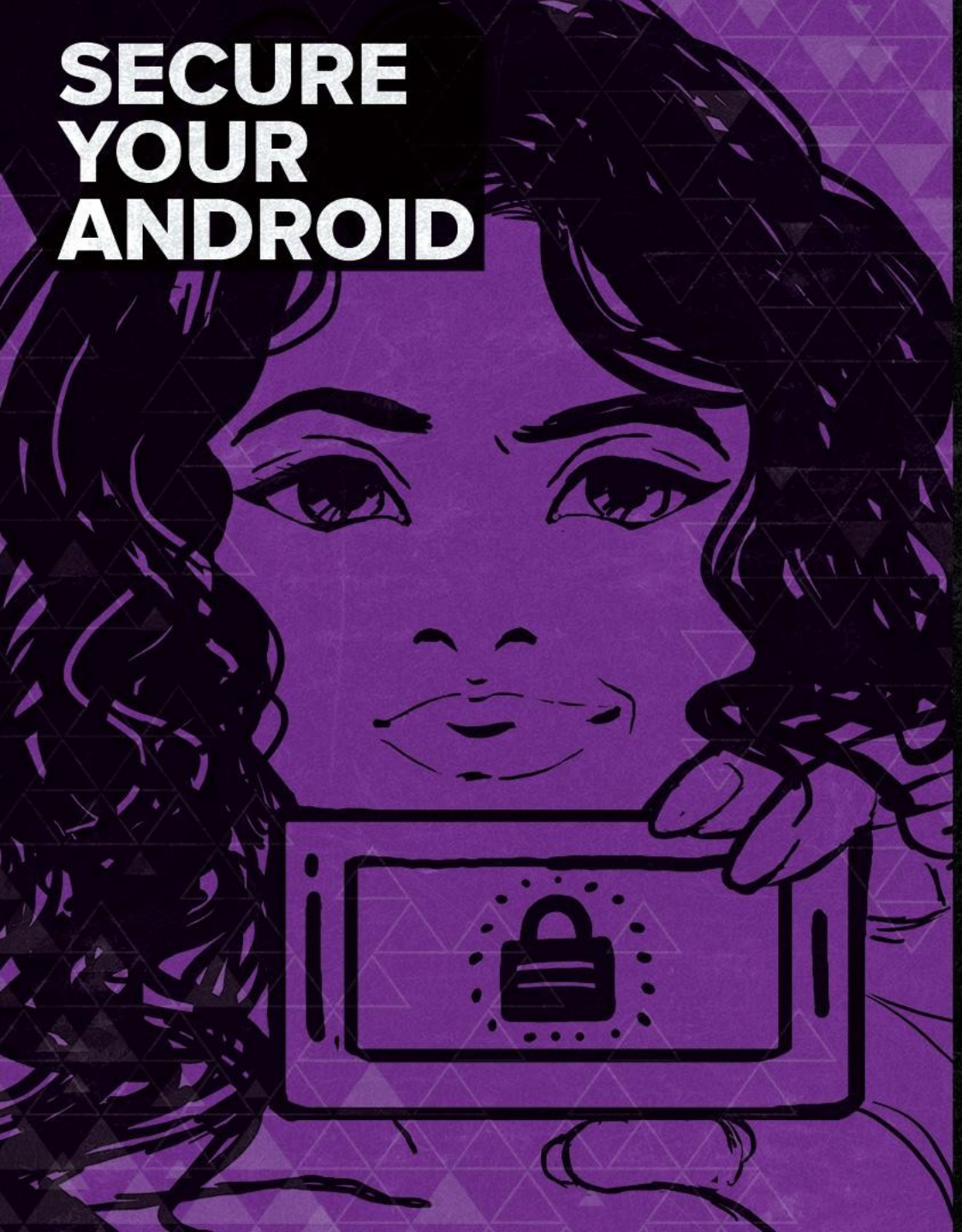
✓ 安卓手機請安裝反惡意

軟體掃描，我們推薦 **malwarebytes** 它可在 Google Play 商店找到。進一步了解請見 https://www.malwarebytes.com/



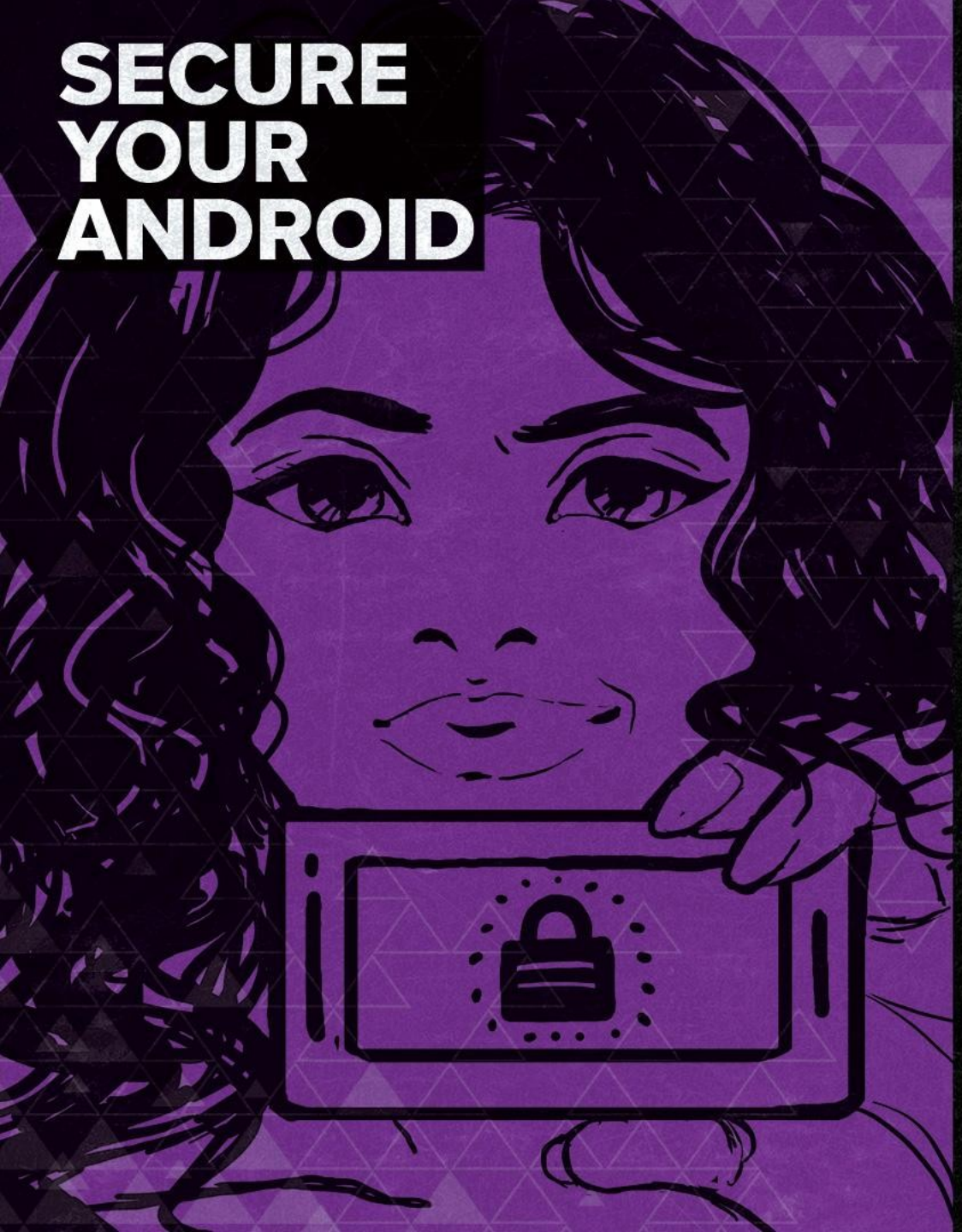
✓ 手機上安裝元數據洗除工具

這樣不至於在網上分享照片時洩漏了重要元數據，它包括地理位置等等訊息。 安卓系統下，這類優秀的應用程式如 **Exif Eraser** 可以抹除元數據。 它可以在 Google Play 商店找到。進一步了解請見 **http://www.exiferaser.com/**



✓ 使用 SIGNAL

把這個應用程式安裝在手機上與利用它的電腦 Chrome 瀏覽器外掛套件。在設定 Signal 時，請確認要查證核實聯絡人。它也具有消除訊息功能，以維持訊息討論串的清爽。一定要仔細核實聯絡人。



✓ 將手機放在無線訊號防護袋裏

在私人會議或是示威抗議場合下，這種袋子可以隔離電子訊號。

✓ 使用 PIN 密碼 不要用觸控指紋辨識。 確保讓 PIN 夠複雜至少有 8 個字元， iPhones 請到：**設定 Settings →** 指紋辨識 **& 密碼 Touch ID & Passcode** 進行變更。 在此設定視窗下檢查當手機上鎖時，哪些 iOS 應用仍可使用，請依照個人的面臨的危險程度來自行決定此取用權限。

✓ **除非真有必要，否則請關閉地理位置功能** 在 iPhones 手機下， 到 **設定 Settings → 隱私 Privacy** 下檢視各應用程式的位置設定權限。除非真有必要，否則關閉應用程式的地理位置功能，作法是在 iOS 底下： **設定 Settings → 隱私 Privacy → 地理位置 Location Services**。 此可讓它不會在背景下默認啟動，降低位置被追踪的風險，也可以節省電池以及減少個人資料在不知道的狀況下被應用程式或電信系統業者取得。然而仍可能透過訊號基地台三角測量法來推測出手機持有者的所在位置，故請小心留意。

此外在同一個選單底下， **Settings → Privacy → Location Services → System Services** 關閉依地理位置所送發的 Apple 廣告與服務建議。 最後在 **Settings → Privacy → Location Services → Product improvement** 關閉產品改善選項設定，包括問題偵測，週圍趨勢、路由狀況與流量等資訊。

✓ **加密和備份手機** iPhone 的 PIN 被激活時，此功能會自動進行。只要確保手機或電腦的備份不要上傳到 iCloud ，把備份檔存在本地電腦上即可。 同時記得，不要把密碼存到 iCloud 。

✓ **當手機不用時，將其設為螢幕上鎖狀態** 我們建議你挑選一個合適的時間間隔，一般大約是 30 秒到 1 分鐘之間如無動作，則讓手機會自行鎖上螢幕。 iPhone 手機此設定變更是在： **設定 Settings → 顯示與明亮 Display & Brightness → 螢幕自動上鎖 Auto-Lock**.

✓ **經常清理手機上的訊息串** 手機的簡訊設定中可以找到選項來清除舊訊息。如果手機遭到沒收，你可能會被脅迫要打開它，而從手機簡訊記錄可能會曝露敏感資訊。

✓ **維持手機系統 iOS 更新** 這些更新包含了重要的安全漏洞補救，用戶可在 手機的 **設定 Settings → 一般 General → 軟體更新 Software Update** 找到選項。

✓ **在手機上安裝 VYPRVPN 以保護連網** 這個軟體可讓用戶匿名化網路流量資訊並躲開網路連線服務業者的過濾檢查。軟體可在 app 商店下載或進一步了解請到 **https://www.goldenfrog.com/vyprvpn**

✓ **改用 DUCKDUCKGO 為上網瀏覽器與搜尋引擎**
Duckduckgo 不會追踪用戶個人資料。使用者可以放心自己的瀏網資訊不會被作成私人企業或政府描繪記錄的個人樣貌圖譜。這個應用程式可以在 app 商店下載。進一步了解請見：
https://duckduckgo.com

✓ **為手機照片安裝元數據洗除工具** 這樣才不至於在網上分享照片時，洩漏了重要元數據，包括地理位置等等訊息。 iOS 系統下，這類優秀的應用程式如 **PixlMet** ，它可以在 app 商店找到。進一步了解請見 **http://www.pixlmetphoto.com/**

✓ **下載 TALKY** 來取代 skype, google hangouts 等語音通話軟體。 **Talky 提供端點對端點加密**且適用於 android, iOS, 等各種電腦平台。利用這個軟體，用戶只要輸入名稱並以生成的網址連結來邀請通話者加入，即可簡單地建立一個電話會議！ 用戶可到 **https://talky.io/** 下載或是在 app 商店找到這個軟體。

✓ **使用 SIGNAL** 把這個應用程式安裝在手機上與加裝電腦 Chrome 瀏覽器外掛套件。在設定 Signal 時，請確認要查證核實聯絡人。它也具有消除訊息功能以維持訊息討論串的清爽。一定要仔細核實聯絡人

✓ **將手機放在無線訊號防護袋裏** ，在私人會議或是示威抗議場合下。 這種袋子可以隔離電子訊號。

✓ **建立高強度密碼** 密碼應要原創、複雜、不含個人資料且每三個月定期更改。 難破解的密碼使用了字母、數字、符號等混合，利用與個資無關的字眼，例如不要用生日，家人、朋友或寵物名字甚至地址等資訊。好的密碼設定方法，請參考 https://securityinabox.org/en/guide/passwords

✓ **建立用戶與管理員帳號** 為避免日常使用中電腦的最高管理者權限受到攻擊。在蘋果電腦上請到蘋果選單 **Apple Menu → 系統偏好 System Preferences → 使用者與帳號 Users and Accounts** 來做設定。 在 Windows 10 的電腦上，可從開始 **Start → 設定 Settings → 帳號 Accounts → 家人或其它人 Family & other people → 電腦新增其它人 Add someone else to this PC**.

✓ **電腦加密** 硬碟加密。 在 Macs 蘋果電腦上，加密的操作步驟為：到系統偏好 ystem preferences 下的安全面板 security panel，開啟 Filevault 即可。 **系統偏好 System Preferences → 安全與隱私 Security & Privacy → 完整磁碟加密 FileVault**

在 Windows 電腦上，可以先打開設定部份，檢查設備加密功能是否啟動。請到系統 **System → 關於 About** 面板下找到「設備加密」**“ Device encryption” 設定**。如果未能找到任何「設備加密」，表示你的電腦並未支援此功能。這種情況下，請使用 **VeraCrypt** ，它是一套免費的軟體可以用來加密任何設備磁碟。詳細使用請到 https://veracrypt.codeplex.com/

✓ **固定使用強壯的反惡意軟體工具** 差不多一週一次。推薦 用 **MalwareBytes** 並經常檢查它的更新。可到其官網取得下載 **https://www.malwarebytes.com/**

✓ **不要隨意開啟附件！** 大多數人因為這樣而遭駭。不信的話，問問美國民主黨吧！ 如果某人傳送給你在某個平台上的檔案，而這個檔案可以被 Google apps 開啟，那就先這樣處理。 這包括了 Word, Excel, PDF, 以及一些圖片檔案。因為 Google 有能力處理惡意軟體，但如果是自己的電腦可能無法發覺這些伏匿的惡意軟體。 如果你不想要把資料上傳給 Google ，那麼就先把檔案下載後，用自己的反惡意軟體工具來描掃檢查。 但一定要確認你防惡意軟體已更新。最後一個方法， 可以把檔案上傳到 **virustotal.com** 進行掃描，這網站包含多種防毒資源庫可作為防惡意軟體的另一種選擇。

✓ **定期更新作業系統** 在 Macs 蘋果電腦上，可到 **Apple Menu → App Store**. 在 Windows 10 電腦上，請到控制台面板下檢查設定自動更新是否開啟，若無可依下列步驟進行操作：

1. Windows 作業系統下開啟搜尋功能，輸入更新 update 以找到 Windows Update 選項。
2. 選擇變更設定
3. 如果還未選取，建議最好點選安裝自動更新

✓ **使用 SIGNAL.** 把這個應用程式安裝在手機上與加裝它的電腦 Chrome 瀏覽器外掛套件。在設定 Signal 時，請確認要查證核實聯絡人。它也具有消除訊息功能以維持訊息討論串的清爽。一定要仔細核實聯絡人

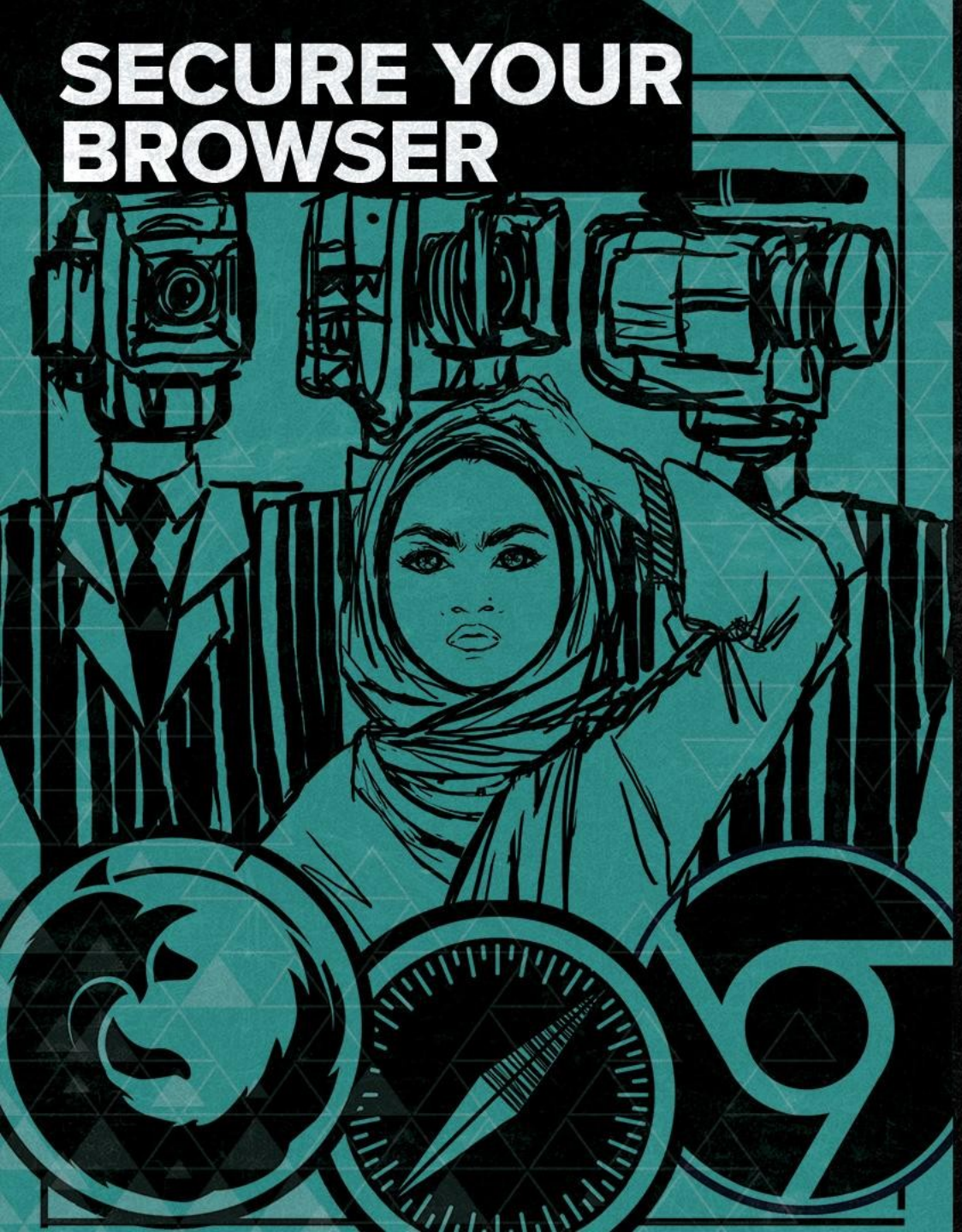
✓ **把 WHATSAPP, MESSENGER, 簡訊，E-MAIL, 手機皆視為不安全．** 如果必須使用 Whatsapp ，請查證聯絡人確保對方也安裝了最新版的 Whatsapp 這樣訊息串是經過端點對端點的加密處理。不幸的是， Whatsapp/Messenger 這兩個軟體是臉書所持有，它們的隱私權政策令人質疑，如果你的個人資料是存放在臉書伺服器上，不要天真地信任他們會保護你的資料安全。

✓ **如要使用電子郵件，請試著習慣利用 GPG 加密。** mac 蘋果電腦請在 **https://gpgtools.org/** 取得這個軟體；Windows 電腦在 **https://www.gpg4win.org/** 下載

✓ **更換電子郵件群組與專案管理管理軟體** 例如 **Spider oak** 開發的 **Semaphor** 搭配 slack。它具有端點對端點加密且皆支援網頁版或桌面客戶端軟體程式。進一步了解，請見： **https://spideroak.com/solutions/semaphor**

✓ **下載 TALKY 應用程式或是在電腦的瀏覽器上安裝 TALKY 延申元件** 用來取代 skype, google hangouts 等語音通話軟體。 **Talky 提供端點對端點加密**且適用於 android, iOS, 等各種電腦平台。利用這個軟體，用戶只要輸入名稱並用生成的網址連結來邀請通話者，即可簡單地建立一個電話會議！ 網址請見
https://talky.io/

✓ **若需要取代 GOODLE DOCS 的工具** 試試 **https://pad.riseup.net/** 來作短期的文件協作工具。 這個線上文字編寫軟體不會儲存用戶 IP 位置且本身在 30 天如果沒被使用就會自動刪除。你也可以在開源平台 **Sandstorm** 上找到其它替代 Google Docs 的工具。這個平台上有許多開源的應用程式，但可能要花一點時間來習慣其操作，也許幫助你擺脫 google apps 依賴的重要一步。更進一步了解請移至官網
https://Sandstorm.io



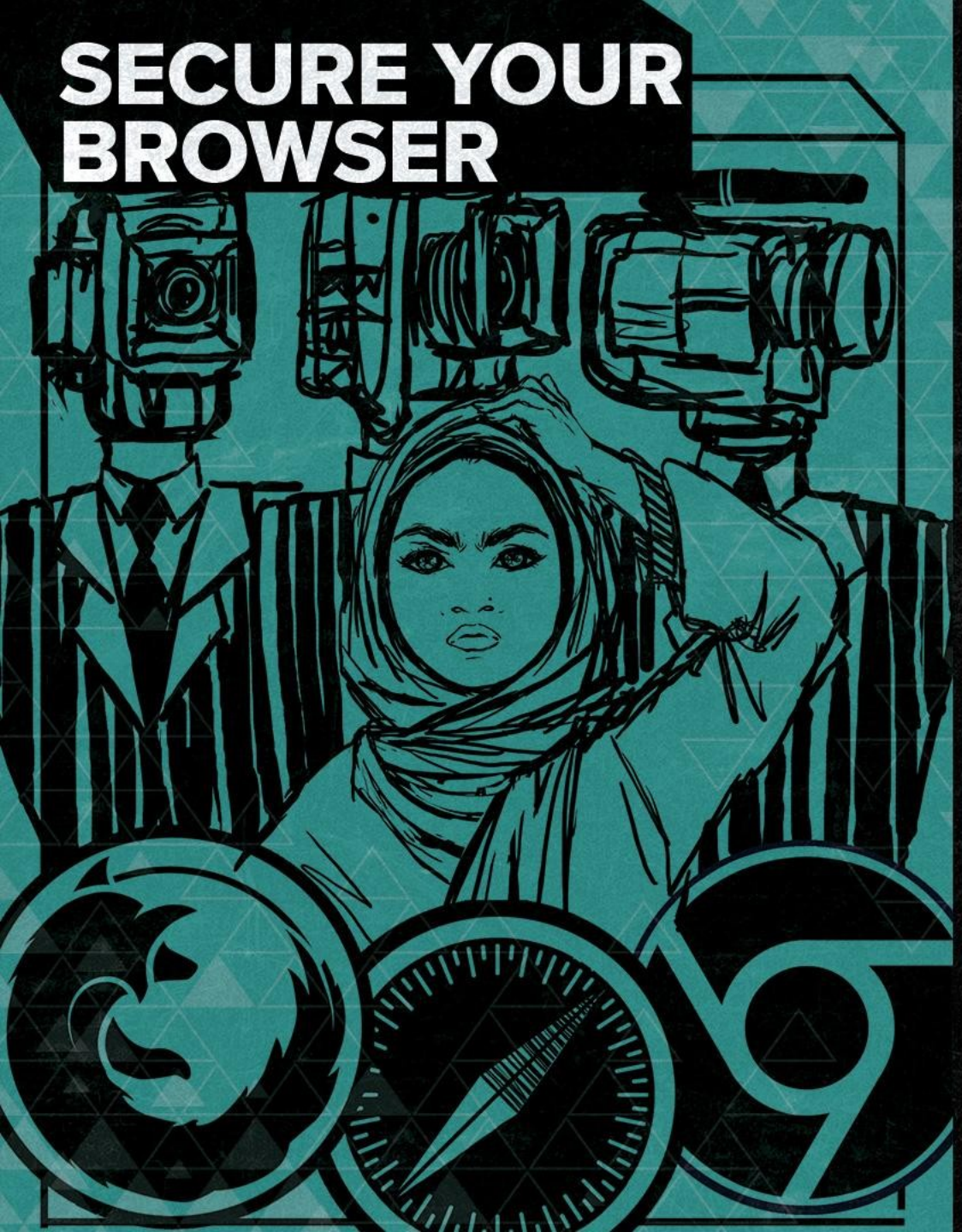
✓ 安裝 HTTPS EVERYWHERE 與 PRIVACY BADGER 瀏覽器延伸套件 **https://www.eff.org/https everywhere** **https://www.eff.org/privacybadger**. 這些延伸套件對瀏覽器是重要的功能加強，它們可幫助確保用戶訪問的是網站的安全連線版本，並且用戶可自行控制網站的監測使用狀況。 .

✓ 當使用別人的電腦時，請在 Chrome 啟用匿名無痕模式 INCOGNITO MODE 或是 FIREFOX 私密瀏覽 在瀏覽器下開啟新視窗，讓你在瀏覽網路時可以私密訪問而不會留下訪問過哪些網站的記錄。

但仍要記住 不管是 **匿名無痕**或是**私密瀏覽**模式都無法阻止其它方想知道你的上網記錄，包括你使用的 ISP 以及訪問過的網站本身。

此外，即便關閉瀏覽器分頁，所有下載請存在電腦上下載資料夾。否則任何使用這台電腦的人都可以看到並打開這些檔案。

機敏地利用這些工具， 進一步了解 Chrome **匿名無痕模式 incognito mode** ，請到 **support.google.com/chrome/answer/95464** / 或是 Firefox 私密瀏覽 **https://blog.mozilla.org/blog/2015/11/03/firefox-now-offers-a-more-private-browsing-experience/**



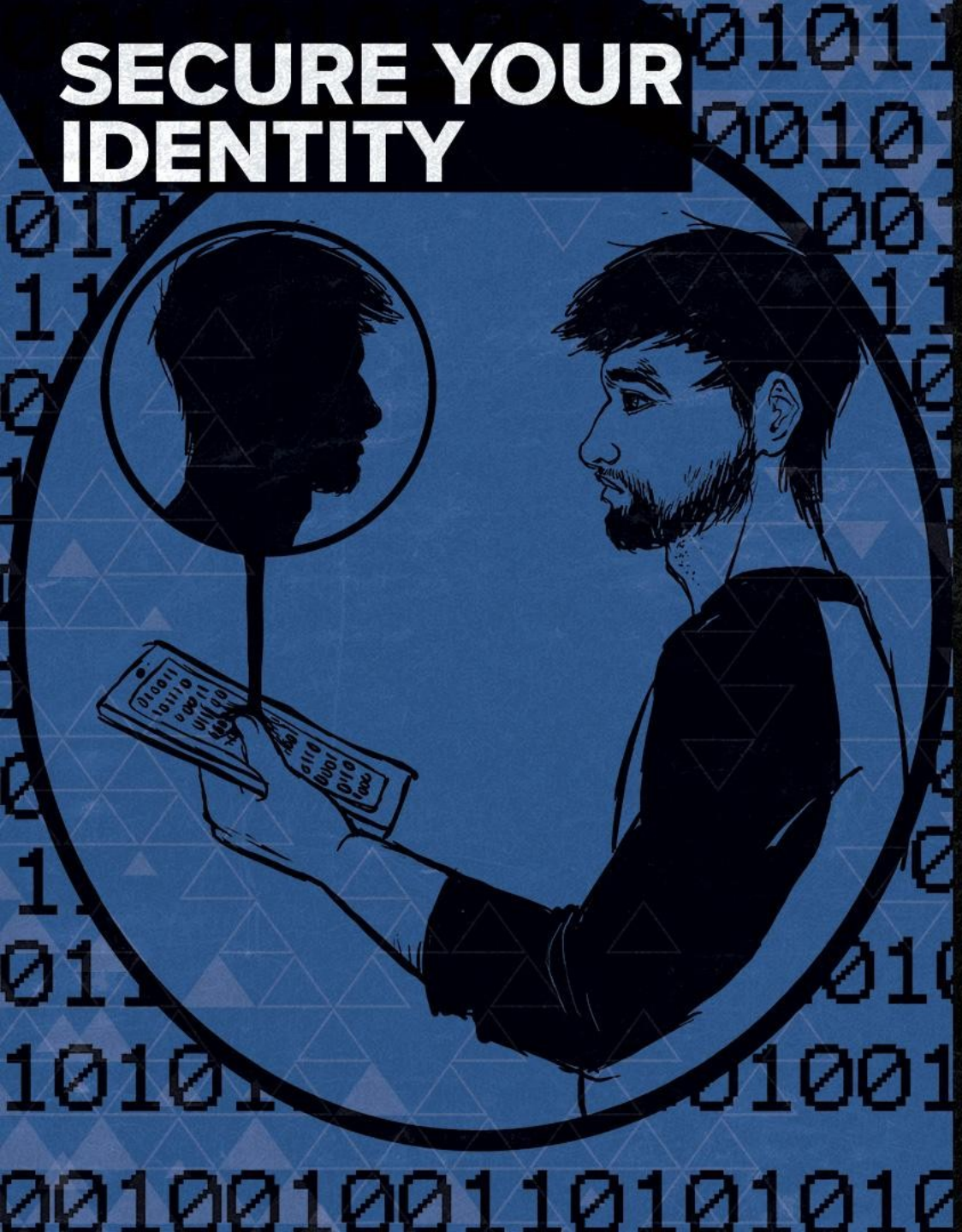
✓ **改用 DUCKDUCKGO** Duckduckgo 不會追踪用戶個人資料。使用者可以放心自己的瀏網資訊不會被作成私人企業或政府描繪記錄的個人樣貌圖譜。 進一步了解請見： https://duckduckgo.com

✓ **連上互聯網時，請全程使用虛擬私人網路（VPN）** 這裏我們推薦 Golden Frog's VyprVpn 。用戶可在此處找到相關資訊 i https://www.goldenfrong/vyprvpn

✓ **當不使用 VPN 時，請用 TOR 瀏覽器** 不使用 VPN ，可用 Tor 瀏覽器來躲開網路審查與進行匿名瀏網。記得要定期更新 Tor 瀏覽器。 https://www.torproject.org/projects/torbrowser

✓ **若需要安全地分享檔案，請採用 ONION SHARE.** 需要者可在此處下載：**https://onionshare.org/** 其相關介紹文件在此： https://github.com/micahflee/onionshare/blob/master/README.md

SECURE YOUR IDENTITY

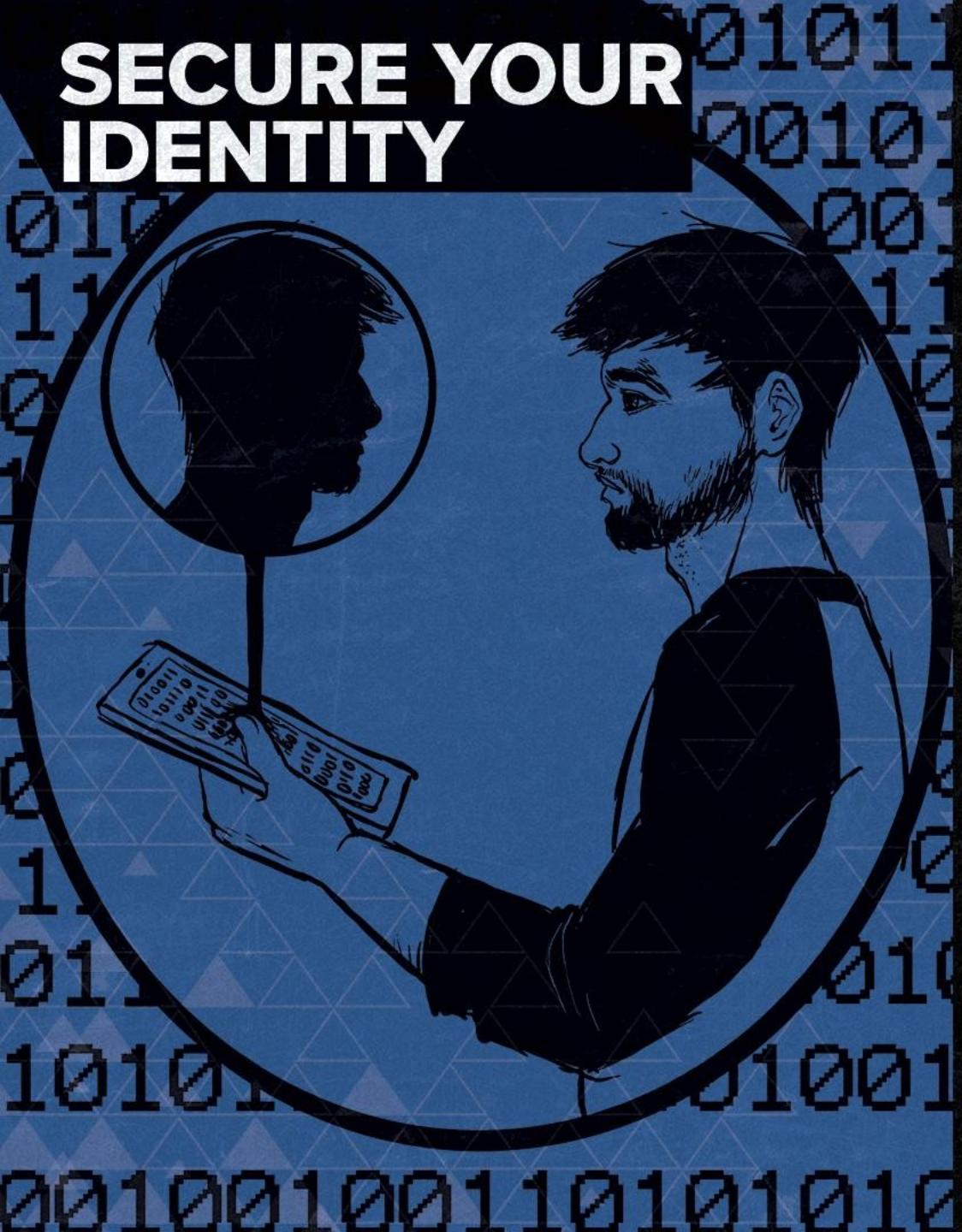


✓ **建立難破解的密碼** 使用密碼管理工具來為每一個帳號生成密碼。定期更換密碼也很重要，最好約每三個月換一次。我們推薦 **keepassX** https://www.keepassx.org/downloads, **1password** https://1password.com/ 與 **lastpass** at www.lastpass.com

✓ **分隔使用的電子郵件與 FACEBOOK, TWITTER, INSTAGRAM, SNAPCHAT 等社交帳號．** 為家庭、個人或政治公眾等不同身份維持分別的帳號。 對於某個身份可能被互相污染的情況要特別小心。確認採用不同的電子郵件或一次性手機來設定帳號。需要協助來建立多個帳號嗎？可利用 郵件服務如 **riseup.net** 以及 **burner app** 它們可以用來協助建立有所區別的不同身份。

✓ **啟用 2- 要素認證授權（2FA）** 在所有帳號底下。 G-mail, Facebook, Twitter 等服務皆有提供 2FA 功能。 下面這個網站有進一步說明，教導如何在各種網路服務下啟用此功能。 https://www.turnon2fa.com/tutorials/

✓ **了解 GOOGLE 知道自己哪些個人資料：** https://myactivity.google.com

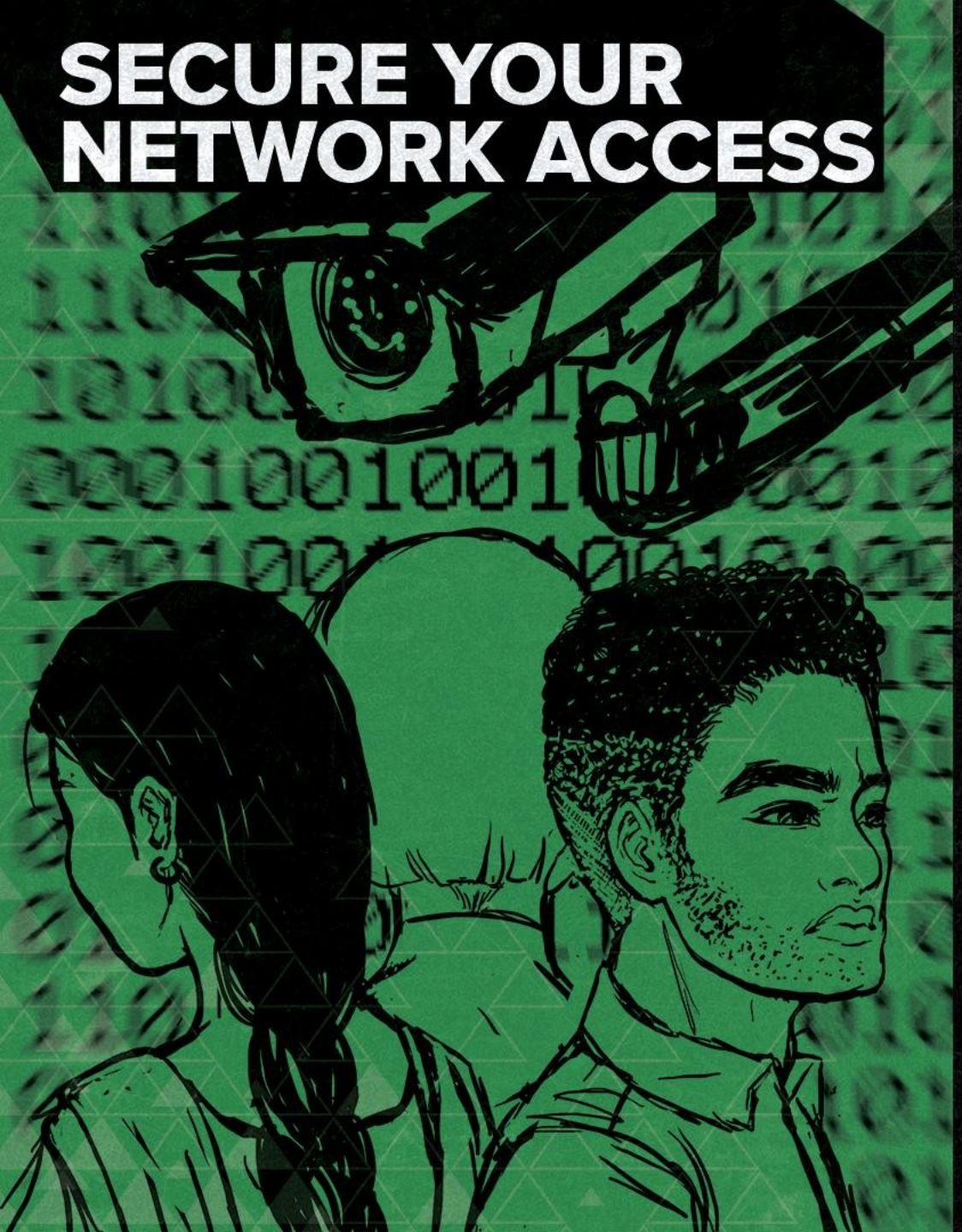


✓ **檢查自己是否成了駭侵活動的受害者** 請到 **https://haveibeenpwned.com** 輸入自己的電子郵件帳號。然後可以查到自己這個電郵與密碼是否已遭到哪一個資料外洩事件的受害帳戶。如果真查到自己某個服務帳密已外漏，請立即更改相關密碼以阻上傷害擴大。

✓ **了解網路惡棍可以掌握你的哪些個人資料** 一旦你知道自己有哪些個人資料流傳在互聯網上，你就可以開始聯絡這些資料代理者，要求移除你的個資。 雖然很難讓這些內容都可以移除，但這些一小步努力都能成為堅實的自我防衛，尤其當遇上網路惡棍成了被攻擊的目標時。

檢查個資外洩的相關網站：
Spokeo (要求移除的方法 : http://www.spokeo.com/opt_out/new)
Anywho.com (要求移除 : http://www.anywho.com/help/privacy)
Intelius (要求移除 : **https://www.intelius.com/optout.php**)
Whitepages (要求移除 : https://support.whitepages.com/hc/en-us/articles/203263794-Remove-my-listing-from-Whitepages-)

欲取得更詳盡的 Trollbusters 的資料代理商清單來檢查自己的個資情況， 可查詢此列表 https://yoursosteam.wordpress.com/2015/08/30/remove-your-mailing-address-from-data-broker-sites/



確保網路連線存取可以安全瀏覽網路很重要，因為網路連線服務供應商 (ISP) 常會進行網路監控。如果未使用安全網路連線軟體，不僅是揭露了自己的地點位置和網路瀏覽閱讀內容，ISP 業者也可以用來過濾、監視甚至屏蔽某些網站。安全的網路連線軟體考量了這些情況，並提供各種方法來保護網路連線的安全。把它想像成是保險套，當電腦連結上網際網路時，可用來防衛與匿名電腦身份。

✓ **利用虛擬私人網路（VPN）**來連結互聯網。我們推薦的優質 VPN 是 Golden Frogs VYPR VPN.
https://www.goldenfrong/vyprvpn

✓ **使用 TOR 瀏覽器．**當不用 VPN 時，請使用 **Tor 瀏覽器**來躲開網路審查和匿名瀏網。記得要定期更新 **Tor 瀏覽器**。下載請到： **https://www.torproject.org**

✓ **使用 TAILS.** Tails 是一個自生作業系統，其最主要目的在於維護用戶隱私和匿名安全。 它是一套設計透過 DVD, USB 隨身碟或 SD 卡來開機使用的完整作業系統，可完全獨立於電腦本身預載的原作業系統。 利用它，不管到哪裏都可以隨時利用某台電腦，匿名地上網和躲避網路審查，而不會留下被追踪的記錄，除非使用者刻意這麼作。進一步了解，請到
https://tails.boum.org/