SEC 教材

教材介紹

SEC (Security Education Companion) 為電子前哨基金會為資安教育者設計的教材，包含教學方法建議、實作活動、問答集等，共有 VPN、密碼安全、雙重驗證、網路安全、釣魚、即時通訊安全和威脅建模（風險評估）等主題。

電子前哨基金會（Electronic Frontier Foundation，EFF）是一個國際知名的非營利組織，他們進行的工作是捍衛網際網路上的公民自由，包含隱私、安全、言論自由和創新等等，並致力於使公眾更了解資訊科技，及監督侵犯個人自由的法律和執法機構。

根據 EFF 的創用 CC 授權，本計劃自 https://sec.eff.org/ 取得教材資源，並進行翻譯重製 SEC 中文教材。

東亞民主論壇－強化公民社會組織資訊安全計畫

本計劃希望蒐集國內外的資安教材，以深入淺出的方式編排，並輔以視覺化的呈現，使專業知識得以轉譯為公民團體能理解的敘述方式，並根據公民團體的需求規劃教材，內容包含資安工具介紹、基本防護觀念、最新的資安威脅趨勢等。

開放文化基金會

開放文化基金會（Open Culture Foundation，OCF）是由臺灣各大開源社群夥伴共同建立的法人組織。秉持相信開放的力量、社群協作的精神，致力推動臺灣開放文化，並持續與臺灣許多公民科技、開源技術社群合作，提供專業行政與專案協助。OCF 實際進行業務包括四大類：支援臺灣開放社群、與其他組織合作、提供開源社群顧問諮詢、促進臺灣開源社群的國際交流。

CSCS 社群

為了促進開源社群及 NGO 團體之間的交流，開放文化基金會與華人民主書院、台灣駭客協會、台灣人權促進會共四個組織共同開啟 CSCS 專案：Civil Society Cyber Shield，希望公民團體及社會運動組織者能夠接觸最新的資安工具、對抗資安威脅，在安全的線上環境中推動社會議題。

翻譯／校對／編輯團隊

Aiya

Chucklee

Claire

Kaichun

Sophia

Wayne

整體編制

本教材最後更新日期為 2020 年 7 月，教材內容可能隨科技資訊更新而有誤，希望能透過開源，不斷編修、維護這份教材。

TAIWAN FOUNDATION for DEMOCRACY 財團法人臺灣民主基金會

開放文化基金會 Open Culture Foundation

Civil Society Cyber Shield

目錄

講義與教材

1. 威脅建模活動講義

我們為威脅建模（風險評估）編寫了兩份雙面的練習講義（中文版）。我們建議在威脅建模工作坊當中發下這些講義，讓學員能在相應的情境中學習，有利於了解整體架構。講師可以將這份講義當作學員的個人習作，然後讓每位學員分享如何完成的。

經過資安工作坊的學員測試、新手教師的回饋，以及資安專家的建議，我們仍在持續改進這份講義。

如何使用這份講義：

講師應簡介威脅建模的基本觀念，如名詞解釋（何謂攻擊者、風險、資產、威脅，以及攻擊者的能力等）和威脅建模的五大問題。接著，講師可以用珠寶店老闆作為示範，帶學員演練一次；也可以先讓學員先自行練習，幾分鐘之後再分享他們寫了些什麼。對於五大問題，他們分別回答了什麼？一間珠寶店要保護的資產可能有哪些？等等。

如果珠寶店的例子對於你群眾的不太合適的話，可以考慮改編這份講義（你可以用簡報軟體編輯）。

如果你要改編，請思考：什麼樣的例子會與你的學員們更有關聯？怎樣的威脅模型更貼近他們？例如，一個水果攤商會需要保護什麼？一個有五歲小孩的媽媽會擔心什麼？如果有人想保護他的腳踏車應該關心些什麼？

然後，讓學員在背面的圖表作標記，圖表上的縱軸是風險性，橫軸是威脅性。我們已經預先放上了一些較荒唐的，和一些較貼近現實的例子。有哪些學員們曾遇過的情境也可以放進這張圖表呢？

第二份講義讓學員根據自己的情況做威脅建模。請給學員足夠的時間填完這份講義，引導他們考慮不同要素：他們想保護什麼？會遭遇哪些攻擊者？（以及攻擊者的動機為何？能耐又如何？）他們的資產會如何受威脅？然後，讓他們將威脅標記在背面圖表的對應座標上。

最後，讓學員們回答剩下的問題：什麼樣的防禦能因應最可能發生的威脅？（要更好地保護自己和資產，下一步可以怎麼做？）鼓勵學員設定一個回顧並更新此威脅模型的日期，因為威脅模型是隨時變動的。

i. 威脅建模活動講義 - PDF
ii. 威脅建模活動講義 - Powerpoint
iii. 威脅建模活動講義 - LibreOffice

2. 兩步驟驗證的講義

我們編寫了一份雙面的練習講義（中文版），其中包含了使用兩步驟驗證的必備知識。我們建議在兩步驟驗證工作坊的最後發下這些講義，給學員複習的機會。

這份兩步驟驗證講義最適合配合密碼、密碼管理器，或兩步驟驗證課程使用，包含兩步驟驗證的基本觀念介紹（也就是你知道的「密碼」，和你所擁有的「裝置或可攜帶的物品」）。建議學員可以先學過密碼和密碼管理器的相關知識，再填寫這份講義。

經過資安工作坊的學員測試、新手教師的回饋、以及資安專家的建議，我們仍在持續改進這份講義。

如何使用這份講義：

這份講義的正面是兩步驟驗證的簡介，以及兩步驟驗證的各項優缺點，包括簡訊、手機和平板的驗證 App，以及 Security Tokens（硬體驗證裝置）。

講義的背面是設計給學員填寫的：這部分可以當作回家作業，也可以在工作坊中透過講師的引導完成。建議學員可以觀看 EFF 的 12 Days of 2FA 或相關網站，以尋找更多如何為特定服務開啓兩步驟驗證的資訊。學員可以運用附件圖表了解自己使用的服務中，哪些有提供 2FA（兩步驟認證），並記錄自己啟用了什麼 2FA 方法。在圖表右半邊，想要進一步提升帳號安全的學員們可以依照指示來做，例如啓用登入行為監控、建立旅遊備份計畫、救援代碼等等。

i. 2FA 核對清單講義 - PDF
ii. 2FA 核對清單講義 - LibreOffice
iii. 2FA 核對清單講義 - Powerpoint

使用 VPN 規避網路審查並加密你的通訊

「我需要 VPN 嗎？」與「我該使用哪個 VPN？」是資安工作坊中常見的提問。學員在尋找如何安全地使用公共場所的 WiFi 時，VPN 就是一個常見的防護措施；有些人，像是記者，可能會想使用 VPN 來偽裝上網的地點。學員可能有興趣了解如何在他們的國家繞過網路封鎖。然而，如何選擇 VPN 需要綜合考量各種因素和其中細微的差異，因此難以簡明地講述。這份課程計畫能幫助學員重新思考他們適合使用哪些工具，以及在挑選 VPN 時該考量哪些因素。

推薦閱讀

- 選擇適合自己的 VPN
- 推薦工具
- 網頁瀏覽的安全性簡介
- 該認識的加密知識
- Wirecutter 2019 年發布給消費者的報告針對不同 VPN 在安全性、隱私與其他消費者會顧慮的面向上做詳細的評比
- Level Up 關於網路審查如何運作的課程
- Localization Lab 的文章敘述如何用迷因在辛巴威普及 VPN 的使用
- Freedom of the Press Foundation 的文章深度解析挑選 VPN 的方法
- Center for Democracy & Technology 的文章解說何謂 VPN 及其運作方式
- NPR 這篇文章很重要，能讓學員了解 VPN 並非完全安全（譯註：文章的重點主要是 VPN 公司有可能會儲存客戶資料並轉售，或是 VPN 軟體本身是病毒）
- Great Fire's 的網站對想了解旅行時的 VPN 應用的讀者很實用
- CyberScoop 的故事以記者的經驗講述使用 VPN 的實例

你可能會遇到的問題與狀況

學員常會搞不清楚 VPN 的角色。許多人們會將 VPN 和 Tor 搞混。此外，學員可能不了解哪些資料和後設資料會暴露在 VPN 服務商下。

一個常見的誤解是 VPN 只能用於單一裝置（例如，「我以為 VPN 只能用在電腦上」）。學員可能不會警覺到無論是用手機或電腦，兩者連線到陌生或奇怪的 WiFi 的風險是相差無幾的。所以，一個重要的秘訣是，手機上也可以使用 VPN 來加密你的連線，就跟在電腦上一樣。

有些講師會使用譬喻法來描述 VPN 的原理，例如用「水管」或「隧道」比喻安全地輸送東西，或用「保險套」比喻連接公共 WiFi 時的保護措施。請務必重視文化脈絡、性別意識，以及學員對你的信任程度，謹慎斟酌使用與性相關的譬喻，因為這可能會讓很多學員不舒服。

可預期的問題與解答

＊你很可能會發現，對於很多問題，真正的答案要視情況而定。

問題：「我感覺被資訊轟炸了！你不能直接推薦一個 VPN 給我就好嗎？」

解答：如果講者有個人偏好且自行評估過的話，推薦一個你用過的 VPN 是沒問題的。然而，我們強烈建議你謹慎考慮推薦工具的方式 。請務必警告學員，要評估一個 VPN 的安全性並不容易，且各個 VPN 的安全性和隱私保障都可能隨時變動。請鼓勵學員透過定期追蹤跟自己所用的 VPN 相關的新聞，以積極瞭解情況。

問題：「為什麼我的 VPN 這麼難用？」

解答：學員可能會因為易用性或速度太慢等問題，而充滿挫折地如此提問。

一個可行的回答是：「不同 VPN 之間的品質差異相當之大。就像 email 一樣，選擇使用哪一家的服務會明顯影響你的使用體驗。」

可以考慮在討論各個 VPN 軟體的優缺點時，再回到這個問題。

問題：「我的公司有提供 VPN，我該直接用它嗎？」

解答：向學員解釋，選擇任何一個 VPN，都是在委託它提供你整個網際網路的使用。你可以舉出以下的例子來闡明使用公司 VPN 的好處與壞處：

「連線到工作用的 VPN 就像是連線到辦公室的 WiFi 一樣。雖然連線到辦公室提供的 VPN，可以在咖啡廳等地方防止某些人偷窺你的連線；但如果你要瀏覽其他公司的職缺，或檢舉公司的不當行為，你顯然有更好的選擇。因為公司的系統管理員可以查看你透過公司 VPN 上網時的一舉一動，跟你人在公司上網沒有兩樣。最重要的是要知道，使用 VPN 只是將你信賴的對象從 ISP 或 WiFi 熱點轉移到 VPN 身上而已。

另一個考量點是，你公司提供的 VPN 使用何種加密？有些加密協定（或演算法）已經過時，所以無法提供足夠的保護。你可以建議學員自己研究並選擇一款公用的 VPN，用來進行較敏感的上網活動，或諮詢公司的 IT 部門以確定公司的 VPN 有多安全。」

問題：「我付不起月費／年費怎麼辦？我可以用免費的 VPN 嗎？」

解答：若要節省費用的話，你可以使用其他防毒軟體套裝提供的 VPN（例如：Dashlane）。有些 VPN 會要求使用者先註冊帳號，並提供免費的 VPN 服務給舊使用者推薦的新人（例如：Riseup）。除此之外，還是有其他免費的 VPN 服務。

你可以給些像這樣的指導：「在調查免費的 VPN 服務時，最重要的是確定他們為何能夠以免費模式營運。他們會賣掉你的資料嗎？如果會的話，你能接受這個代價嗎？有些時候，免費 VPN 也可能含有惡意廣告。」

問題：「我聽說可以自己架設 VPN，我該這麼做嗎？」

解答：即使你的學員已經熟練系統管理與終端機，架設 VPN 仍然非常具有挑戰性。有些路由軟體（例如 OpenWRT 或 LEDE）會在後臺執行 OpenVPN 並提供一個網頁界面供你設定，但僅建議最進階的使用者嘗試。對於一般學員，最好還是不要離題去講太多設定 VPN 的細節，請鼓勵進階學員在課後來找你繼續討論。

問題：「我將要前往一個有言論審查的國家，我該注意什麼？」

解答：這是一個較深的問題，通常需要更多脈絡與協助。

情勢會變，所以重要的是隨時跟進該國 VPN 政策的資安近況。在某些國家，特定的 VPN（或任何 VPN）可能是違法的，攜帶預裝好 VPN 的電腦進入這些國家可能會有些冒險，尤其入境是最容易遭遇搜查的時刻。你可以鼓勵學員在下課後來找你討論。

問題：「如果我已經有 VPN 了，我還需要使用 HTTPS 嗎？」」」

解答：你可以提到 HTTPS 和 VPN 都是傳輸層的一種加密形式，用以防止學員的通訊被竊聽。然而，HTTPS 和 VPN 保護資訊的方式大大地不同。一定要知道的一點是，盡可能使用 HTTPS 來獲得更完全的保障，使用 VPN 或 Tor 時也不例外。

你可以讓學員閱讀 網站瀏覽安全概述 以瞭解更多。

問題：「VPN 和 Tor 有什麼不同？」

解答：雖然 Tor 網路跟大多 VPN 一樣使用加密通訊，但有一個關鍵的差別：當你使用 Tor 時，你並不需要信任任何公司或服務商。

Tor 網路是由志工共組的一套系統，你會在存取目標服務前，經過三台分散在全球、正在執行 Tor 程式的電腦，這些執行 Tor 的電腦稱為「節點」。資料傳輸途中的每一個節點（或稱「跳板」或「中繼」）只會解開一層加密並揭露下一個目的地。這麼做是為了維持訊息內容和路徑的隱密性。有了三個節點聯合起來遮掩身份，要想知道個別訊息是從哪裡、從誰手上發出的——將會極度困難。

（註：有些學員可能會不清楚執行 Tor 瀏覽器並不等於執行 Tor 中繼站；你可能要澄清，Tor 中繼站是由專門的志工電腦提供的。）

VPN 跟 Tor 網路不同的是，它本身是單一個中繼站。這點很重要，因爲政府可以透過傳票或法院命令向 VPN 公司索取資料，所以你必須信任 VPN 公司會積極保護你的資料（或者，最好完全不要蒐集資料）。

另一個講解 VPN 和 Tor 差異的方式，是網路審查與隱私考量的取捨：如果你想要規避審查，但不那麼在意隱私問題，那就用 VPN；如果你同時希望規避審查又保有隱私，你可能會想瞭解一下 Tor。告知學員使用 Tor 有其限制，並推薦學員實際使用看看，有興趣的學員可以造訪 Tor 專案網站：torproject.org。

問題：「政府或網路服務供應商（ISP）會知道我在使用 VPN 嗎？」

解答：是的，ISP 或政府會知道你在使用 VPN。在某些地區，政府甚至有可能即時透過 ISP 知道這件事。

有些軟體，像是 Tor，可以偽裝成是別的軟體而不被識別；然而，你需要在啓動 Tor 瀏覽器之前選擇這個選項。但要知道這種偽裝不是完美的——政府仍然可能用精細的方法偵測到你正在使用 Tor。

學習目標

學員將能達到以下目標：

- 至少說出一種使用 VPN 的好處（例如：安全性、連接陌生 WiFi 時的隱私，規避網路審查，保護資料不被 ISP 或政府偷窺）
- 能夠總結當使用 VPN 時，網路服務供應商（ISP）和 VPN 服務供應商分別能窺視哪些資料。
- 認識到 VPN 能在網路不安全的情況下提供額外的保護，並能舉出常見的不安全網路的例子（例如：咖啡廳、旅館、機場的 WiFi 等各種極度危險的網路）

- 知道手機也可以使用 VPN，不只是電腦。
- 對如何評估 VPN 的可信度有概念，並能舉出兩項選擇 VPN 時的考量點（例如：VPN 宣稱的安全性與隱私性、商業模式、評價、資料搜集行為、加密協定，以及該 VPN 受哪國法律管轄）。
- 知道如果他們想要匿名瀏覽，他們應該使用 Tor ——並另外學習如何使用 Tor 瀏覽器。

先備知識

- 關於加密，我該知道些什麼？
- 我如何保護自己免於遭遇惡意軟體？

師生比例

講師：學員＝1：10

建議教材

- 繪圖活動用的紙跟筆
- 投影機或白板，用來講解 VPN 的連線原理

課程內容

暖身：被封鎖的內容、探討可信度，及自我介紹

問大家一個問題：「有沒有人曾經想在線上閱讀文章、看電視劇或玩線上遊戲，但卻發現你使用的網路不讓你這麼做？請舉手。」如果學員不能理解，你可以舉例說明，像是在使用學校、公司或某些國家的網路瀏覽特定網站或服務時被封鎖了。

如果學員看來很進入狀況，你可以繼續問：「當你發現你想看的內容被封鎖時，你會怎麼做？」

有些人可能會回答：「試試看手機版網站」、「試試看把網址結尾改成不同國家的網域名稱」、「用 Google 翻譯來觀看網頁」、「用 Google 搜尋一段文字來尋找其他網站上有沒有相同的內容」、「試試看改用 HTTPS」、「用 Tor 瀏覽器」、「放棄」，或者「使用 VPN」。聚焦在 VPN 相關的回答上——你可以請一位自願的學員來分享，他們如何使用 VPN，以及 VPN 對他們而言是什麼。

然後，將學員分成 4～5 人一組，給他們 5～10 分鐘，用以下的破冰問題來介紹自己。

1. 你的名字和代名詞（例如：他/她/其他）是什麼？
2. 你今天為何來參加這個課程？
3. 曾有人請你幫他們保管東西嗎？例如，請你幫忙顧包包？
    - 他們如何知道你值得信賴？
    - 你如何處置他們交付的重要物品或資訊？

現在重新集合，讓學員分享他們曾被委託保管哪些貴重的東西。問他們：曾經有陌生人請你保管東西嗎？他們是在咖啡廳或車站，請你幫忙保管錢包、背包或電腦嗎？

知識分享：關於 ISP 能看到些什麼，和 VPN 是什麼的基本觀念。

你可以使用他們在暖身活動的答案作為引導，以解釋網際網路服務供應商（ISP）是如何保管有價值的資訊。

講師：「網際網路服務供應商，也就是 ISP，能夠在你連接 WiFi 上網時看到有價值的資訊。舉例來說，他們能看到哪些東西呢？」

你可能會得到的答案有：「我的電子郵件」或「我的瀏覽記錄」。有些學員可能會在討論 ISP 掌握什麼時，提到網路中立性，例如 ISP 可以控制降速或封鎖特定內容。

然後問學員們，他們是否信任 ISP，就跟他們信任朋友或家人保管敏感資訊或個人物品一樣。

虛擬私人網路（VPN）是一套軟體，透過伺服器將你的網路活動繞道傳輸，可以掩飾你的 IP，讓 IP 看似來自其他地方。它經常被用於規避網路審查——例如：當你使用經學校審查的網際網路，或在有網路內容封鎖的國家上網時，使用 VPN，你應該就能造訪被封鎖的網站。

講師應該強調：「沒有『一體適用』的 VPN，每個人使用 VPN 的需求都不一樣。」接著解釋就像你對每個人的信任程度不一，有些 VPN 較值得或不值得信賴。通常很難評估 VPN 的可信度，不過仍有一些重點是調查 VPN 的可信度時可多加留意的。

知識分享：怎樣的 VPN 值得信賴？

讓學員回到小組，並提出以下問題：「選擇 VPN 時你會尋找哪些資料？想想是什麼讓你信任一個人，並以此為準則。接下來討論五分鐘，之後我們來分享討論的內容。」

讓小組互相討論，再重新召集。請學員們分享他們在小組中得到的答案。你可能會得到的答案有：「他們的聲譽很好」或「他們有受其他人信任的經歷」。向學員說明，就像我們決定是否信任他人時一樣，VPN 的聲譽非常重要。其他可能出現的答案有，「他們妥善保管了資料」，並解釋 VPN 的加密技術如何保障資料安全。

學員可能會提出問題而不是答案——例如「我怎麼知道 VPN 會照它說的去做？」鼓勵這些提問，因為它們顯示出資安專家在應對軟體評估等難題時也會有的批判性思考。你可以在解釋 VPN 的工作原理之後再回來討論他們的問題。

活動：畫出「你」、「ISP」，和「VPN」

現在要求學員各自或分組畫出他們認為自己、ISP 和 VPN 之間的關係。在他們開始之前，解釋一些可能有幫助的圖像：

- 「水管」或「隧道」可以用來圖解資訊流通的路徑
  - 水管可以嵌套在其他水管內
- 「卷軸」或「明信片」可以用來圖解有價值的資訊，例如：朋友間的訊息、你瀏覽的網站和閱讀的文章
- 「機器人」或「電腦」可以用來圖解 ISP 和 VPN
  - 他們可以舉起水管（維持基礎建設的運作）
  - 作為水管的起點或終端（例如連線的目標）

給學員 5 到 10 分鐘畫畫，要求他們標註每個元素。如果學員卡住了，你可以給他們以下的指導：

- 圖中應該畫出嘗試連上網站的電腦或手機
- 圖中應該畫出與 VPN 的連線
- 圖中應該畫出與 ISP 的連線
- 圖中應該畫出要連接的目標（網站）

學員畫完後，可以將成品張貼到牆上。在討論每張圖解時可著重詢問學員：

- 解釋圖示中的系統如何運作？
- 圖示運作中分享了哪些資訊？

檢視每張畫作並在看到跟 VPN 正確運作相關的概念出現時，給予正面回饋。仔細紀錄下任何學員們誤解的地方，再與全體學員一起看過每個誤解的概念。

講師可以透過詢問以下問題確認學員是否有真的理解：

- 連接管道（就是「水管」或「隧道」）是透明的嗎？它有掩飾任何資訊嗎?

- 如果你沒有使用 VPN，ISP 可以看到什麼資訊？
- 如果連接 VPN，會有什麼改變？
- VPN 可以看到什麼資訊？
- ISP 會認為你是從哪裡連接上網的？
- VPN 會認為你是從哪裡連接上網的？

一一看過學員的畫作後，講師可以畫出自己的圖示，以此講解各元件之間的關係。

知識分享：VPN 的限制

現在學員已經大致了解 VPN 的角色，你可以更深入詳述 VPN 的特性。

隱私及安全性聲明

一些 VPN 主張不分享或出售使用者資料。你應該鼓勵學員思考：如何證明這些主張是真的？鼓勵學員仔細研究 VPN 提出的所有主張，並強調行銷聲明並非保證。例如：即使 VPN 不直接將資料賣給第三方，查閱 VPN 的隱私權政策通常會發現 VPN 如何利用你的資料獲利。

商業模式

即使 VPN 不出售你的資料，它也必須用某種方式維持營運。如果 VPN 不是靠出售服務本身獲利（亦即，如果是免費的 VPN 服務），讓學員學會思考：「它是如何經營下去的？它募捐嗎？它的商業模式是什麼？某些 VPN 以「免費增值」模式營運，這意味著你可以免費使用，但在你使用一定的資料用量之後開始收費。有些 VPN 則是完全免費，但要可能付出一定的隱私作為代價（例如：他們可能會出售資料，或用其他方式從你的資料獲利）。尤其是當學員的預算有限時，要注意這些重要的考量事項。這些都是學員在選擇適合他們的 VPN 之前應該考慮的重要因素。

聲譽

另一項考量因素是聲譽，這可能很難做出判斷。值得對與 VPN 相關的人員和組織進行一些研究。他們是否得到資安專家的認可？如果該 VPN 是由資安社群的知名人士建立，可能比較值得信賴。該 VPN 是否有相關新聞報導？對於那些無人以聲譽擔保，或由一家不知名的公司營運的 VPN 應保持懷疑態度。

資料蒐集行為

一個從一開始就不蒐集資料的服務，就不可能會出售你的資料了。瀏覽隱私權政策時，請看看該 VPN 究竟有無蒐集使用者資料。如果它並未表明不會蒐集使用者資料，那它很可能就有。再者，根據法律管轄權，政府可以發出法院傳票索取該資料。

即使該公司聲稱不會記錄連線資料，也不一定保證他們會守規矩。鼓勵學員們調查媒體報導中出現過的 VPN 案例，有些公司可能曾被抓到誤導或欺騙消費者。一個簡單的搜尋會很有幫助。

加密

你可以鼓勵學員瞭解他們的 VPN 加密的安全性；也就是說，VPN 使用的傳輸層加密是否如預期般運作，你可以用先前圖畫中的管子是否「透明」或「易碎」為例。如果該 VPN 使用壞掉的加密方式——如「點對點隧道協議（PPTP）」或「弱加密金鑰」——就好像你的隧道是透明的一樣。任何通過的資料都可以被 ISP、政府和壞人看見。評估 VPN 加密的強度可能很困難，因此你可能需要向學員介紹在「出版自由基金會（Freedom of the Press Foundation）」的「實用 VPN 指南」中概述的技術注意事項，或這份 VPN 比較表中的「TECHNICAL Security」欄位。如果有任何學員正在使用（或正考慮使用）自己公司提供的 VPN，請他們諮詢 IT 部門以瞭解連線的安全性。

所在地和法律

最後，有些學員可能會根據營運商總部所在地來選擇 VPN。你可以提及，對於有些人，例如社運人士或高風險新聞工作者，根據適用資料隱私法規與否選擇 VPN 可能是一個重要的考量因素。但也務必提到，公司政策和法律可能隨時變動。

知識分享：VPN 和軟體

既然學員們學會了一些評估 VPN 的標準，你可以更詳細講解他們可以如何連接到 VPN，以及在安裝軟體時應考慮什麼。你可以問：「某些 VPN 會要你安裝專用的軟體，這有什麼好處？」

你可能會聽到的答案是，這樣會更方便使用。有友善的使用者界面的 VPN 通常比需要自行設定的通用界面（例如：輸入伺服器名稱與連接埠來連線）更容易上手。

你可以說明：「沒錯，專用的程式非常好用。它使得連接 VPN 的過程變得很輕鬆，無需輸入令人困惑的設定，例如伺服器名稱與連接埠。」

然後，你可以提出這個問題：「但是，安裝 VPN 軟體會有什麼危險呢？」

有人可能會回答：「因為 VPN 可能不值得信賴！」不像 ISP，網路上的任何人都可以輕易架設 VPN 服務。你可以說明，因為你安裝的任何軟體都有可能是偽裝的惡意軟體，因此在安裝任何軟體之前先確認 VPN 是否值得信任很重要。

講師應該強調這點：「你必須對任何選擇安裝的 VPN 軟體有把握，因為安裝任何惡意軟體都會造成很大的危害。VPN 軟體之中，很少做過正式的安全審核，即允許外部人員對軟體的安全性及行為進行全面評估。」

鼓勵學員研究一下 VPN 供應商，並在考慮安裝任何 VPN 軟體之前，查閱可信媒體來源上的文章。

回顧活動：VPN——有哪些優點和哪些缺點？

你已經講述了使用 VPN 的優點，以及學員在評估任何 VPN 服務的隱私與安全性時應考慮的重要事項，現在你需要跟學員一起複習一下。

將學員分成幾組，給他們以下的提示，並讓他們把答案逐個寫在便條紙上：

「你們將有五分鐘的時間回答這個問題——VPN 為什麼有用？」

同時，在看得見的地方，你可以寫下以下類別：

- 安全性
- 使用不可靠網路（例如陌生 WiFi ）時的隱私
- 規避審查
- 防止 ISP 窺探資料
- 防止政府窺探資料

學員在便條紙上寫完想法之後，請說明你提出的類別，然後讓學員把他們的答案放在適當的類別下。等所有人都完成之後，你可以講解，如他們所見，VPN 有廣泛的用途。大聲朗讀一些便條紙上的答案，並為脫穎而出的答案提供正面的補充。

完成後，請學員在小組中討論：「VPN 有什麼壞處？幾分鐘後，我們會來分享我們的討論。」

等他們聊了 2～3 分鐘之後，請他們分享所討論的內容。答案可能包括：「VPN 無法確保真正的匿名性」、「VPN 無法阻止政府使用傳票得到你的資料」，或「VPN 無法保護我的瀏覽器不受追蹤」等。

學員可能會有很多問題，請保留足夠的問答時間。

學員會需要複習本課程中的各主題。請務必告知他們以下的資源：

- 選擇適合你的 VPN
- 關於加密，我該知道什麼？
- 網路瀏覽安全性的導論

對於（比起繞過網路審查）較關心匿名性，或者如何對 ISP 與政府保有隱私的學員，你可以請他們參閱 SSD 的「Tor 瀏覽器指南（MacOS／Linux／Windows）」，以及 Tor 專案中關於如何使用 Tor 瀏覽器的相關介紹。請注意，Tor 瀏覽器在保持匿名性上有其特別需要考量的點，所以建議使用者要經過特別訓練。

密碼 - 初階

即使建立一個安全的強密碼是網路安全中最重要的事情之一，對於學員來說仍是非常困難的。安全密碼規範可能互相矛盾，而且難以全部落實及記憶。在這個章節中，我們將討論強密碼背後的「如何」以及「為什麼」。

推薦閱讀

- 建立高強度密碼
- 動畫介紹：如何用骰子製作一個超級安全的密碼
- 使用密碼管理器以確保上網的安全性
- XKCD 關於密碼強度及密碼生成系統 Diceware 的漫畫

你可能會遇到的問題與狀況

- 產生新密碼時，可能會有一些學員忘記他們的新密碼。 如果人們在不記住密碼的情況下更改了重要帳戶或設備的密碼，此活動可能弊大於利。
- 考慮建議人們寫下他們的密碼（抄在紙上或是記錄在密碼管理器中）。 提醒那些寫下密碼的人提防別人偷看他們的筆記，並將這些筆記保存在安全的地方！
- 對於那些難以記住其密碼的人，我們可以考慮使用一些輔助記憶技巧。例如在連結圖像記憶、使用助記詞 (mnemonics) 或連結一個好笑的故事等來幫助他們記憶密碼。
- 有些人可能因為行動不便而無法輸入長的密碼。在這種狀況下，請提供他們適度的協助並考慮降低密碼長度要求。
- 有些人可能對於 Diceware 或亂數字典單字選擇技術所產生的密碼有疑問，可能是因為他們沒有辦法拼寫這些單字。考慮幫助他們選取其他較為熟悉但仍然隨機的單字。

學習目標

學員將會：

- 能給出弱密碼的範例
- 能夠描述攻擊者容易猜到的弱密碼
- 能夠描述為什麼在不同帳號中使用相同密碼會帶來風險
- 能夠解釋為什麼誠實的回答「安全問題」會帶來危險
- 能夠描述強密碼是怎麼生成的
- 能夠解釋為什麼使用骰子或書籍可以幫助產生隨機密碼
- 產生高度安全的密碼短語

先備知識

- 如果你計劃讓學員實際產生自己的密碼和短語，那麼他們應該擁有自己的設備並在上面安裝密碼管理器（請參閱密碼管理器章節）。
- 學員應大致了解 Web 瀏覽器是什麼，並熟悉如何登入網站。

師生比例

講師：學員 = 1:4

建議教材

學員視線範圍的一個可繪畫區域，例如白板
如果要展示外部資源，需要準備一台電腦和投影機

課程內容

暖身：介紹夥伴

在白板或投影片上的可見位置寫下三個問題：

1. 你的名字和代名詞（例如：他/她/其他）
2. 早餐吃什麼
3. 你第一次為網站建立帳號是什麼時候？你有設定密碼嗎？如果你願意分享你第一個密碼嗎，那是什麼？

讓所有人各自配對，並讓他們彼此回答問題。然後巡視教室，讓每個人向大家介紹他們的夥伴。 例如：「這是奈瑪。她早餐吃雞蛋。她第一次設定密碼是在 3 年級時，為了一個關於帶卡通寵物進行冒險的網站所設定的。密碼是 『iamcool』。」

你會在破冰遊戲中發現：

- 你的學員在社交及團體合作的情形如何
- 他們是否了解什麼是密碼
- 他們對於遵循指示及記憶細節的配合程度

這款破冰遊戲有趣之處在於，人們的記憶能力其實比他們想像的還好。稍後你在解釋如何記住密碼短語時，可以提醒他們記住夥伴的隨機細節是多麼容易。

活動：什麼是弱密碼？

講師可以在活動中使用白板，也可以在紙上寫下註釋。

狹義觀點：如果有人認識你，什麼是弱密碼？

講師可以分配 2～4 分鐘的時間討論下列主題，我們建議讓學員在限定時間內完成討論，以免討論太過發散。

講師：請在接下來的 X 分鐘內，與你配對好的夥伴互相回答下列問題

1. 你是否能夠根據你對某人的了解，例如某人的生日、最喜歡的動物、喜歡的歌曲或興趣來猜測某個人的密碼？
2. 是否曾經有人與你共享密碼，而你對他們的密碼完全不感到驚訝？
3. 想一想你認識的人。你有辦法代替他們回答他們的安全性問題嗎？

在雙方討論之後，講師可以把大家重新組織起來。講師可以要求一個自願者，在公開或不公開密碼本身的前提下，分享一個「簡單」或「毫不奇怪」的密碼及背後的故事。

講師：「在接下來的 X 分鐘，請繼續與你的夥伴討論以下內容『如果有人要在這種情況下用 Google 搜索你的朋友，或者查看他們的社交媒體帳戶，或在辦公桌周圍尋找提示，他們是否能夠猜出該朋友的興趣？而這些興趣有可能讓他們獲得密碼的提示嗎？ 有可能讓他們更容易猜到安全性問題嗎？』」

在時間結束後，講者可以把大家重新組織起來。

講者可以要求學員舉手回答問題，或者讓他們用手或腳製造聲響。

講者：「根據朋友無意間透露的訊息，你們之中有多少人能夠找到有關你朋友密碼的資訊？」

廣義觀點：參考資料本身，什麼是弱密碼？

講者：「請猜猜看，最常見的密碼有哪些？請跟你的夥伴在接下來的 X 分鐘內至少找出 5 個常見密碼。」

時間到，講者會詢問大家得出什麼結論。

講者會把得到的密碼寫在白板上，講師可以偶爾問大家：「請問有任何人曾經用過這些密碼嗎？並特別把這些密碼圈起來。每當有人舉手，可以在這些密碼旁邊加上一次

星號。」

學員可能會想到「密碼」的拼寫、鍵盤上常用鍵的位置（如「 qwerty」）、序號（如「 123456」）、流行文化中的常用短語（如「芝麻開門」）或其他不太適合的字，甚至網頁上包含的單詞，例如「admin」和「Facebook」。

講者可以提示學員：「最喜歡的運動呢？最喜歡的顏色？常用的字詞？電影或書籍的名言？歌曲歌詞？」

講者：「我希望大家跟自己的夥伴在下一分鐘中進行討論『你認為人們如何確定最常用的密碼是什麼？』」

講者將在分配的時間後重新組織大家，並詢問學員。「你想到什麼？」並期待學員提出洩漏資料或遭駭客入侵的網站資料庫等來源。

如果最近新聞中有重大的資料庫洩露事件（例如 Yahoo! 在 2013 年，Adobe 在 2013 年，LinkedIn 在 2012 年），講師可以將其列為討論重點，以了解為什麼強密碼很重要，以及為什麼不該在不同帳號使用相同密碼。

活動：對於弱密碼，我們能做什麼？

講師可以展示這個紀錄密碼外洩的資料庫的網站 https://haveibeenpwned.com/

講師可以根據這個網站來說明：「密碼外洩可能是了解人們習慣如何設定密碼的重要依據。透過這些前車之鑑，我們可以看到，在選擇私密且寶貴的密碼時，人們普遍的行為是可以預測的。」

講師解釋：「假設你只是知道了有關社交網站資料庫洩露的訊息，並知道可以下載這些洩漏檔案來獲得密碼、安全性問題和答案以及數百萬用戶的相關電子郵件。 哦，不！ 該網站沒有對這些敏感資料使用強加密。這可是很大一筆資料。如果你是一個想要賺錢的攻擊者，應該是一筆大豐收。」

講者：「請與你的夥伴進行 X 分鐘的討論：『要如何處理這些電子郵件、安全性問題和密碼？』我希望你們設想一些情境。如果你是攻擊者，這些資訊對你有什麼價值？」

講者在時間結束後，再次提出問題：「你想到什麼？ 你將如何使用這些電子郵件和密碼？ 你將如何使用這些安全性問題和答案？」並等待學員回答。 他們可能有多種答案，包括「注意用戶名稱」、「嘗試尋找有價值的人」、「與其他攻擊者共享該資訊」、「在其他相關的帳號上嘗試所有密碼的排列組合」等等。

講師可以了解討論的方向，並讓學員有機會思考懷有惡意的人在所有情況下是如何看待使用者的帳號所包含的詳細資訊。

講師：「讓我們談談攻擊者的能力。這是一個數字遊戲，在這種情況下，攻擊者憑藉的是人們的可預測性。許多人在不同的網站上使用相同的密碼，可能在尾端添加一些數字，或者將字母換成數字。對於攻擊者來說，用暴力破解法到盡可能嘗試多個帳戶是一種相當普遍的做法；也就是說，『攻擊者會在不同網站中盡可能使用來自這些漏洞的密碼。他們可以透過電腦為他們輸入帳號訊息來迅速達成目的。他們可以為自己的電腦編寫程式，好做到在密碼尾端添加數字，或將數字與字母交換等嘗試，並從已知的常用單詞，常用引號和短語中獲得提示。」

講師：「你可能會記得 （在這裡提起任何一個資料洩漏的新聞，可能是駭客入侵，或是 HaveIBeenPwned 的漏洞列表）。當發生此類洩漏行為時，你該怎麼辦？」

學員的回答可能包括：「不知道怎麼辦」和「刪除你的帳戶」，到更主動的「監控帳號資訊」、「設置兩步驟驗證」或「更改你的密碼」等建議。講師應該鼓勵最後三個行為並告訴學員可以使用這三種方法以及其優點。

講師可以使用「更改密碼」的建議來提示以下討論：「你可以將密碼更改為什麼？」

知識分享：什麼是強密碼？

講師：「假設你決定更改密碼。請記住，你已經學到了：

- 我們可能會選擇與我們個人相關的密碼，別人可以透過對我們興趣或經歷的了解來推測密碼
- 即使密碼與我們的個人經歷沒有直接關係，別人還是能預測我們對密碼的選擇
- 我們傾向於對同一密碼進行可預測的變化
- 我們傾向於在許多網站上使用相同或相似的密碼
- 密碼越短，電腦越容易猜測

講師將上述限制寫在白板上、放在投影片或以其他可見方式呈現。

講師：「考慮到這些常見的弱密碼，強密碼可能具有哪些要件？請與你的夥伴用一分鐘討論。」

講師再次詢問，希望學員得出與「長」、「隨機」和「唯一」等仲要關鍵字類似的結論。

然後，講師應以可見的方式寫出這些重點：

- 隨機
- 唯一
- 長

密碼對於每個網站都應該是隨機的、較長的且唯一的。

講師可以展示 XKCD 漫畫來說明這一點。 https://xkcd.com/936

學員可能會問：「但是我怎麼可能記住這些隨機的、唯一的長密碼呢？」此時是向學員推薦密碼管理器的絕佳機會。

密碼 - 進階

即使建立一個安全的強密碼是網路安全中最重要的事情之一，對於學員來說仍是非常困難的。安全密碼規範可能互相矛盾，而且難以全部落實及記憶。在這個章節中，我們將討論強密碼背後的「如何」以及「為什麼」。

推薦閱讀

- 建立高強度密碼
- 動畫介紹：如何用骰子製作一個超級安全的密碼
- 使用密碼管理器以確保上網的安全性
- XKCD 關於密碼強度及密碼生成系統 Diceware 的漫畫

你可能會遇到的問題與狀況

- 產生新密碼時，可能會有一些學員忘記他們的新密碼。 如果人們在不記住密碼的情況下更改了重要帳戶或設備的密碼，此活動可能弊大於利。
- 考慮建議人們寫下他們的密碼（抄在紙上或是記錄在密碼管理器中）。 提醒那些寫下密碼的人提防別人偷看他們的筆記，並將這些筆記保存在安全的地方！
- 對於那些難以記住其密碼的人，我們可以考慮使用一些輔助記憶技巧。例如在連結圖像記憶、使用助記詞 (mnemonics) 或連結一個好笑的故事等來幫助他們記憶密碼。
- 有些人可能因為行動不便而無法輸入長的密碼。在這種狀況下，請提供他們適度的協助並考慮降低密碼長度要求。
- 有些人可能對於 Diceware 或亂數字典單字選擇技術所產生的密碼有疑問，可能是因為他們沒有辦法拼寫這些單字。考慮幫助他們選取其他較為熟悉但仍然隨機的單字。

學習目標

學員將會：

- 能夠解釋為什麼使用骰子或書籍產生密碼能有效地保證隨機性
- 產生高度安全的密碼短語 (passphrase)。

師生比

講師：學員 = 1:4

建議教材

講師可提供便利貼和筆，以便學員寫下他們的新密碼。

可選：書
可選：骰子
可選：EFF 的骰子字彙表

課程內容

知識分享

回顧：引導學員了解為什麼爛密碼容易被猜出。

- 常用英文單字
- 常用英文單字（有些字母被轉成數字，例如 o 寫成 0）
- 名字和日期
- 鍵盤連續按鈕
- 展示最常見的密碼列表 https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

你可以提到的其他重點包括：

- 顯示強密碼的範例。
- 討論為什麼永遠不要在不同網站或服務使用重複的密碼。
- 討論為什麼密碼管理器很有幫助。
- 討論主密碼或密碼短語的目的。
- 討論如何記住密碼短語。

活動：產生密碼短語（passphrase)

在產生密碼短語的過程中，有幾種方法可用於引導學員。這些活動的好處是，學員即使沒有攜帶電腦或其他設備，也可以參與其中。

以下活動要求學員記住他們的新密碼。背誦對每個人來說不一定可行，訓練結束後人們可能會忘記新的密碼短語。 提供學員便利貼和筆以寫下他們的新密碼可能很有幫助。

講師可以提供加強記憶的建議，例如使用助記符（例如，用「 ERN」記住「Elephant Rainbow Novel」），或依據密碼短語建立視覺故事（例如「Elephant Rainbow Novel」，想像大象在彩虹上行走，然後在彩虹的盡頭讀書。）

從書中選擇單字

這個方法只需要每個學員手中都有一本書，這是在學校、圖書館或其他有很多書籍的地方進行培訓的好處之一。

1. 閉上你的眼睛
2. 隨機翻開書的一頁
3. 將手指放在頁面上的某處

4. 睜開眼睛，寫下最靠近手指的單詞
5. 如果該單詞是一個常見且易於猜測的單詞，請返回步驟 1
6. 重複步驟 1～5 四次，總共得到五個單詞
7. 完成！ 你得到了一個新的密碼短語

知識分享：使用 Diceware 生成密碼短語（非強制活動）

產生密碼短語的另一個方法是使用一個稱為 Diceware 的系統，在該系統中，你使用一組骰子（共 5 個）和一個預定的單詞列表來生成密碼短語。我們是 EFF Diceware 的忠實擁護者。我們甚至創建了自己的 EFF 骰子集和我們自己的單詞列表。對於喜歡新奇方法的用戶而言，這方法可能會很有趣。

不過，Diceware 也可能會嚇到一些學員。如果你手頭沒有好幾套骰子和單詞列表，那麼當每個人都在等待輪到自己時，可能會造成尷尬的靜默。

有關使用 Diceware 和使用該列表的說明，請參考 eff.org/dice。

兩步驟驗證（Two Factor Authentication）- 初階

兩步驟驗證（也稱為「2FA」）是保護帳號安全最簡單的手段之一，但是進行 2FA 的教學可能會有點棘手。不同的線上服務在設置 2FA 的過程時可能會牽涉不同的語彙跟設定流程，而且有些應用程式可能不支援每個線上服務的 2FA。面對不容易的教學現場，本課程會幫助你在處理 2FA 主題時，減少學員的困惑，並不讓他們失去興趣。

推薦閱讀

- 如何啟用兩步驟驗證
- 哪些網頁服務支持 2FA
- 網路上常見的兩步驟驗證指南
- 12 天上手 2FA，如何為你的線上服務帳戶開啟兩步驟驗證

你可能會遇到的問題與狀況

兩步驟驗證最大的挑戰是，儘管想法和實踐都看似容易，但存在許多容易分散學員注意力的附帶問題。

- 在教學這個概念時，有很多系統的設計對於學員來說「像是」2FA，實則不然，像是帳戶恢復、密碼重置和安全性問答。
- 許多服務對於兩步驟驗證也使用不同的名稱，讓辨識及找到相關的設定變得困難。常見的包括「多因素身份驗證（Multi-Factor Authentication）」、「兩階段驗證（Two-step Authentication）」、「登入批准（Login Approvals）」。
- 線上服務可能會把開啟 2FA 的設定藏在深處，且每個的位置皆不一致。
- 2FA 可能會在一些情況失效而鎖住帳號，例如當手機不在你身邊時，你就無法

登入帳號。

- 有些 2FA 的實作方式無法保護你免受攻擊者的侵害，例如，當攻擊者掌握你的手機，而驗證碼又是透過手機簡訊傳送時。
- 2FA 的應用程式非常多樣且可以互相取代，因此沒有一個最「標準」或「正確」的選擇。

策略上，講師應盡量提供與學員有關的知識，不需太費心告知他們無法掌控的問題。例如：

- 指導學員該如何找到「兩步驟」的相關資訊，而不是學習操作某個特定的流程。
- 將 2FA 定調為「額外的小步驟」——它並非完美（畢竟幾乎所有 2FA 系統都有它的未竟之處），也不是絕對必要，但比起只使用密碼來說，還是有幫助。
- 引導學員了解他們可以在自己的線上帳戶開啟 2FA 的參考資源，例如 https://twofactorauth.org。

你不必談到所有 2FA 可能失效的情形（failure modes）。可以著重討論它減少了哪些危害，而非做不到的功能。

可預期的問題與解答

問題：「如何為『某線上服務』啟用兩步驟驗證？」

解答：「我們一起看看 https://twofactorauth.org/ ……」（依照培訓的結構，逐步指導學員或協助他們瞭解）

問題：「如果我旅行在外、弄丟手機或沒有兩步驟驗證的裝置怎麼辦？」

解答：如果你有電話但沒有收訊，你仍然可以使用身份驗證應用程式。另外，許多網站都可以讓你存下或列印出「備用驗證碼」。當你沒有手機或無法接收簡訊時，能使用這些備用碼取而代之。每個代碼僅供一次使用，無論是抄下、列印或是存在電腦裡，請將它們保存在安全的地方，以免弄丟或遺忘，否則他人可能有機會發現並用來盜用你的帳號。

問題：「我不喜歡每次都要這麼麻煩！」（技術上來說，這不是一個問題，但這是一個經常聽到的發言）

解答：你通常可以讓它「信任這台電腦」，隔一段時間後才重新要求一次，下次注意登入時旁邊的選項。

（譯註：CSCS 社群的立場是不建議這麼做，這會在電腦遺失或被盜用的時候產生風險。）

問題：「我聽說『某次資安事件』中駭客繞過了兩步驟驗證進行攻擊。」

解答：這可能是電話系統被入侵（透過 SS7 系統 劫持或攔截簡訊），也可能是攻擊者致電電信業者的客服並騙他們拿出簡訊。或者，帳號救援流程的安全性出了問題，並被用來繞過常規的登入系統。

如果你並不使用簡訊，而是兩步驟驗證 App 或是硬體 Token 裝置，那這些都不必擔心！

如果你確實使用簡訊，那也不需要過於擔憂。要使攻擊者成功繞過你的簡訊 2FA，他們必須知道你的密碼，以及花大量時間和精力針對你研擬攻擊策略。如果你擔心被攻擊的風險，那麼使用簡訊 2FA 可能就不適合你，但若你被針對攻擊的風險很小，那簡訊 2FA 應該都還稱得上安全。

請記住：沒有完美的資安手段，基於簡訊的 2FA 自然不例外。與其關注那些缺陷，不如考慮它的優勢跟劣勢，以及這些折衷對於具體情況有何影響。

問題：「為什麼服務不是只要求第兩個密碼，而要使用手機等等的方式？」

解答：跟學員說明這不符合「記在腦裡的 + 拿在手上的」的「兩步驟」結構，而且這樣同樣有密碼失竊的風險。

問題：「為什麼我應該相信 Google Authenticator 這樣的應用程式呢？我不希望他

們看到我的 2FA 驗證碼。」

解答：的確，理論上 Google 可以利用 Authenticator 取得你的驗證碼，但他們不太可能這麼做。這些公司設計 Authenticator 來加強他們服務的安全性，所以要是他們自己藉此動手腳，那也是破壞他們服務的安全性。再來，別忘了：只取得你的驗證碼也是不夠的，他們還需要你的密碼。網路上也存在一些開放原始碼（Open Source）的替代方案，因此要是你真的不想使用 Google Authenticator，也可以考慮這些開放原始碼的應用程式，比方說 FreeOTP 等等。

問題：「這類的驗證 App 是怎麼運作的？或者，TOTP（Time-based One-time Password，基於時間的動態密碼系統）是怎麼運作的？」

解答：這是一個很進階的問題，建議個別回答這樣的技術細節問題。可以推薦他們參考這個討論串：[Google 身分驗證器是如何運作的？]

學習目標

學員將：

- 了解什麼是兩步驟驗證，以及它如何避免帳號遭到未經授權的盜用及入侵。
- 了解兩步驟驗證的各種稱呼。
- 能分辨出 2FA 驗證 App 以及簡訊接收驗證碼之間的區別，並且能描述兩種方法的優缺點。

師生比例

靈活有彈性

建議教材

- 兩步驟驗證文件
- 兩步驟驗證講義

知識分享可能是一個進行培訓的好方式。可以用一個討論形式的小講座來讓大家了解兩步驟驗證。

要找到每個線上服務的兩步驟驗證設定頁面可能需要費些力氣，因此如果有助教的話對培訓會很有幫助（一名助教協助五名學員）。

啟用兩步驟驗證的實作可能會需要一對一（或一對二）的教學。

建議閱讀

- 如何啟用兩步驟驗證
- 哪些網頁服務支持2FA
- 網路上常見的兩步驟驗證指南
- 12 天上手 2FA，如何為你的線上服務帳戶開啟兩步驟驗證

課程內容

知識分享：什麼是「兩步驟」？

某些服務會提供「兩步驟驗證」的設定，也就是說，除了密碼之外，可以在帳號登入時多進行另一個項目的驗證。

通常，他們會要求你輸入從簡訊收到的某個驗證碼，或要求你使用一個額外的 App 來確認你的身份。它能確認登入者不僅知道密碼，個人手上還持有其他的東西，像是具

有正確電話號碼的手機，或是手機上預先設置好的 App。

這樣可以防止密碼被盜，攻擊者也無法在沒有手機的情況下進入你的帳戶。

注意！如果你是使用以發送簡訊到手機進行的 2FA，那便需要對服務商提供你的電話號碼，或至少是一個可接收簡訊的電話號碼。對於某些人來說，這可能不是理想的選擇。對於那些想維持匿名的人，在平台上啟用簡訊 2FA 不是個好主意。

趣味活動：「惱人的保全」

問台下的學員：「這邊有沒有人曾經在即將要進入聚會、派對、活動、辦公室的時候，被一個疑心很重的保全擋在門外過呢？」

在學員中挑選一些人擔任「保全」的角色，如果這是一個很小的小組討論，那可以讓每個學員都擔任「保全」。

「我會試著證明我確實可以通過（進入聚會或活動），但無論我說什麼，你都應該回應一個理由，說明這不足以證明我可以被授權進入。」「我的名字有在受邀名單上被列出，只是保全不能確認我是不是這個人而已。」

「你好，我叫 XXX，我是來這裡授課資訊安全的講師，你在名單上看到我的名字了嗎？」

保全應該提出例如：「我沒看到你的名字」或是「我怎麼知道這真的是你？」這類的藉口，依次檢查其他可能的辨識方法，可以越來越荒唐，比方說：「好吧，這是我的信用卡，上面貼有我的名字」或是「這是我的護照，上面有我的相片」，或「你隨便去問一個認識我的人，他們都知道我是一個非常出色的舞者，所以這是我的招牌舞」、「這是我和你老闆在 Instagram 上的合照」等等……。

這個活動說明沒有一種完美的方式來讓人證明自己的身份，但能證明自己身份的方式越多，這就越有可能屬實。保全持懷疑的態度並沒有錯，最終這些證據的有效性可以合理地證明某人就是他們聲稱的那個人。

完成「惱人的保全」活動後，請說明這與本課的關係：

「現在將這個想法套用在帳號登入上。大多數登入都僅要求使用者以一種方式證明身份：密碼。密碼的問題是它們可能會被其他人盜取，這就是一個惱人的保全會注意到的。」

「你在生活中的其他部分也會遇到這類的問題，提款機就是一個很好的例子：你會需要插入卡片以及輸入密碼才能被允許取款或存款。其他人有機會取得你的密碼或是可能會偷取你的提款卡，但他們不太可能一次同時達成這兩件事。」

「因此，兩步驟只是意味著『密碼之外的其他東西』，你的密碼是你進行驗證的第一個『步驟』，然後你需要再提供另一個。」

請詢問學員：「在你登入線上帳號時，網站能問你什麼資訊作為驗證？」並強調它必須是密碼之外的資訊。

兩步驟驗證（Two Factor Authentication）- 進階

兩步驟驗證（也稱為「2FA」）是保護帳號安全最簡單的手段之一，但是進行 2FA 的教學可能會有點棘手。不同的線上服務在設置 2FA 的過程時可能會牽涉不同的語彙跟設定流程，而且有些應用程式可能不支援每個線上服務的 2FA。面對不容易的教學現場，本課程會幫助你在處理 2FA 主題時，減少學員的困惑，並不讓他們失去興趣。

推薦閱讀

- 如何啟用兩步驟驗證
- 哪些網頁服務支持 2FA
- 網路上常見的兩步驟驗證指南
- 12 天上手 2FA，如何為你的線上服務帳戶開啟兩步驟驗證

你可能會遇到的問題與狀況

兩步驟驗證最大的挑戰是，儘管想法和實踐都看似容易，但存在許多容易分散學員注意力的附帶問題。

- 在教學這個概念時，有很多系統的設計對於學員來說「像是」2FA，實則不然，像是帳戶恢復、密碼重置和安全性問答。
- 許多服務對於兩步驟驗證也使用不同的名稱，讓辨識及找到相關的設定變得困難。常見的包括「多因素身份驗證（Multi-Factor Authentication）」、「兩階段驗證（Two-step Authentication）」、「登入批准（Login Approvals）」。
- 線上服務可能會把開啟 2FA 的設定藏在深處，且每個的位置皆不一致。
- 2FA 可能會在一些情況失效而鎖住帳號，例如當手機不在你身邊時，你就無法

登入帳號。

- 有些 2FA 的實作方式無法保護你免受攻擊者的侵害，例如，當攻擊者掌握你的手機，而驗證碼又是透過手機簡訊傳送時。
- 2FA 的應用程式非常多樣且可以互相取代，因此沒有一個最「標準」或「正確」的選擇。

策略上，講師應盡量提供與學員有關的知識，不需太費心告知他們無法掌控的問題。例如：

- 指導學員該如何找到「兩步驟」的相關資訊，而不是學習操作某個特定的流程。
- 將 2FA 定調為「額外的小步驟」——它並非完美（畢竟幾乎所有 2FA 系統都有它的未竟之處），也不是絕對必要，但比起只使用密碼來說，還是有幫助。
- 引導學員了解他們可以在自己的線上帳戶開啟 2FA 的參考資源，例如 https://twofactorauth.org。

你不必談到所有 2FA 可能失效的情形（failure modes）。可以著重討論它減少了哪些危害，而非做不到的功能。

可預期的問題與解答

問題：「如何為『某線上服務』啟用兩步驟驗證？」

解答：「我們一起看看 https://twofactorauth.org/ ……」（依照培訓的結構，逐步指導學員或協助他們瞭解）

問題：「如果我旅行在外、弄丟手機或沒有兩步驟驗證的裝置怎麼辦？」

解答：如果你有電話但沒有收訊，你仍然可以使用身份驗證應用程式。另外，許多網站都可以讓你存下或列印出「備用驗證碼」。當你沒有手機或無法接收簡訊時，能使用這些備用碼取而代之。每個代碼僅供一次使用，無論是抄下、列印或是存在電腦裡，請將它們保存在安全的地方，以免弄丟或遺忘，否則他人可能有機會發現並用來盜用你的帳號。

問題：「我不喜歡每次都要這麼麻煩！」（技術上來說，這不是一個問題，但這是一個經常聽到的發言）

解答：你通常可以讓它「信任這台電腦」，隔一段時間後才重新要求一次，下次注意登入時旁邊的選項。

（譯註：CSCS 社群的立場是不建議這麼做，這會在電腦遺失或被盜用的時候產生風險。）

問題：「我聽說『某次資安事件』中駭客繞過了兩步驟驗證進行攻擊。」

解答：這可能是電話系統被入侵（透過 SS7 系統 劫持或攔截簡訊），也可能是攻擊者致電電信業者的客服並騙他們拿出簡訊。或者，帳號救援流程的安全性出了問題，並被用來繞過常規的登入系統。

如果你並不使用簡訊，而是兩步驟驗證 App 或是硬體 Token 裝置，那這些都不必擔心！

如果你確實使用簡訊，那也不需要過於擔憂。要使攻擊者成功繞過你的簡訊 2FA，他們必須知道你的密碼，以及花大量時間和精力針對你研擬攻擊策略。如果你擔心被攻擊的風險，那麼使用簡訊 2FA 可能就不適合你，但若你被針對攻擊的風險很小，那簡訊 2FA 應該都還稱得上安全。

請記住：沒有完美的資安手段，基於簡訊的 2FA 自然不例外。與其關注那些缺陷，不如考慮它的優勢跟劣勢，以及這些折衷對於具體情況有何影響。

問題：「為什麼服務不是只要求第兩個密碼，而要使用手機等等的方式？」

解答：跟學員說明這不符合「記在腦裡的 + 拿在手上的」的「兩步驟」結構，而且這樣同樣有密碼失竊的風險。

問題：「為什麼我應該相信 Google Authenticator 這樣的應用程式呢？我不希望他

們看到我的 2FA 驗證碼。」

解答：的確，理論上 Google 可以利用 Authenticator 取得你的驗證碼，但他們不太可能這麼做。這些公司設計 Authenticator 來加強他們服務的安全性，所以要是他們自己藉此動手腳，那也是破壞他們服務的安全性。再來，別忘了：只取得你的驗證碼也是不夠的，他們還需要你的密碼。網路上也存在一些開放原始碼（Open Source）的替代方案，因此要是你真的不想使用 Google Authenticator，也可以考慮這些開放原始碼的應用程式，比方說 FreeOTP 等等。

問題：「這類的驗證 App 是怎麼運作的？或者，TOTP（Time-based One-time Password，基於時間的動態密碼系統）是怎麼運作的？」

解答：這是一個很進階的問題，建議個別回答這樣的技術細節問題。可以推薦他們參考這個討論串：[Google身分驗證器是如何運作的？]

學習目標

學員將：

- 能夠找到他們使用的一個線上服務的兩步驟驗證設置頁面。
- 為其服務打開兩步驟驗證。

可以用一個討論形式的小講座來讓大家了解兩步驟驗證。

要找到每個線上服務的兩步驟驗證設定頁面可能需要費些力氣，因此如果有助教的話對培訓會很有幫助（一名助教協助五名學員）。

啟用兩步驟驗證的實作可能會需要一對一（或一對二）的教學。

建議閱讀

- 如何啟用兩步驟驗證
- 哪些網頁服務支持2FA
- 網路上常見的兩步驟驗證指南
- 12 天上手 2FA，如何為你的線上服務帳戶開啟兩步驟驗證

課程內容

活動：打開 2FA

帶學員閱讀「12 天上手 2FA」網頁。

學員應該能從列表中選擇一個帳戶，並透過網頁指導為該帳戶開啟 2FA。如果他們沒有該頁面上列出的服務/平台帳戶，則可以依照他們有使用的帳戶，指導他們打開兩步驟驗證。

收尾活動（非強制）

進行一個兩步驟驗證大冒險！登入 Facebook 或其他線上服務，讓學員嘗試在上面找到 2FA 的選項。

社群媒體防護－初階

如何安全又自在地使用社群媒體，對許多學員而言是個挑戰。在此課程中，我們將會分享一些在使用及設定社群媒體時應注意的基本觀念。

推薦閱讀

- SSD 的〈在社群網站上保護自己〉英文版，中文版
- Hack*Blossom

你可能會遇到的問題與狀況

不同的平臺：網路上有數不清的社群媒體平臺，你的學員們可能使用了很多種。如果可以的話，試著在課前調查一下他們使用什麼社群媒體平臺。根據你對學員的瞭解，在課前自己複習一下主流平臺的安全性及隱私設定（Facebook、Twitter、Instagram，和 LinkedIn 等）。如果你有時間，且覺得學員會有興趣的話，不妨也參考一下線上約會網站（例如 OKCupid、Tinder 和 Bumble）。這些預備知識能幫助你應對不可預期的問題和疑難雜症！

敏感資訊與身份：有時候，人們會因為經歷可怕的騷擾、人肉搜索、跟蹤，或因為朋友遭遇這些事情，而想加強社群媒體上的安全性防護。這些經歷可能令人難以啓齒，且可能使人焦慮及擔憂。請謹記，社群媒體平臺就像其他環境一樣，可能充斥各種風險，情況因性別、種族或性傾向而異。女性、有色人種，及 LGBTQ 族群是在網路上遭受最多騷擾的一群人。其他重要的事包括定位的隱私、分享電話號碼的風險、維持多重帳號及身份，及線上約會的安全性及隱私。

夥伴制度：得知自己有多少個人資訊出現網路上可能是一件令人畏懼的事。許多人與其面對這痛苦的過程，寧願不知道自己在線上公開了多少資訊。如果可以，鼓勵學員

帶一位信任的朋友或家人一起參加工作坊。知道自己的電話號碼一直公開在網路上，或發現自己以為未公開的照片公開在網路上，可能是很大的刺激，如果有人在旁支持，會比較不那麼難受。

可預期的問題與解答

當你要求學員思考他們要在社群媒體保護的內容時，他們可能會陷入「反正沒有任何一項資安防護措施是完美的，我們應該乾脆放棄」（security paralysis / security nihilism）的狀態。有人可能會說：「你不可能將所有內容都封鎖。我不知道該從哪開始著手，甚至完全想不到下一步可以做什麼。」或「掙扎到底有什麼意義呢？隱私設定可能會改動，資訊會洩漏，這一切都在我掌控之外。」

一個好的回答是「調整目標」。無論在電話簿時代或是社群媒體時代，要讓個資滴水不漏都是不切實際的。網路上也有許多資訊不在我們的掌握之中，但沒有關係。我們的目標並不是要在網路上徹底移除我們的資訊，而是將重要資訊的外洩最小化。任務是儘可能瞭解自己在暴露在網路上的資訊，然後根據我們的關心及擔憂來減少這些資訊。如果我們能將可以控制的公開資訊最小化，那麼當環境改變或我們出了小差錯時，我們將會處於更有力的位置。

學習目標

學員將：

- 能夠指出他們想要在社群媒體上保護哪些資訊，而不讓哪些人看見
- 知道該怎麼在各種常用的社群媒體平臺上調整隱私設定
- 概略地說明他們為了保護個人資訊需要做出哪些改變
- 能夠解釋為何他們會想維持不同平臺上的帳號彼此獨立

師生比例

講師：學員 ＝ 1：5（一位講師對五位學員）

理想的師生比至少要 1：5。雖然這部分不需要指導學員安裝工具，但是會有很多個人疑問及個人威脅建模考量。可考慮將處境或擔憂相近的學員分到同一組。

課程內容

破冰

「如果你今天用過一次社群媒體平臺，請舉手。兩次的呢？三次的呢？」希望這會引起一些笑聲，並明確傳達社群媒體平臺對人們的日常生活是不可或缺的。

暖身

請學員分成幾對或幾組，討論他們最喜歡的社群媒體用途。例如：分享圖片、舉辦活動、與遠方的親友保持聯繫、參加線上社群、宣傳他們的藝術／工作／社會運動等等。

知識分享

認識這麼多的社群媒體平臺，和了解這麼多種不同的設定，可能會使學員（甚至你！）不知所措。在深入講解如何設定和各種問題的核心之前，請務必講解適用於所有平臺或設定的基本概念。這可能包括：

什麼是個人可識別資訊（PII）？

PII，有時也被稱為「敏感個人資訊（Sensitive Personal Information）」或「潛在可識別資訊（Potentially Identifying Information）」是可被用於識別個人的資訊。PII 與其他資訊結合在一起就可以找出某人的所在位置，以聯繫他們或蒐集更多關於此人生活的資訊。許多公司出於廣告投放、醫療文件，或帳單等各種目的蒐集這種資訊。雖然很難控制公司蒐集個人資訊和資料，學員仍可以控制他們在社群媒體上公開呈現的資訊。

「別自責」

有時，當學員開始學著了解他們想要在社群媒體上保護哪些內容時，他們會感到尷尬或丟臉。他們可能會覺得之前在隱私內容保護上的大意，或是之前在不自覺中與別人分享過多個人資訊是個嚴重的錯誤。作為講師，你可以向他們保證這不是他們的錯。你可以說：「我不希望你將大科技公司和社群媒體平台對你的隱私所做的事情，歸咎於自己。」相反地，你可以幫助他們採取小而有力的行動來保障自己的隱私。

安全及隱私檢核表

Facebook、Google 和其他主要網站有提供「安全檢核表」功能。這些教學指南以簡單的語言帶你認識常見的隱私和安全設定，可以善加利用。

隱私 vs. 安全性；安全性 vs. 帳號設定

即使每個社群媒體平臺都有各自的設定方式，你仍然可以找到一些相似的模式。

隱私設定通常會回答以下的問題：「誰可以看到什麼？」這裡你可能會找到關於受眾的設定（「公開」、「朋友的朋友」、「僅限朋友」等）、位置、照片、聯絡資訊、被標註的內容，以及人們是否可以搜尋到你的個人檔案。

安全性設定通常跟封鎖／取消追蹤其他帳號比較相關，以及當未經授權的裝置登入你的帳號時，你是否會收到通知。有時你會在這個區塊找到登入設定——例如兩步驟驗證，及備援 email／電話號碼；有時這些設定則會在「帳號設定」或「登入設定」區，並且有更改密碼的選項。

定位

定位設定可以幫助你避免不小心分享自己的所在位置。有些服務會在你貼文時，預設分享你的大約位置。定位資訊可以詳細描繪你的生活習慣、住處和工作地點；因此，如果洩漏資訊令你感到不安，請務必將其關閉。

照片

照片揭露的資訊遠遠比表面上看起來得多。除了後設資料可能包含拍攝時間和地點之外，圖像本身也可能提供更多資訊。當你要發佈圖片之前，先問自己：這是在住家或工作場所之外的地方拍的嗎？照片中看得到任何門牌或路標嗎？如果你經常在每天的固定時間發佈照片，會不會暴露你的生活習慣？

照片也可能連結你打算分開使用的帳號。這是履歷和約會網站上一個驚人的常見問題，如果你想要保持匿名性，或將某個帳號的身份與其他帳號分開，請確保使用的是你完全沒在其他地方用過的照片。要檢查這點，你可以使用 Google 的逆向圖片搜尋功能。

確保不同帳號並不互相連結

對許多人而言，區隔不同的帳號是非常重要的。這可適用於約會網站、履歷網站、匿名帳號和各種社群帳號中。除了電話號碼和圖片之外，其他需要留意的潛在連結因素包括你的姓名（包括暱稱）和 email。如果你發現其中一條資訊出現在你預期之外的地方，則很容易感到恐慌。這時要一步一步慢慢來，與其試著從整個網際網路上抹除所有你的相關資訊，不如只關注特定資訊：這些資訊在哪，以及你可以做些什麼。

社團設定

Facebook 社團漸漸成為社交活動、倡議行動和其他敏感活動的場所，而社團設定可能令人困惑。如果學員想瞭解更多關於社團設定的資訊，請他們參考這份指南。

如何安裝 Signal－初階

讓學員開始使用即時通訊軟體 Signal。我們會先簡單討論為何需要保護通訊紀錄的原因和作法，然後再討論安裝和使用 Signal 的細節。

推薦閱讀

- 如何在 iOS 上使用 Signal（中文）
- 如何在 Android 上使用 Signal（中文）
- 不同加密方式
- 資安自我防禦字彙表
- Signal 支援中心

你可能會遇到的問題與狀況

- 有時，新聯絡人要稍等一下才會顯示在的 Signal 聯絡人列表上，或者必須更新 Signal 聯絡人列表。在培訓中務必記住這點。考慮讓學員在培訓一開始就先和課堂夥伴交換電話號碼。

- 和安裝其他工具一樣，你可能會遇到連線問題。可以考慮架設自己的無線網路，讓其他人使用。

- 培訓中，有些學員可能不願意和其他學員交換電話號碼，或者不願意使用個人電話號碼註冊 Signal。下面的文章可以協助你處理這種情況：

    - 如何在不提供電話號碼的情況下使用 Signal？ 作者：Jillian York
    - 不用你的電話號碼使用 Signal 作者：Martin Shelton
    - 如何在不提供電話號碼的情況下使用 Signal？ 作者：Micah Lee

- Signal 保護你的通訊，但不能防止他人閱讀你的訊息或惡意程式擷取你的訊息。需要跟學員強調，Signal 並不是對付所有威脅的萬靈藥。

- 有時學員沒有足夠的儲存空間來安裝 Signal 。可以讓學員在這堂課前想想他們有哪些應用程式是不必要的。

可預期的問題與解答

問題：「如果我不想讓 Signal 存取我的聯絡人呢？」

解答：Signal 有一種很酷的功能叫做「搜尋聯絡人」，讓你能在不向 Signal 服務透露聯絡人的情況下，確定手機裡的聯絡人是不是 Signal 使用者。想了解詳情的人可以到 Signal 的部落格文章了解這項功能，不過有不少技術本質的細節。

問題：「如果 Signal 這麼安全，那幹嘛要記錄我所有訊息？」

解答： Signal 有個功能叫做「銷毀訊息」，可以確保對方看到訊息後一段時間內，從雙方裝置中刪除。若要啟用通訊的「銷毀訊息」，請打開向連絡人發送訊息的介面，然後點擊螢幕上方的聯絡人姓名，然後點開「銷毀訊息」的選項。

問題：「那 WhatsApp 呢？我所有朋友都在用。」

解答：我們目前不建議用 WhatsApp 進行安全通訊，但我們知道國際上有很多人在使用。來看看我們的 Android 和 iOS 的 WhatsApp 指南。

問題：「如果我在手機上安裝了端到端加密應用程式，會變成攻擊目標嗎？」

解答： 在某些國家，使用 Signal 或其他端到端加密的訊息程式確實可能成為執法機關、政府當局或其他網路監控人員的危險信號。如果你會擔心這個問題，那麼 Signal 大概不是適合你的選擇。

問題：「我要怎麼讓朋友使用這個應用程式？我朋友好像都不關心通訊安全，他們都覺得沒什麼好隱瞞的。」

解答：建議的回答方式包含，可以詢問要不要幫他們安裝這個應用程式，告訴他們 Signal 是聯絡你的最佳 (或唯一！)方式，並告訴他們 Signal 免費，可以跨國使用。

學習目標

課程結束後，學員將：

- 明白為什麼需要保護自己的通訊。
- 了解什麼是後設資料，以及 Signal 會蒐集哪些資料。
- 在手機上安裝 Signal 。
- 透過與夥伴或老師驗證安全號碼，展現對安全號碼的理解。
- 寄送加密訊息給夥伴或老師。

先備知識

- 學員都知道什麼是端到端加密通訊。
- 大家可以投入至少 1.5 小時在這個課程。

師生比例

講師：學員＝1:5 (一名講師指導五名學生)

課程內容

破冰活動

問大家：「小時候有沒有用過祕密語言或密碼和朋友傳訊息？」

邀請學員描述經驗，包括自創語言、其他密碼、檸檬汁墨水、其他隱形墨水等。

暖身運動

問大家：「為什麼有人想保護自己的通訊內容？哪些團體或個人可能會想保護自己的通訊，不受電話公司、執法機關、政府部門等的干涉？」

答案可能包括：

- 記者
- 律師
- 人權捍衛者、行動者、持不同政見的人
- LGBTQ 的年輕人
- 學術研究者

接著問：「怎樣才能進一步保護自己的數位通訊」

聽完大家的想法，然後將討論引向端到端加密通訊。學員應該之前已經上過端到端的課程，這就當作稍微複習。

分享知識：介紹 Signal

介紹主題：「Signal 是用端到端加密通訊的工具之一，今天我們將學習如何在手機上下載這個應用程式。」

藉此機會和學員一起回顧學習目標，並分享以下幾點：

- Signal 是一款由 Open Whisper Systems 開發的免費開源應用程式，在 iOS、Android 和桌機都採用了端到端的加密方式。
- Signal 使用電話號碼做為聯絡資料，可以在使用數據或 WiFi 的 Signal 使用者之間發送端到端的加密通話、訊息、視訊電話和檔案。這意味著用戶不需要支付簡訊和多媒體簡訊費用，但參與對話的雙方的行動裝置都必須連上網。
- 如果你下載了程式並允許程式存取聯絡人，你可能會驚訝地發現有些朋友已經在用了。
- 這個程式比一般的電話和簡訊更安全。
- 如果你在一個監控人民通訊的國家，政府可能會尋找 Signal 流量。如果你對此感到擔憂，可以和你信任的同事和倡議者聊聊，查一下相關的新聞。
- Signal 的隱私政策簡明扼要，和 WhatsApp 不同，Signal 不儲存任何後設資料。(說到這裡請暫停，向學員解釋後設資料)。 Signal 伺服器所儲存的與後設資料最接近的資訊，是使用者連接到伺服器的最後一次時間，而且該資訊的單位只剩下天，而不是小時、分鐘或秒。

問問學員目前為止有沒有問題要發問。

安裝

1. 把班級分成幾個小組 (一組最多五人)，告訴他們接下來要逐步安裝。如果可能，讓 Android 用戶分在同一組， iOS 使用者分在另一組。

   提示：使用安裝卡。給使用者一張綠卡、一張黃卡和一張紅卡。如果他們完成了一個步驟且無須協助，就放綠卡；如果他們正在進行某步驟，就放黃卡；如果他們遇到問題，就放紅卡。

2. 提示學員前往 Google Play Store 或 Apple App Store，搜尋「Signal」，並下載應用程式。然後等一下，確認所有人都成功安裝再繼續。

3. 請見 如何在 iOS 上使用 Signal 和 如何在 Android 上使用 Signal 繼續安裝程式。每個步驟都要暫停一下，確保所有人都完成步驟。接著在「使用 Signal」前暫停。

知識分享：指紋和安全碼

介紹主題時開頭先說：「在透過應用程式傳訊息前，要先驗證收訊者的身分。」

提醒學生端到端加密通訊主題中的「指紋驗證」的部分。如果有必要，可用一個活動或投影片複習此概念。

端到端加密的應用程式通常有方法可以驗證你朋友的身份。提醒一下，指紋是你的加密金鑰的簡短數學表徵 (mathematical representation)，看起來像是亂碼。你可以使用指紋來驗證你正在和正確對象通訊，且你的消息未遭篡改。

Signal 使用的是「安全碼」稍微不同。Signal 的安全碼是你和你的收件者之間對話的數學表徵 (一半是你的公共金鑰，另一半是他們的)。安全碼的每一半都是永久的，直到持有者重新安裝 Signal (會建立新密碼身分)。

安全碼這種方式相當強大，可以檢查你和朋友通訊的安全性，並防止所謂的「中間人攻擊」或「中間機器攻擊」。不過，要知道安全碼也會因為某些原因而改變，譬如你的聯絡人買了一個新手機、重新安裝 Signal 或將 Signal 轉移到新裝置上。

如果你知道你要換新電話，可以事先通知朋友，你要改安全碼了。有幾種方法可以做到：買新手機前發訊息，在 http 加密的網站上發佈公告、親自告訴他們等。這樣他們就不會對裝置資訊變更了感到意外。

進行下一個活動前，先暫停一下。告訴學員，休息結束後要和夥伴 (或講師) 驗證安全碼。講師要準備好回答問題。

活動：驗證安全碼

讓學員找一個夥伴交換電話號碼。老師或助手可以和那些不想把電話號碼給陌生人的人一組。確定你的電話號碼或拋棄式電話號碼可在台上或投影機上出現。

訣竅：使用安裝卡。

1. 讓學員與夥伴交換號碼。大家應該在自己的手機中建立一名新聯絡人，並在聯絡人列表輸入對方的電話號碼。
   停下來檢查，確保所有人都順利新增聯絡人。

2. 在「如何在 iOS 上使用 Signal」和「如何在 Android 上使用 Signal」指南中，查看「如何驗證聯絡人」下的說明。在每次完成步驟之後都暫停一會，確保所有人都完成了步驟。在「使用 Signal」章節之前停下來。

   如果是進階學員：不介意和他人交換安全碼的學員，可以在教室找其他人交換安全碼，而講師則幫助有困難的學員。

3. 請成功和他人驗證安全碼的學員出示綠卡。

4. 所有人都完成後，就把大家集合起來。

問一下學員目前為止有沒有任何問題。

活動：傳送端到端加密訊息

介紹下一個活動時，可以說：「現在大家都已經驗證通訊對象的身分了，可以傳送端到端加密訊息了。」讓學員找到自己的夥伴。(備註：在某些情況下，夥伴可能是老師或助手。)

訣竅：使用安裝卡並參考 Signal 指南的「如何發送加密訊息」。

1. 叫所有人開啟手機訊號，點擊螢幕右上角的合成圖示。
   暫停一下，確認所有人都有找到。

2. 在 Signal 指南的「如何發送加密訊息」中，逐步完成指示。

3. 學員順利傳送加密訊息時，請他們出示綠卡。

結尾活動（非強制）

讓學員寫下三個他在培訓後有意願協助安裝 Signal 的聯繫對象。

如何安裝 Signal－進階

讓學員開始使用即時通訊軟體 Signal。我們會先簡單討論為何需要保護通訊紀錄的原因和作法，然後再討論安裝和使用 Signal 的細節。

推薦閱讀

- 如何在 iOS 上使用 Signal（中文）
- 如何在 Android 上使用 Signal（中文）
- 不同加密方式
- 資安自我防禦字彙表
- Signal 支援中心

你可能會遇到的問題與狀況

- 有時，新聯絡人要稍等一下才會顯示在的 Signal 聯絡人列表上，或者必須更新 Signal 聯絡人列表。在培訓中務必記住這點。考慮讓學員在培訓一開始就先和課堂夥伴交換電話號碼。

- 和安裝其他工具一樣，你可能會遇到連線問題。可以考慮架設自己的無線網路，讓其他人使用。

- 培訓中，有些學員可能不願意和其他學員交換電話號碼，或者不願意使用個人電話號碼註冊 Signal。下面的文章可以協助你處理這種情況：

    - 如何在不提供電話號碼的情況下使用 Signal？ 作者：Jillian York
    - 不用你的電話號碼使用 Signal 作者：Martin Shelton
    - 如何在不提供電話號碼的情況下使用 Signal？ 作者：Micah Lee

- Signal 保護你的通訊，但不能防止他人閱讀你的訊息或惡意程式擷取你的訊息。需要跟學員強調，Signal 並不是對付所有威脅的萬靈藥。

- 有時學員沒有足夠的儲存空間來安裝 Signal 。可以讓學員在這堂課前想想他們有哪些應用程式是不必要的。

可預期的問題與解答

問題：「如果我不想讓 Signal 存取我的聯絡人呢？」

解答：Signal 有一種很酷的功能叫做「搜尋聯絡人」，讓你能在不向 Signal 服務透露聯絡人的情況下，確定手機裡的聯絡人是不是 Signal 使用者。想了解詳情的人可以到 Signal 的部落格文章了解這項功能，不過有不少技術本質的細節。

問題：「如果 Signal 這麼安全，那幹嘛要記錄我所有訊息？」

解答： Signal 有個功能叫做「銷毀訊息」，可以確保對方看到訊息後一段時間內，從雙方裝置中刪除。若要啟用通訊的「銷毀訊息」，請打開向連絡人發送訊息的介面，然後點擊螢幕上方的聯絡人姓名，然後點開「銷毀訊息」的選項。

問題：「那 WhatsApp 呢？我所有朋友都在用。」

解答：我們目前不建議用 WhatsApp 進行安全通訊，但我們知道國際上有很多人在使用。來看看我們的 Android 和 iOS 的 WhatsApp 指南。

問題：「如果我在手機上安裝了端到端加密應用程式，會變成攻擊目標嗎？」

解答： 在某些國家，使用 Signal 或其他端到端加密的訊息程式確實可能成為執法機關、政府當局或其他網路監控人員的危險信號。如果你會擔心這個問題，那麼 Signal 大概不是適合你的選擇。

問題：「我要怎麼讓朋友使用這個應用程式？我朋友好像都不關心通訊安全，他們都覺得沒什麼好隱瞞的。」

解答：建議的回答方式包含，可以詢問要不要幫他們安裝這個應用程式，告訴他們 Signal 是聯絡你的最佳 (或唯一！)方式，並告訴他們 Signal 免費，可以跨國使用。

學習目標

課程結束後，學員將：

- 打一通端到端加密電話。
- 打一通端到端加密視訊電話。

先備知識

學員已經完成此課程的初階部分。

師生比例

講師：學員＝1:5 (一名講師指導五名學生)

課程內容

能輕易向夥伴傳送端到端加密訊息的學員，可以開始嘗試進行端到端加密通話。如果這項任務也能輕鬆完成，就讓他們建立一個加密的群組，和教室裡的另一組夥伴聊天。

活動：撥打端到端加密電話

1. 叫所有人開啟手機訊號，點選一個聯絡人。(如果學員不認識任何使用 Signal 的人，講師可以提供他們自己的電話號碼或為本培訓所設的虛擬電話。)

2. 按照「如何撥打加密電話」的逐步說明進行操作。

3. 學員順利打給朋友或講師後，請他們拿出綠卡。

活動：撥打端到端加密視訊電話（非強制）

所有人互相打完電話後，指出通話螢幕上的視訊通話鈕。(更多螢幕截圖等細節，請參閱「如何撥打加密電話」。)

問問學員目前為止有沒有問題。

結尾活動（非強制）

讓學員寫下三個他在培訓後有意願協助安裝 Signal 的聯繫對象。

釣魚與惡意軟體－初階

學員們最常在線上面臨的威脅是偽裝過的連結和檔案——亦即網路釣魚和惡意軟體。要防禦這些狡猾的駭客策略，並不只是下載新工具或軟體，而應該多培養學員的危機意識和理解力。

推薦閱讀

- 如何避免釣魚攻擊？
  最佳實踐綜合指南

- 動畫概述：保護你的設備，免於駭客攻擊
  解釋惡意程式的短動畫（約兩分半鐘）——惡意程式會怎麼做，如何從電郵、隨身碟和線上連結感染惡意程式。

- 如何保護自己免於惡意程式攻擊？
  更多針對國家等級攻擊者的防範保護措施。有針對敏感目標的釣魚信件案例。

- 數位援救工具包
  如果你懷疑被釣魚攻擊了，你該怎麼做。

- PBS's 的資安遊戲有一個辨識釣魚的小測驗，及其他有用的指南。
  Social Engineering Challenge

可預期的問題與解答

問題：「最好的防毒軟體是什麼？」

解答：我們傾向於使用系統內建的防毒軟體（Windows Defender、蘋果的內建系統）。跟學員討論寫壞的防毒軟體可能會使情況更糟，並且無法提供解決方案。

問題：「如果你認為自己的裝置可能被感染，應該怎麼辦？」

解答：你可以參閱 Digital Defenders 的急救指南。定期備份很重要，以防你的設備被感染。將手機資料刪除（或「恢復原廠設定」）也很重要。你可以在這裡查閱更多：[數位援救工具包]

問題：「我們總是會使用附件檔案的功能，這是在告訴我，我不能再傳送或接收檔案了嗎？」

解答：建議使用一個共享的空間來存放頻繁使用的文件，像 Dropbox 或 Google Drive。我們在這裡說一下 EFF 自己的做法——我們寄送文件，但我們會數位簽署自己的訊息，並鼓勵外部單位將檔案上傳到我們可以安全檢查的地方。你也可以強調，這不是一個全有全無的提議。你當然可以傳送和接收文件——而當你這麼做時，要練習建立有無異狀的基本知識，判斷可能是釣魚或惡意程式的跡象。

問題：「如何檢舉網路釣魚？」

解答：強調大規模網路釣魚（例如垃圾郵件）和魚叉式網路釣魚（spear-phishing）之間的區別。研究人員通常樂意幫忙辨別對弱勢群體進行的魚叉式釣魚，且樂意協助預防。你可以寄送電子郵件至 EFF，地址為 info@eff.org，或者聯繫 Access Now 的資訊安全熱線（help@accessnow.org）尋求幫助。另外，美國聯邦貿易委員會也收集了大規模網路釣魚的案例，你可以轉寄釣魚信至 spam@uce.gov，FTC 的網路釣魚頁面說明了你在轉寄信件中應該包含哪些資訊。

問題：「我擔心自己感染了惡意軟體。你能檢查一下嗎？」

解答：惡意軟體並沒有一定或明顯的跡象；例如，電腦變慢或電池消耗得很快，有很多其他的可能的原因。學員很有可能因為打開了垃圾郵件或因為常規的網路釣魚而感染了病毒，你可以建議他們安裝防毒軟體來檢查這種可能性。對於大多數社群而言，面臨來自政府或其他大型集團的針對性攻擊的可能性相對較小。如果想讓提問者放心，你可以談論一下，要寄送具有針對性的釣魚信件所花費的人力和研發成本。

學習目標

學員將：

- 能描述釣魚是什麼
- 瞭解他們為何可能成為釣魚的目標
- 能夠給出一些防範釣魚的策略

師生比例

講師：學員＝1：10（一位講師對十位學員）

課程內容

暖身

讓人們談談他們曾看過的聳動垃圾郵件標題。 可以讓他們檢查垃圾信件夾（如果他們知道在哪裡的話），或者你可以引用一些你看過的內容。

如果你需要建議，試著搜尋：「Busted: The Worst Email Subject Lines Ever!」及「19 Terrible Email Subject Lines」

還可以追問其他問題：

- 「你只在 email 收過這種垃圾訊息嗎？有沒有在電話或簡訊收過垃圾訊息？」
- 「垃圾信件的目的是要你做些什麼？」（可能的答案：買東西、匯款、交出信用卡資訊、被詐騙等）
- 「如果有人試著誘導你點擊某個連結，他們會怎麼做？」

另外，請學員嘗試撰寫要寄送給其他組員的電子郵件，以說服他們點擊連結。（這對於熟悉或樂於共享資訊的小組來說是最好的。否則，請以名人或假想的人作為收件者。）

提出一些問題後，你可以按照以下內容進行快速說明：「網路釣魚是垃圾郵件的一種，因為它是為了從你身上獲取資訊在試圖使你有所作為。魚叉式釣魚是針對你或你的組織進行攻擊。其他類型的危險垃圾郵件會試圖誘騙你下載監視你的程式，或綁架你的檔案來進行勒索。」

知識分享

網路釣魚是一個容易使人過度擔憂或引起隱私虛無主義（privacy nihilism）的議題。你希望人們思考攻擊者如何欺騙他們的方法，但不要讓學員誤以為沒有人可以信任，或者沒有辦法防範網路釣魚電子郵件。切記：用令人信服的電子郵件警示學員後，請提供解決方案。這可能包括以下方法：檢查標題、如何進行帶外確認（指使用獨立管理通道進行裝置維護）、在 Google 文件中打開檔案以及啟用兩步驟驗證等。

我們建議把焦點從垃圾郵件轉移到網路釣魚攻擊，因為人們經常覺得被垃圾郵件欺騙很可笑。你可以根據學員的擔心程度，將學員對魚叉式釣魚的看法從「超級恐怖的駭客技術」轉變為「可能沒用」。

通常，人們沒辦法區分程式是不是在自己的設備上執行，並且可能無法識別不同類型的檔案。他們熟悉閱讀訊息，並對訊息中的要求採取行動。建議講師著重提升閱讀訊息時的警覺性，並提供學員確實可行的保護措施，而不是著眼於哪些特定的動作是危險的而哪些不是危險的。（例如，不是「不要打開 PDF 和 Word 檔案，而是說：「當電子郵件要求你點擊某些內容時，請三思。」）

釣魚的關鍵基礎點之一是身份驗證——你如何知道自己正在與誰談話？你如何知道電子郵件的寄件人是誰？這封奇怪的電子郵件真的來自我的同事嗎？這可疑的警示真的是我的銀行發出的嗎？魚叉式網路釣魚的解決方案通常是低技術含量的——用電話打給對方確認、找出他們平常不會用的用語習慣、自己前往銀行或組織的網站，而不是點擊信件中的內容等。

一旦建立觀念，你就可以將「知道自己在與誰交談」的重要性，應用於其他更嚴格的資安概念，例如網站憑證和簽名。

注意！ 人們可能會對難以接受自己受騙的想法，或者反駁他們可能曾經受騙的想法。除非你對學員的界限非常了解，否則請勿嘗試對受眾群體開玩笑，也不要利用私人的知識來構造網路釣魚郵件。

如果有的話，分享個人經驗也很有幫助，或者通常可以強調「任何人都可能發生這種情況！」。說法可以是「儘管不是特別高科技，但這些釣魚信可能確實十分狡猾。 信不信由你，幾年前，我點擊了以為是美國銀行寄來的一封信，然後迅速意識到自己做了什麼，並要求取消並重辦一張新卡！」

如果人們感到尷尬或難為情，會降低他們求助或採取行動的意願。 你可以用以下方式回應此問題：「不要吝於用嚴格的眼光看待陌生的電子郵件，也別害羞於打電話給朋友去確保他們真的寄了郵件。」

如果有人聲稱他們永遠不會被電子郵件欺騙，那就不要挑戰他們的說法。教室裡的其他人有可能早就習慣了他們的態度，而且他們會因為堅信自己不會被愚弄，而學不到任何東西。將注意力轉移到在乎這件事的學員身上。（「你似乎很會防範網路釣魚！不過如果有一個你認識的人不小心點擊了附件，那麼你的個資就可能會從他們的帳號洩漏。你想教他們什麼？」）

端到端加密通訊：手機應用程式－初階

協助你的學員建立基本的概念，理解端到端加密會如何保護他們的通訊。這節課，我們將從「私密通訊」和「加密」開始探索，然後深入了解端到端加密的基礎知識 (和限制！)。這堂課之後，學員應有更完善的知識來學習如何選擇、安裝和使用端到端加密訊息應用程式。

建議閱讀

- 如何在 Android 上和 iOS 上使用 Signal。
- 如何在 Android 上和 iOS 上使用 WhatsApp
- 和其他人聯繫。

你可能會遇到的問題與狀況

- 如果學員沒有行動裝置怎麼辦？
- 如果學員沒有自己的行動裝置，或者擔心裝置內已經有惡意軟體怎麼辦？
- 如果學員不想提供電話號碼怎麼辦？有沒有備用方案或是他們可以用於練習用的電話號碼？
- 課堂上的學員覺得尷尬時怎麼辦？如果大家彼此不認識怎麼辦？

可預期的問題與解答

問題：「為什麼你推薦這些應用程式，而不是推薦 [其他應用程式]？」

解答：講師應該參考這篇 EFF 如何選擇工具的文章。

預設情況下，工具都是端到端加密的，而且一律免費，可以在 Android 和 IOS 手機上使用。

這些應用程式還具有強大的安全功能。Signal、WhatsApp 和 Wire 等應用程式都使用了一種名為 forward secrecy 的技術。簡單說就是，應用程式用一組新的加密金鑰加密每條訊息，這樣可以保護過去進行的通訊不受密碼或密鑰在未來暴露的威脅。這與端到端加密電子郵件不同；在端到端加密電子郵件中，加密金鑰會無限期保留在使用者手中，直到使用者選擇生成新的金鑰 (可能是幾年後)。如果有攻擊者得到了他們的私人金鑰，那麼這個攻擊者就可以解密之前發送的所有訊息。

（譯註：forward secrecy 每則訊息都產生不同金鑰，端到端加密則是每個用戶端產生一把金鑰，前者更頻繁更換金鑰所以比較安全。）

問題：「WhatsApp 不是 Facebook 旗下的嗎？這代表什麼？」

解答：是的。WhatsApp 最初承諾不會和 Facebook 分享資訊，後來又改變了立場。WhatsApp 仍然是端到端加密，但他們和 Facebook 分享後設資料（metadata），譬如誰在聯絡誰。不過，WhatsApp 的一個好處是它是一款主流應用程式，這意味著你的朋友和聯絡人很有可能都會使用。要瞭解更多 EFF 關於 Whatsapp 的資料，請參閱 SSD 指南，瞭解如何在 Android 和 iOS 上使用 Whatsapp。

問題：「那如果我想匿名通訊呢？」

解答：這又是另一種不同的擔憂，這可不僅是想保持通訊內容的隱私。你是否不想和你聊天的對象有所連結？這可能對記者和消息來源、吹哨者等聯繫很重要。和敏感人士聯繫的後設資料有不同的風險和考量。我們提及的工具都不提供匿名通訊。

如果你會擔心匿名問題，我們可以在工作坊結束後討論。

問題：「Signal 真的沒有保留這些資訊嗎？你怎麼知道？」

解答：請參考 2016 年 的大陪審團傳票：
(https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/)

不過他們應該也知道，如果 Signal 收到美國法院的命令，他們會被迫蒐集這類資訊。

問題：「我聽說有人可以駭進 Signal，真的嗎？」

解答：不可能。對 Signal 最有效的破解方法是你裝置上的惡意軟體。你若下載到惡意檔案或點擊釣魚連結，惡意軟體可以感染你的裝置。如果端點 (即設備) 被惡意軟體破壞，沒有端到端加密工具可以保護你的訊息。這並不表示該工具提供的端到端加密沒有用——只是能力有限。

問題：「那如果我不想用真實的手機號碼呢？」

解答：你有幾個選擇。你可以用 Wire 這個軟體，或者如果你在美國，你可以用 Google Voice 電話號碼或 Twilio 電話號碼進行匿名通訊。你也可以更換 SIM 卡。

學習目標

課程結束後，學員將：

- 能明白「私密通訊」代表什麼。
- 熟悉加密這個概念。
- 有能力解釋為什麼通訊者不信任第三方和公司等媒介時，端到端加密是有用的。
- 知道在哪裡可以找到更多端到端加密通訊的資訊，並下載相關的應用程式，如 Signal。
- 能辨識簡訊是不安全的通訊方式。

先備知識

- 如果要安裝程式，學員必須攜帶行動裝置。
- 講師已對這個群組進行威脅建模分析。

師生比例

講師：學員＝1：5 (一名講師指導五名學生)

建議教材

- 投影機
- 如要安裝應用程式，學員應攜帶自己的智慧型手機。

課程內容

暖身活動

講師將學員分為兩組。

講師：「請用你喜歡的名字向旁邊的同學介紹自己。然後我希望你們在接下來的五分鐘內解決下列問題。歡迎大膽運用想像力，在五分鐘內盡可能想出最多的主意。」

對第一組說：「你們這組負責通訊。假設你要傳一則秘密訊息給朋友，你不介意別人知道你和朋友在通訊，但你要確保資訊的內容不會外流。你會怎麼做？」

對第二組說：「你們這組負責攔截。你們要試圖攔截第一組要寄送的秘密訊息。你們非常想要那則秘密資訊。那你們可以採取什麼選擇，或用什麼能力來戰勝他們的聰明才智？」

「比賽開始！」

講師可以鼓勵他們回答時想法大膽一點。譬如第一組的學員可以這麼說：「把用隱形墨水寫的紙條摺好傳出去、傳送簡訊文字訊息、使用冷門遊戲的聊天頻道聊天、親自跑去和朋友在秘密地點見面來傳遞紙條、用只有自己和朋友知道的自創語言書寫、使用加密訊息應用程式等。」

第二組的學員可能說：他們想像自己是政府，有各種能力和資源，如律師、系統管理員、執法人員和情報組織。他們可以雇人協助他們破解資訊或在裝置上安裝惡意軟體。或者，他們可以想像自己是技術嫻熟的駭客團隊。又或者，他們可能是行動電話公司，可以攔截簡訊。他們的目標是要能夠想出各種想獲取訊息的角色。

五分鐘結束後，提出下列問題。根據學員的回答，講師可以花五分鐘讓兩組檢閱各個答案。

- 使用隱形墨水有什麼優點？如果有人發現紙條是用隱形墨水寫的，有人能破解嗎？
- 傳簡訊有什麼優點？有人能破解這招嗎？破解方法容易嗎？
- 在秘密地點見面有什麼優點？有人知道你們在哪裡見面嗎？這個方法容易嗎？
- 使用冷門工具，譬如遊戲的聊天系統，有什麼優點？其他人會知道你們在哪裡見面嗎，還是他們不太可能會去看？
- 用自創語言書寫有什麼優點？有人能破解自創語言嗎？自創語言被解譯出來後又會發生什麼情況？

對於什麼安全、什麼不安全，會根據學員的觀點而異。

講師可以討論：「有人提出使用加密嗎？大家知道哪些加密的例子？我們可以用加密做些什麼？」

講師可以等待學員回答，並引導他們做出下列解釋：「我們可以將訊息加密轉換成無意義的亂碼，然後再轉換回可讀懂的資訊。」

知識共享：簡訊 vs 端點到端點加密資訊

(講師可以出示 這張 gif 呈現簡訊如何在手機間傳送)

講師：「這是一則透過手機網路發送的簡訊。什麼樣的電腦可以存取這則文字？有多少人可以使用那些電腦？」

引導學員回答出：行動電話公司和其他可以使用行動通信基地台的公司。而這些公司可以靠業務合作夥伴 (可能是成千上萬的人) 跨國分享資訊。

講師可以引導舉手，點人起來回答。

提問和回答

提問：「這裡誰有 iPhone？」

提問：「用 iPhone 的人有沒有注意到，你傳給其他 iPhone 使用者的資訊跟你傳給非 iPhone 使用者的資訊顏色不同？是什麼顏色的？」

回答：藍色！

提問：「有人知道那個顏色代表什麼嗎？」

回答：蘋果 iPhone 手機的 iMessage 使用了端到端加密。

提問：「那你們傳訊息給用 Android 手機的人時，會發生什麼？」

回答：訊息是綠色的，表示訊息沒有經過加密。

——轉折——

提問：「如果你想跟沒有 iPhone 的人聊天，但你也想要端到端的加密通訊，那該怎麼辦？」

答：(此時學員可能已經知道有哪些端到端加密應用程式可以下載。)

談話要點

講師：「大家要注意的是，雙方都要下載端到端加密工具，才能進行私密通訊。」

講師：「電信網路和網路使人們的交流比過去任何時候都容易，但也讓監視比過去更為普遍。如果不採取額外措施來保護隱私，所有電話、簡訊、電子郵件、即時訊息、IP 語音 (VoIP) 電話、視訊聊天和社群媒體資訊都可能被竊聽。

通常最安全的溝通方式是面對面，完全不涉及電腦或電話。但這不見得辦得到，所以第二好的方法就是使用端到端加密。」

講師：「端到端加密是什麼意思？」

(講師應該引導學員回答：「端到端加密可以保證資訊變得不可讀，由原發送方加密訊息，只有接收者能解碼」或是「端到端加密可以讓不同裝置之間的訊息成為亂碼，當你不信任服務供應商或協助傳訊息的公司時相當有用」

講師：「除了你之外還有誰可以存取你們的簡訊和語音通話內容？」

(學員可能會說一些公司的名稱，譬如網際網路服務供應商或電信公司，或手機製造商。)

知識共享：有關端到端加密應用程式的知識

談話要點

- 我們推薦的大多數端到端加密訊息應用程式都是免費的。
- 這些應用程式都很適合在 WiFi 和手機行動上網使用，不會吃掉太多流量。
- 有很多都能跨國運作。
- 也有很多有視訊聊天、群組聊天和銷毀訊息的功能。

你也可以分享一些更深入的觀點：

- **譬如後設資料很重要**

  電話服務營運商知道你在使用端到端加密應用程式，因為他們可以存取你手機的「後設資料」。提供應用程式下載商店的公司 (如 Apple App Store 或 Google Play Store) 也知道你在使用這些應用程式。他們可以看到你的訊息或後設資料，包括你下載應用程式的時間等細節。根據應用程式的不同，後設資料可能僅限於此，也可能更詳細。例如，應用程式可能會記錄你常聯絡的對象、連絡時間和時間長度，即使訊息本身內容只有你和你的目標收件者才能看到。

- **在選擇手機應用程式之前，請先檢查應用程式開發人員儲存了哪些使用者資訊**

  依據你安心程度選擇合適的工具。

- **檢查你使用的端到端加密訊息應用程式是否預設端到端加密。**

- **了解應用程式遇到未加密訊息怎麼通知你。**

  不熟悉應用程式介面的人可能會誤認為未加密訊息已經過加密。例如，有些應用程式會讓你知道，你在和未使用端到端加密應用程式的人聯絡，會顯示類似「未加密簡訊」或「未加密文字」之類的內容。請注意這些文字！

- **許多加密訊息和手機應用程式都會要求你提供電話號碼，有些人可能會擔心這件事。**

  有一些替代方案是將你的帳戶連結到 Signal 和 WhatsApp 等應用程式的代理電話號碼上。

  還有其他的應用程式可以讓你選擇使用者名稱，例如 Wire。如果你很在意是否會被輕易的辨識身份，可選一個不同於其他帳戶的使用者名稱或和身份相關的用戶名。

- **你的國家可能不允許部分加密訊息應用程式。可以關注一下 Google Play Store 和 Apple App Store 最近的限制事件。**

- **許多端到端加密訊息應用程式可以驗證朋友的裝置身分，這能避免竊聽者試圖假裝是你朋友：**

  這種做法稱為「金鑰驗證」，也就是在類似 Signal 的應用程式中檢查的「安全碼」。

  這種做法能協助你確保在和正確的對象傳訊！發送消息時，有一種稱為中間人攻擊 (MitM) 的風險，即某人偽裝成你打算通訊的對象，並能夠攔截你的訊息。防止這種情況的方法是透過「金鑰驗證」的做法。

  你可以藉由驗證密鑰，和通訊對象的人驗證彼此的身份，為你的通訊加一層保護，讓你更能確定你正在和正確目標通訊。金鑰驗證允許你的聯絡人確認和他們通訊的人確實是你，而你可以親自或透過另一個安全管道相互檢查，確認對方身分無誤。

  實際上，這種做法通常像是你用手機鏡頭掃描朋友手機的 QR code，然後他們也做同樣的事情。這樣就能確定他們的手機是他們的。

講師在開始指導安裝前，可以問問現場有沒有其他問題。

結尾活動（非強制）

現場進行調查，並確認學員是否理解：

- 公司、服務供應商和電信公司在你通訊時可以看到哪些資訊？
- 在某平台上使用加密技術時，該平台業者能看到什麼？(答案不是「都看不到」，而是亂碼，且他們還是會知道你在和其他人通訊。)
- 使用端到端加密和某人通訊時，服務提供商和電信公司可以看到哪些資訊？(引導學員回答後設資料。)
- 有哪些主流服務不使用端到端加密？
- 端到端加密通訊有什麼幫助？
- 什麼是中間人/機器攻擊?
- 假設你的裝置上有惡意軟體。那端到端加密通訊還算隱密嗎？(答案是「不一定」。如果學員對這點上有疑惑，請解釋靜止加密和傳輸加密之間的區別。)

端到端加密通訊：手機應用程式－進階

協助你的學員建立基本的概念，理解端到端加密會如何保護他們的通訊。這節課，我們將從「私密通訊」和「加密」開始探索，然後深入了解端到端加密的基礎知識 (和限制！)。這堂課之後，學員應有更完善的知識來學習如何選擇、安裝和使用端到端加密訊息應用程式。

建議閱讀

- 如何在 Android 上和 iOS 上使用 Signal。
- 如何在 Android 上和 iOS 上使用 WhatsApp
- 和其他人聯繫。

你可能會遇到的問題與狀況

- 如果學員沒有行動裝置怎麼辦？
- 如果學員沒有自己的行動裝置，或者擔心裝置內已經有惡意軟體怎麼辦？
- 如果學員不想提供電話號碼怎麼辦？有沒有備用方案或是他們可以用於練習用的電話號碼？
- 課堂上的學員覺得尷尬時怎麼辦？如果大家彼此不認識怎麼辦？

可預期的問題與解答

問題：「為什麼你推薦這些應用程式，而不是推薦 [其他應用程式]？」

解答：講師應該參考這篇 EFF 如何選擇工具的文章。

預設情況下，工具都是端到端加密的，而且一律免費，可以在 Android 和 IOS 手機上使用。

這些應用程式還具有強大的安全功能。Signal、WhatsApp 和 Wire 等應用程式都使用了一種名為 forward secrecy 的技術。簡單說就是，應用程式用一組新的加密金鑰加密每條訊息，這樣可以保護過去進行的通訊不受密碼或密鑰在未來暴露的威脅。這與端到端加密電子郵件不同；在端到端加密電子郵件中，加密金鑰會無限期保留在使用者手中，直到使用者選擇生成新的金鑰 (可能是幾年後)。如果有攻擊者得到了他們的私人金鑰，那麼這個攻擊者就可以解密之前發送的所有訊息。

（譯註：forward secrecy 每則訊息都產生不同金鑰，端到端加密則是每個用戶端產生一把金鑰，前者更頻繁更換金鑰所以比較安全。）

問題：「WhatsApp 不是 Facebook 旗下的嗎？這代表什麼？」

解答：是的。WhatsApp 最初承諾不會和 Facebook 分享資訊，後來又改變了立場。WhatsApp 仍然是端到端加密，但他們和 Facebook 分享後設資料（metadata），譬如誰在聯絡誰。不過，WhatsApp 的一個好處是它是一款主流應用程式，這意味著你的朋友和聯絡人很有可能都會使用。要瞭解更多 EFF 關於 Whatsapp 的資料，請參閱 SSD 指南，瞭解如何在 Android 和 iOS 上使用 Whatsapp。

問題：「那如果我想匿名通訊呢？」

解答：這又是另一種不同的擔憂，這可不僅是想保持通訊內容的隱私。你是否不想和你聊天的對象有所連結？這可能對記者和消息來源、吹哨者等聯繫很重要。和敏感人士聯繫的後設資料有不同的風險和考量。我們提及的工具都不提供匿名通訊。

如果你會擔心匿名問題，我們可以在工作坊結束後討論。

問題：「Signal 真的沒有保留這些資訊嗎？你怎麼知道？」

解答：請參考 2016 年 的大陪審團傳票：
(https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/)

不過他們應該也知道，如果 Signal 收到美國法院的命令，他們會被迫蒐集這類資訊。

問題：「我聽說有人可以駭進 Signal，真的嗎？」

解答：不可能。對 Signal 最有效的破解方法是你裝置上的惡意軟體。你若下載到惡意檔案或點擊釣魚連結，惡意軟體可以感染你的裝置。如果端點 (即設備) 被惡意軟體破壞，沒有端到端加密工具可以保護你的訊息。這並不表示該工具提供的端到端加密沒有用——只是能力有限。

問題：「那如果我不想用真實的手機號碼呢？」

解答：你有幾個選擇。你可以用 Wire 這個軟體，或者如果你在美國，你可以用 Google Voice 電話號碼或 Twilio 電話號碼進行匿名通訊。你也可以更換 SIM 卡。

學習目標

課程結束後，學員將：

- 下載端到端加密通訊軟體到自己的手機上。
- 練習傳送訊息給其他人。
- 練習打電話給其他人。
- 練習傳送群組訊息。
- 和其他人驗證金鑰/指紋/安全碼 (如掃描 QR code 或本人親自驗證)

先備知識

- 如果要安裝程式，學員必須隨身攜帶手機。

- 講師已對此群體進行威脅建模。
- 學員已經完成此課程的初階部分。

師生比例

講師：學員＝1：5（一名講師指導五名學生）

建議教材

- 投影機
- 如要安裝應用程式，學員應攜帶自己的智慧型手機。

課程內容

選擇下列其中一項延伸活動：

- 如何在 Android 上和 iOS 上使用Signal。
- 如何在 Android 上和 iOS 上使用 WhatsApp。

使你更安全的瀏覽器外掛：HTTPS Everywhere 跟 Privacy Badger - 初階

瀏覽網頁也需要小心一點：需要避免不安全的 HTTP 網站及被網站蒐集、追蹤使用時產生的數據資料。這就是電子前哨基金會（EFF）的兩個瀏覽器外掛出場的時刻了。一個提供額外的安全性，另一個把關你的隱私。

HTTPS Everywhere 瀏覽器外掛會預設在瀏覽網站時是使用 HTTPS 的安全連線。而 Privacy Badger 外掛可幫助你避免間諜軟體及第三方追蹤器在你瀏覽諸多網站時蒐集你的上網習慣等數據。在本課程中，我們將分享一些方法，供學員瀏覽網路時能保護自身隱私。

推薦閱讀

- 加密類型簡介
- 網路瀏覽安全指南
- 5 個能保護自己線上隱私安全的 EFF 工具
- Privacy Badger 網站
- HTTPS Everywhere 網站
- Panopticlick 網站
- 加密網路
- Moxie Marlinspike 的 SSLStrip 的攻擊資訊

你可能會遇到的問題與狀況

對這兩個工具可能有的誤解。

Privacy Badger 和 HTTPS Everywhere 不是完美的解決方案

需要釐清這兩個瀏覽器外掛能解決哪些問題，及他們的使用限制。

Privacy Badger 的威脅建模：Privacy Badger 阻止公司蒐集你的上網習慣之數據，對那些試圖針對你的攻擊者（例如罪犯、跟蹤者及政府）只能提供最基礎的保護。

HTTPS Everywhere 的威脅建模：HTTPS Everywhere 有助於提高你日常使用的加密級別，這確實可以增強防範一些被監視的可能性，但它沒辦法完全加密你的所有通訊。

可以把這兩個外掛視作維他命：他們為大多數人提供最基礎的保障，但是如果你遭受的攻擊特別嚴重，則需要更強的解決方法。

Privacy Badger 不是廣告攔截器

有時會聽到 Privacy Badger 被拿來與 Adblock Plus 之類的廣告攔截器一起討論。然而，請務必強調 Privacy Badger 不是一個廣告攔截器；相反的，它是一個追蹤攔截器。Privacy Badger 會阻擋意圖蒐集你線上行蹤的有害追蹤器，無論它是否隨著廣告一起出現。同樣的，Privacy Badger 只會在廣告程式蒐集你的資料時才會攔截此廣告。（有關更多訊息，請參閱 EFF 的「不追蹤」政策）透過這種方式，Privacy Badger 希望鼓勵廣告更透明、更負責任地尊重個人的隱私。

HTTPS Everywhere 並不能加密所有東西

如果你沒有事先接觸過這類工具的話，很容易以為 HTTPS Everywhere 能在沒有 HTTPS 連線的時候創建 HTTPS 連線。你可以透過解釋清楚「一個網站的管理者會決定『是否在其網站提供 HTTPS』」來解決這樣的疑慮（幸運的是，每天都有越來越多的網站開始提供）。網站管理員啟用 HTTPS 後，HTTPS 便能有效提升你在瀏覽時的安全性。然而有些網站，即使它們啟用了 HTTPS 的相關設定，仍有些不完美的地方，包括沒有將它改為預設、未能讓它加密整個網站的內容、或是網站上的連結仍導向未加密的頁面等等。借助 HTTPS Everywhere，你有機會化解這些更複雜的狀況，並確保使用者能盡可能獲得加密的連線。如果你希望所有的上網行為都通過加密進行，

可以勾選「阻止所有未加密的請求」的選項。但是要記住，這會讓你不能連上那些僅支援 HTTP（不安全的連線）的網站。

Internet 連線與其他安裝問題

安裝瀏覽器外掛是一個簡單的流程，但還是有些需要顧慮的地方。你可能需要事先檢查場地的網路連線，並錯開學員下載檔案的時間。如果你需要進行培訓前的諮詢或調查，請詢問學員所使用的瀏覽器為何。你甚至可以鼓勵較有經驗的學員事先安裝好瀏覽器外掛。

可預期的問題與解答

請務必參考 HTTPS Everywhere 的常見問題
以及 Privacy Badger 的常見問題

學習目標

學員將：

- 能夠解釋 HTTPS 與 HTTP 有何不同
- 能夠解釋「第三方 Cookie」中的「第三方」是什麼
- 安裝 HTTPS Everywhere
- 了解當網站不提供 HTTPS 時，HTTPS Everywhere 便無法建立 HTTPS 連線
- 安裝 Privacy Badger
- 了解即使 Privacy Badger 能攔截追蹤程式，但它並不是一個「廣告攔截器」
- 透過 Panopticlick 了解瀏覽器指紋識別和第三方追蹤的資訊（非強制）

先備知識

- 學員需自備電腦

- 學員的電腦裝有網路瀏覽器（Firefox、Firefox for Android、Opera 或 Google Chorme 等）
- 學員了解什麼是網路瀏覽器（並且沒有將其誤解成搜尋引擎或網路）

師生比例

一個講師對 10 個（或以上）學員

建議教材

講師可以透過電腦和投影機示範使用這些工具、展示瀏覽器外掛的功能。

本課程主要是知識分享，大部分的對話是一對多進行的。

外掛程式的安裝流程基本上只需要點擊幾下就能完成，但有些人可能需要進行故障排除。在安裝時，你可以請已經順利安裝 HTTPS Everywhere 和 Privacy Badger 的學員，去協助遇到困難的學員。

課程內容

暖身問題

你是否曾經在上網時因為看到某些廣告，讓你懷疑他們是不是知道你在另一個網站瀏覽或購買了什麼，讓你覺得很毛骨悚然？請大家分享關於廣告掌握了你的行蹤的經驗或故事。

大家有注意過網址欄中的綠色鎖頭符號嗎？有人知道這個鎖頭代表什麼意涵嗎？

知識分享

在引導大家開始安裝 Privacy Badger 和 HTTPS Everywhere 之前，這些討論可能會有幫助：

什麼是瀏覽器？為什麼我該下載這些外掛呢？

瀏覽器（例如 Firefox、Google Chrome、Safari、及 Internet Explorer）是你拿來上網、瀏覽網頁的工具。通常在你開始使用之前，電腦便會裝有瀏覽器供你使用。許多瀏覽器有內建的保護安全及隱私的措施。安裝這些外掛時，他們會在這些既有的保障上提供更近一步的保護。

誰是 EFF（電子前哨基金會），為什麼推薦使用他們的東西？

標準答案大致如下：電子前哨基金會是一個總部位於舊金山的非營利組織，進行的工作是捍衛數位世界的公民自由，包括隱私、安全、言論自由和創新等等。根據你的學員，可以對這個解釋進行調整，建立一些與學員的關聯性。你可以解釋自己對 EFF 的了解，或是 EFF 有關注哪些與你我相關的議題。（在安裝軟體這個情境下，強調 EFF 是非營利組織、關注消費者權益等等通常會有所幫助。）你可能還會想強調一下，這些外掛是開源的，也就是說使用者可以檢查其中的程式碼，確保程式不會在電腦上進行不符合預期的行為。

下載這兩個外掛是一種最簡單的資訊安全措施。安裝完成之後，外掛會自己完成大部分甚至全部的程序，確保你不會在網路上被輕易追蹤，並盡可能使用安全的連線上網。

Privacy Badger 能做什麼？

當廣告商及網站在未經你的同意下，透過程式碼追蹤你在網站間瀏覽時的各種行為，我們稱為「**第三方追蹤**」。這在線上廣告中是相當普遍的做法。Privacy Badger 通過偵測疑似在進行追蹤的第三方網域，並攔截那些數據，使你重新獲得資料的控制權。與其他「追蹤攔截器（Tracker Blocker）」不同的是，Privacy Badger 不需要建立一個龐大的追蹤器名單來判斷追蹤器，而是通過觀察追蹤器特有的行為來認定它要攔截的網站。儘管 Privacy Badger 實務上攔截了許多廣告，但比起嚴格的「廣告攔截器（Ads Blocker）」，它更是一種隱私工具。Privacy Badger 鼓勵廣告商尊重使用者的隱私，並且透過不攔截符合 EFF 的「不追蹤政策」的網站來達成這一點。你隨時可以透過打開選單來確認外掛當下偵測或攔截的網域有哪些，並根據需要進行調整。

HTTPS Everywhere 能做什麼？

HTTPS Everywhere 是一個由 EFF 和 Tor Project 協力開發的瀏覽器外掛，支援 Firefox、Chrome、Opera 等瀏覽器，它能使你在上網時盡可能使用 HTTPS 的加密連線與網站主機進行通訊。有一些聲稱支援 HTTPS 的網站對 HTTPS 的支援並不一致，像是以使用未加密的 HTTP 為網頁預設，或是從安全的 HTTPS 頁面連結到未加密的 HTTP 頁面。此外，當使用者在瀏覽器中輸入「example.com」網址時，瀏覽器大多數而言都會嘗試連線到該網站的不安全 HTTP 版本，並且僅在該網站要求「重定向」到 HTTPS 時才升級連線。這使瀏覽器容易受到針對重定向流程破壞的攻擊（例如 SSLStrip）。HTTPS Everywhere 將這些網站的請求（request）改寫為 HTTPS，自動啟用加密以及 HTTPS 保護來解決這些問題，否則 HTTPS 能提供的保障可能會無法發揮到最大。

為此，HTTPS Everywhere 的團隊製作了最完整的支援 HTTPS 的網站列表，這個列表也被 Brave 瀏覽器或 Automatic HTTPS Rewrites 等軟體所使用。HTTPS Everywhere 也運用在 Tor 瀏覽器，盡可能確保匿名上網的安全。

究竟什麼是 HTTPS？

上網時，網站有兩種跟瀏覽器連結的方式：HTTP 和 HTTPS。顧名思義，這兩者的差別在於這個代表「安全」的「S」(secure)。通過 HTTP 上網的過程容易受到連線竊

聽、內容注入(content injection)、Cookie 或憑證竊取、內容審查或屏蔽等等的其他風險。但是 HTTPS 在預設情況下會確保連線過程是安全的。
當你在瀏覽器上方的網址欄看到「HTTPS」的字樣和旁邊一個綠色的小鎖頭時，表明你正在使用安全的連線。在線上購物或輸入信用卡訊息時，通常一定會看到它。
如果有人試圖在區域網路竊聽、監視使用者正在上哪些網站，此時 HTTP 連線形同赤裸，沒有任何保護。HTTPS 則不會揭露你正在查看的頁面為何，「/」之後的所有內容都會被保密。例如，如果你使用 HTTPS 連線到 www.eff.org/ssd，竊聽者只能推敲出「www.eff.org」的部分。使用 HTTPS，竊聽者無法得知你正在瀏覽一個網站中的哪一部分。

活動：安裝

讓學員打開 Privacy Badger 和 Https verywhere，並指示他們按下自己瀏覽器的安裝按鈕。此時，可能需要協助一些人辨識他們正在使用的瀏覽器，你可以為此提供協助，並且當學員完成安裝後，你也可以請它們去協助其他學員。

活動：試試 Panopticlick 檢測

如果你想測試瀏覽器外掛對隱私的保護程度，可以執行 Panopticlick 上的測試。如果學員在課程後已經安裝了 Privacy Badger，那就會在 Panopticlick 上看到自己的瀏覽器已經得到更好的保障。你可以鼓勵學員在身邊朋友或家人的瀏覽器上執行這個測試，以了解他們的瀏覽器是否具備有效的保護。如果他們的瀏覽器的保護不足，則學員可以建議他們安裝 Privacy Badger。

推薦給想知道更多相關資訊的學員

關於未經同意的第三方追蹤：

- Cookie 的新技術：變得更常用來追蹤你、更難偵測和移除
- 網路追蹤公司如何得知你在網路上做了什麼（以及社群網路如何協助他們）
- 單單「瀏覽器版本」就帶有平均 10.5 位元的辨識資訊

關於「不追蹤政策（Do Not Track policy）」，EFF 如何鼓勵負責任的廣告行為：

- 了解 EFF 的「不追蹤政策」
- Twitter 的新政策背棄了長期承諾的隱私考量
- Twitter（和其他網站）加倍地配合廣告與追蹤
- Privacy Badger 讓 Twitter 少了點威脅

關於 EFF 發起的「Encrypt the Web」計畫：

- 把網際網路全都加密吧
- 「把網際網路全都加密吧」影片

威脅建模 (Threat Modeling) - 初階

在保護資訊安全的領域裡，工具和技巧可能不斷更新，但永恆不變的是對「威脅模型」的考量。建立「威脅模型」的觀念是教學其他資訊安全概念的基石，它可以使學員在規劃防禦手段時建立信心，並協助講師根據學員的資安需求調整更有效的教學方式，讓他們準備好了解自己所面對的風險、規劃因應的行動。

推薦閱讀

- 評估你的風險
- 如何梳理數個不同的威脅模型

你可能會遇到的問題與狀況

- 學員最好由一群面對相近疑慮、風險和威脅的人組成。如果無法做到，那麼你將需要準備同時處理多個不同威脅模型的情況。
- 學員可能會對「威脅建模」一詞感到恐懼，並將其與軍事術語連結在一起（事實上，這個概念是來自軟體工程），出於這個原因，一些講師更喜歡將這個部分稱作「評估你的風險」。
- 學員在遇到那五個「威脅建模」的問題時可能會感到不知所措。

學習目標

學員將：

- 了解「威脅建模」的定義是什麼。
- 了解他們在日常生活中已經在進行類似的分析。
- 了解威脅建模的五個核心問題和概念。
- 了解學員在應用威脅建模時應了解的五個術語。
- 考慮過各種能夠攔截電子郵件的方式。

先備知識

沒有！這是為一系列培訓揭開序幕的一個好方式。

師生比例

靈活有彈性

推薦教材

威脅建模活動講義
筆
便條紙或便利貼

課程內容

暖身活動

問學員：「當你在做……（以下活動）時，你會怎麼思考呢？」

- 你在開車時會如何決定在哪邊停車？
- 你如何選擇住處使用的鎖頭 / 警報器？
- 你如何決定步行或騎車到某處的路線？

結論是，每一位學員都在日常生活中進行了某種程度的威脅建模。我們課程的任務則是要將這種思維應用於保障資訊安全和隱私。

另外，你可以嘗試看看一些小遊戲，例如 Lucy Parsons Labs 的培訓活動：給每個學員一副紙筆，請他們寫下他們對於數位安全或隱私方面最擔心的一兩件事情。一些有效的發問可以包括：

- 是什麼讓你想參加今天的培訓？
- 你期待化解哪些相關的疑慮呢？

根據情境，你可以在小組間四處走動，讓參與者分享他們的回答，也可以收集卡片在課程中參考。

知識分享

首先提出五個問題：

- **我要保護什麼？**
- **我想保護它免於誰？**
- **如果失敗了，後果是什麼？**
- **我有多大的必要主動保護它？**
- 我願意付出多少代價以防止潛在的後果發生？

逐個帶過這裡的問題，記得停下來解釋牽涉到的名詞和概念，讓學員有辦法自己回答這些問題、建立這五項重要的觀點。

- 我要保護什麼？稱作**資產**。
- 我想保護它免於誰？稱作**威脅者**。
- 如果失敗了，後果是什麼？稱作**威脅**。
- 我有多大的必要主動保護它？這取決於威脅者的能力。

對於這四個問題中的每一個，鼓勵學員列舉粗體字的例子，例如，你擁有哪些「資產」？你可以想像哪些「威脅者」？依此類推。

- 我願意付出多少代價以防止潛在的後果發生？這就是你自己對**風險**的衡量。

現在，讓我們退一步來討論為什麼，儘管每個概念看似都很簡單，但實際上牽涉的卻非常複雜，尤其是在資訊安全這方面。

- 例如，當你在考慮「該把車停在哪裡」這個威脅模型時，你正在處理已知的狀況、位置和事物。

- 在資訊空間中，存在著更多的不確定性。很難確切地知曉不同資訊的所在位置或不同威脅者的能力所及範圍。例如，電子郵件可能在從寄件的使用者到收件人的這段漫漫長路（使用者的電腦到路由器、路由器到電子郵件服務商、在電子郵件服務商之間、服務商到收件人之間）上的許多節點之一遭到攔截。

活動

「想像一下，你正在向朋友發送電子郵件，這封信是怎麼從你這邊一路送到對方的收件夾裡的？中間會經過哪些步驟？」

在一個小組中，你可能有機會讓每個人告訴你他們的想法。在較大的小組中，你可以將學習者分成小組來進行討論，或著隨機邀請學員鼓勵他們分享。

如果你擁有一些材料（便條紙、筆等等），則還可以請學習者試著把他們的想法畫出來展示。

在和學員聊聊他們的認知之後，利用投影片或流程圖向他們解說一封電子郵件會行經的所有環節，並且在這各個環節之中哪些威脅者得已藉機竊取。

威脅建模 (Threat Modeling) - 進階

在保護資訊安全的領域裡，工具和技巧可能不斷更新，但永恆不變的是對「威脅模型」的考量。建立「威脅模型」的觀念是教學其他資訊安全概念的基石，它可以使學員在規劃防禦手段時建立信心，並協助講師根據學員的資安需求調整更有效的教學方式，讓他們準備好了解自己所面對的風險、規劃因應的行動。

推薦閱讀

- 評估你的風險
- 如何梳理數個不同的威脅模型

你可能會遇到的問題與狀況

- 學員最好由一群面對相近疑慮、風險和威脅的人組成。如果無法做到，那麼你將需要準備同時處理多個不同威脅模型的情況。
- 學員可能會對「威脅建模」一詞感到恐懼，並將其與軍事術語連結在一起（事實上，這個概念是來自軟體工程），出於這個原因，一些講師更喜歡將這個部分稱作「評估你的風險」。
- 學員在遇到那五個「威脅建模」的問題時可能會感到不知所措。

學習目標

學員將：

- 將威脅建模的觀念運用於一個假設的情境

先備知識

學員已完成本課程的初階部分。

師生比例

可以先使用講座的方式，再於結束後將學員分成小組進行活動

課程內容

活動

將學員分成人數為偶數的小組，每組分成：一隊將試著保護特定的資產，另一隊是試著獲取該資產的威脅者。給他們一個特定的情境，讓學員利用 15 分鐘左右討論如何保護資產或攻擊資產，然後進行小組報告。

這時最適合的便是針對受眾學員所設計的情境，例如：

- 對於一群記者來說，資產可能是匿名線人提交的消息。你將如何保護這個線人的匿名性？或者，如果消息之後被報導後你遇到了其他的狀況，你要如何揭露這個線人／消息來源？

- 對於比方說在美國城市中的一群社運工作者而言，資產可能是一群信任的人或是組織間交流的各種事務。要採取什麼預防措施來確保這些訊息始終維持其機密性？或者，如果你是一位執法機關或大學的官員，你要如何事前得知這些運動組織在討論些什麼？

- 對於面臨網路霸凌的學生，資產可能是社群媒體的身份跟個資。你如何確保在線上分享的內容只被預期的對象看到？或者，如果你是一個霸凌者，你要如何取得那些個人資訊？

情境也可以有點滑稽！其中可能包括：

- 一方是小丑、另一方是蝙蝠俠。
- 一方是銀樓老闆、另一方是國際珠寶大盜。

如果你有一個小時以上的時間：

威脅建模可以幫助你繼續針對學員個別的疑慮和情形進行探討，根據學員在課程之前及威脅建模活動中提供的狀況，你可以個別解釋比方說密碼與密碼管理工具、網路釣魚保護、社群媒體隱私、匿名瀏覽及 Tor 等主題。

密碼管理器－初階

管理許多密碼對於網路使用者來說可能是一個挑戰，使用密碼管理器可能是一個解決方案。但是，使用密碼管理器可能對於學員來說有點新穎，需要一些時間才能習慣。在本章節中我們會解釋密碼管理器的原理，然後幫助學員慢慢習慣這個工具。

推薦閱讀

- 如何使用 KeePassXC （中文版）
- SEC 系列課程：密碼
- 建立強式密碼
- EFF 利用骰子建立密碼
- 動畫介紹：利用密碼管理工具，維持線上安全。

你可能會遇到的問題與狀況

密碼管理器的使用流程可能會讓許多學員感到陌生，除非他們事先接觸過類似的工具。講師可能需要先多次示範如何用密碼管理器執行指定的實作練習項目，學員也需要花一些時間在自己的裝置上練習以熟悉實作內容。

當你在為重要的服務設定新密碼（例如密碼管理器本身的密碼）時，可能有一些學員會忘記他們的新密碼。如果人們在不記住密碼的情況下更改了重要帳號或設備的密碼，這件事情可能弊大於利。考慮建議人們寫下他們的密碼（在紙上或在密碼管理器中）。對於那些寫下密碼的人，提醒他們提防別人偷看他們的筆記，並將這些筆記保存在安全的地方！

對於那些難以記住其密碼的人，我們可以考慮使用一些輔助記憶技巧。例如在連結圖像記憶、使用助記詞（mnemonics）或連結一個好笑的故事等來幫助他們記憶密碼。

可預期的問題與解答

問題：「如果我的密碼管理器公司遭到入侵怎麼辦？不是說沒有完美的軟體或完美的安全性之類的東西嗎，為什麼我應該信任他們？」

解答：這是一個很棒的問題，充分展現提問人擁有資訊安全的思考脈絡。任何安全工具都將涉及折衷和權衡，密碼管理器也不例外。 所以最終問題可能是：信任密碼管理器與沒有密碼管理器的情況相比如何？ 對於大多數人來說，密碼管理器可以有效防止帳號洩露的最大原因——也就是在各個帳戶中使用相同的密碼。但我們必須權衡密碼管理器公司本身遭受破壞的風險比較大，還是不使用管理器的風險比較大。

1Password 和 LastPass 之類的密碼管理器會將你的密碼儲存在一個加密檔案中，該加密檔案只有你擁有的密鑰可以解密，因此即使有人駭入密碼管理器公司並偷走了你的密碼檔案，他們也無法對其進行解密。

問題：「如果駭客侵入我的電腦怎麼辦？使用密碼管理器會不會意味著駭客只要拿走我的密碼管理器檔案就可以看到所有的密碼？」

解答：如果駭客在你的電腦上安裝了允許他們存取所有文件的惡意軟體，則讀取一個文件中的所有密碼，比等待你登入每個帳號並手動輸入密碼的速度來的更快。如果你沒有用密碼管理器，而是直接將密碼記錄在一個檔案上，那駭客就只要看檔案就好了；如果你用了密碼管理器，其儲存密碼的檔案是有用主密碼加密保護的，所以無法直接存取。

問題：「如果我忘記我的密碼管理器主密碼怎麼辦？」

解答：記住你的主密碼是很重要的。與其他加密工具一樣，記得密碼與否會影響你是否可以存取其加密的資訊。請務必記住你的主密碼！

將密碼寫在一張紙上並將其保存在安全的地方，然後在記住密碼後將這張紙銷毀可能是一個好方法，你可能在想，等等，難道我們不應該將密碼記憶在頭腦中，永遠不要

寫下來嗎？實際上，寫下來並將密碼的紙本備份儲存在錢包或其他安全的地方其實非常有用，這樣你至少可以知道你寫的密碼是否不見或被偷。

骰子密碼法是一個產生強度高，隨機且易於記憶的密碼的好方法。如果你在記憶主密碼時遇到麻煩，則可以設定一組基於一段故事的密碼，或者為自己創建一組助記詞。對於有記憶困難問題的人，若不擔心同居者可能看到，寫下密碼可能是個好主意。

問題：「所有人都適合使用密碼管理器嗎？」

解答：對於某些人來說，密碼管理器可能不是一個好的主意。例如，處於不對等權力關係中的人可能會被人強迫解鎖密碼管理器，暴露其所有線上帳號清單與其所有網上活動紀錄。兒童可能也會面臨相同的情況，特別是 LGBTQ 青少年，或因宗教或政治信仰在家庭或社區中受到污名化的青少年。

密碼管理器的目的是確保人們為每個帳戶建立長、難於猜測、獨一無二的密碼，但是如果某人有以上這種人身安全的風險或威脅，密碼管理器就可能不是正確的選擇。

學習目標

學員將學會：

- 了解密碼管理器儲存的密碼資料只有使用主密碼才能讀取
- 能夠舉例說明何時可以使用密碼管理器（記住密碼、提示，甚至是隨機生成的安全問題答案）。
- 了解單機版（離線版）密碼管理器和雲端版（線上版）密碼管理器之間的區別。
- 如果有時間：動手實作，安裝離線版密碼管理器。

先備知識

- 學員必須知道如何選擇一個好的主密碼

課程內容

暖身

你可以問：「這裡有多少人曾經在多個帳號上使用過重複的密碼？」這是一種吸引學員的好方法，並且可以讓講師評估學員的技術水準。你也可以修改問題，詢問學員：「這裡有多少人曾經把一個密碼做了一點改動，來當作多個帳號的密碼」（譯註：例如在強密碼的最後面加上數字流水號）？

順著問題的脈絡，你可以繼續說：「沒關係。因為我們被迫註冊很多網站，我們自然希望有一種簡單的方式來記住密碼。但是，在不同的網站上重複使用相同的密碼是導致帳戶被入侵的第一大原因。密碼管理器可以為提供我們密碼上的協助！」這種對話能讓學員不會感覺挫折，並且有機會改善自己的操作方式。

知識分享

不同的密碼管理器具有不同的特性及需要投入的使用時間。密碼管理器的兩種基本類型為：

單機版／離線版密碼管理器：這些密碼管理器通常作為獨立的檔案存在於你的裝置上，並要求你將登入資訊從密碼管理器複製貼上到指定的登錄介面。儘管這會讓同步跨設備變得更加困難，但是單機版密碼管理器非常適合希望將密碼保存在單獨的設備設備（如隨身碟）上的使用者。單機版密碼管理器特別適合共用設備的情況。

雲端版／線上版密碼管理器：你可以通過網站使用它們，也可以下載為電腦的瀏覽器外掛和手機的應用程式。它們能夠在不同裝置間同步密碼。最重要的是，這種密碼管理器非常適合防止網路釣魚攻擊。對一般人來說可能很難分辨偽造的登入頁面與合法的登入頁面，但這種密碼管理器可利用技術線索來區分它們。一個不會觸發密碼管理器的登入頁面，對使用者來說就是個要注意的異常狀況。

有些密碼管理器公司同時提供上述兩種密碼管理器，例如 KeePassXC 和 1Password。EFF 目前推薦 KeePassXC，它是一個離線版的密碼管理器，但也提供瀏覽器外掛。學員可以根據各自的風險分析，選擇使用其他密碼管理器，例如 1Password、LastPass 或 Dashlane。

活動

當學員了解為什麼需要密碼管理器，就可以指導大家進行密碼管理器的安裝步驟。請參閱「 如何使用 KeePassXC 」中的步驟，並在進入「如何安裝瀏覽器外掛」部分時停止。進階課程將學習如何安裝 KeePassXC 瀏覽器外掛。

如果你沒有時間進行此工具的實作培訓，請考慮使用視覺輔助工具幫助學員記住關鍵概念（例如我們虛構的密碼管理器）。

密碼管理器－進階

管理許多密碼對於網路使用者來說可能是一個挑戰，使用密碼管理器可能是一個解決方案。但是，使用密碼管理器可能對於學員來說有點新穎，需要一些時間才能習慣。在本章節中我們會解釋密碼管理器的原理，然後幫助學員慢慢習慣這個工具。

推薦閱讀

- 如何使用KeePassXC （中文版）
- SEC 系列課程：密碼
- 建立強式密碼
- EFF 利用骰子建立密碼
- 動畫介紹：利用密碼管理工具，維持線上安全。

你可能會遇到的問題與狀況

密碼管理器的使用流程可能會讓許多學員感到陌生，除非他們事先接觸過類似的工具。講師可能需要先多次示範如何用密碼管理器執行指定的實作練習項目，學員也需要花一些時間在自己的裝置上練習以熟悉實作內容。

當你在為重要的服務設定新密碼（例如密碼管理器本身的密碼）時，可能有一些學員會忘記他們的新密碼。如果人們在不記住密碼的情況下更改了重要帳號或設備的密碼，這件事情可能弊大於利。考慮建議人們寫下他們的密碼（在紙上或在密碼管理器中）。對於那些寫下密碼的人，提醒他們提防別人偷看他們的筆記，並將這些筆記保存在安全的地方！

對於那些難以記住其密碼的人，我們可以考慮使用一些輔助記憶技巧。例如在連結圖像記憶、使用助記詞（mnemonics）或連結一個好笑的故事等來幫助他們記憶密碼。

可預期的問題與解答

問題：「如果我的密碼管理器公司遭到入侵怎麼辦？不是說沒有完美的軟體或完美的安全性之類的東西嗎，為什麼我應該信任他們？」

解答：這是一個很棒的問題，充分展現提問人擁有資訊安全的思考脈絡。任何安全工具都將涉及折衷和權衡，密碼管理器也不例外。 所以最終問題可能是：信任密碼管理器與沒有密碼管理器的情況相比如何？ 對於大多數人來說，密碼管理器可以有效防止帳號洩露的最大原因——也就是在各個帳戶中使用相同的密碼。但我們必須權衡密碼管理器公司本身遭受破壞的風險比較大，還是不使用管理器的風險比較大。
1Password 和 LastPass 之類的密碼管理器會將你的密碼儲存在一個加密檔案中，該加密檔案只有你擁有的密鑰可以解密，因此即使有人駭入密碼管理器公司並偷走了你的密碼檔案，他們也無法對其進行解密。

問題：「如果駭客侵入我的電腦怎麼辦？使用密碼管理器會不會意味著駭客只要拿走我的密碼管理器檔案就可以看到所有的密碼？」

解答：如果駭客在你的電腦上安裝了允許他們存取所有文件的惡意軟體，則讀取一個文件中的所有密碼，比等待你登入每個帳號並手動輸入密碼的速度來的更快。如果你沒有用密碼管理器，而是直接將密碼記錄在一個檔案上，那駭客就只要看檔案就好了；如果你用了密碼管理器，其儲存密碼的檔案是有用主密碼加密保護的，所以無法直接存取。

問題：「如果我忘記我的密碼管理器主密碼怎麼辦？」

解答：記住你的主密碼是很重要的。與其他加密工具一樣，記得密碼與否會影響你是否可以存取其加密的資訊。請務必記住你的主密碼！

將密碼寫在一張紙上並將其保存在安全的地方，然後在記住密碼後將這張紙銷毀可能是一個好方法，你可能在想，等等，難道我們不應該將密碼記憶在頭腦中，永遠不要

寫下來嗎？實際上，寫下來並將密碼的紙本備份儲存在錢包或其他安全的地方其實非常有用，這樣你至少可以知道你寫的密碼是否不見或被偷。

骰子密碼法 是一個產生強度高，隨機且易於記憶的密碼的好方法。如果你在記憶主密碼時遇到麻煩，則可以設定一組基於一段故事的密碼，或者為自己創建一組助記詞。對於有記憶困難問題的人，若不擔心同居者可能看到，寫下密碼可能是個好主意。

問題：「所有人都適合使用密碼管理器嗎？」

解答：對於某些人來說，密碼管理器可能不是一個好的主意。例如，處於不對等權力關係中的人可能會被人強迫解鎖密碼管理器，暴露其所有線上帳號清單與其所有網上活動紀錄。兒童可能也會面臨相同的情況，特別是 LGBTQ 青少年，或因宗教或政治信仰在家庭或社區中受到污名化的青少年。

密碼管理器的目的是確保人們為每個帳戶建立長、難於猜測、獨一無二的密碼，但是如果某人有以上這種人身安全的風險或威脅，密碼管理器就可能不是正確的選擇。

學習目標

學員將學會：

- 實際動手安裝單機版／線下版密碼管理器以及瀏覽器密碼管理器
- 為密碼管理器產生一個主密碼
- 練習使用密碼管理器產生密碼
- 練習複製密碼管理器中的密碼到登入網頁使用
- 了解怎麼將常用網站的網址（URL）儲存在密碼管理器中以防止釣魚（改成安裝瀏覽器外掛並使用自動填入密碼的功能）

先備知識

- 學員完成密碼管理器初階課程

建議教材

- 學員必須攜帶電腦或手機

課程內容

活動

指導學員安裝單機版密碼管理器和單機版的瀏覽器外掛。請參閱 如何使用 KeyPassXC 裡的步驟說明。

事後提出的問題

你認為經常使用密碼管理器會遇到哪些挑戰？又有什麼好處？

你需要改變任何使用習慣以配合密碼管理器嗎？你需要採取什麼措施來確保持續使用密碼管理器？

結尾活動（非強制）

讓學員更改至少一個密碼，並將新密碼儲存在其密碼管理器中。可以是他們的電子郵件、社群網站或他們經常瀏覽的網站的登入密碼。