公共 Wi-Fi

學員將認識公共 Wi-Fi
網絡的相關資訊，及其風險與好處。更明確的是，他們將學習如何判斷不安全的 Wi-Fi、瞭解使用不安全的 Wi-Fi 所必須做出的犧牲，以及決定何時該連線使用不安全的 Wi-Fi。

資源

- 無線數據機圖像
- 網絡安全講義

什麼是 Wi-Fi？

第一部分

講授內容

您會使用哪些裝置上網？

這些裝置如何連上網絡？

Image Class Interaction

Wi-Fi 是一種常見的裝置連線方式。Wi-Fi
可以透過無線電訊號連接裝置，而不需要實體或線路連接。

想像您家裡有三個手提電腦要連線上網。為了上網，您必須準備：

1.存取點：存取點是指任何可以傳輸 Wi-Fi 訊號並且提供網絡連線的裝置。您的裝置必須接收到這些訊號才能順利連線上網。有時候您必須取得特殊權限（例如用戶名稱與密碼）才能登入並且使用存取點的無線訊號。

2.路由器：路由器是一種可以在特定地點（例如學校、圖書館或自家）建立所有裝置（例如電腦、平板電腦、手機）連線網絡的裝置。通常路由器都會內建存取點（參考上圖）。

> 路由器的發射範圍有限（通常很短）。所以如果您的裝置距離路由器太遠，Wi-Fi 訊號就會變得很弱或甚至完全沒有。此外，如果裝置和路由器之間有阻礙物（例如建築物或磚牆），訊號也會減弱。
>
> 雖然連接到路由器可以獲得網絡權限，但這並不代表就是互聯網。如果要讓同一個網絡的多台裝置連線上網，路由器就必須連接數據機。

3.數據機：數據機可以建立並維持與網絡服務供應商 (ISP) 之間的連線，這樣您才能夠使用互聯網。數據機能夠將指定地點的外部訊號轉換為您的電腦與其他數碼裝置可以使用的訊號。

> 通常在設定時，存取點與路由器是一個獨立的實體裝置，並且會用一條「乙太網絡」傳輸線連結至數據機。這也是大家經常說的連線互聯網。
>
> 流動裝置也可以使用數據連線來連線上網，特別是當手邊沒有學校、圖書館或家用網絡可以用的時候。數據連線是一種無線的無線電訊號，覆蓋範圍比路由器大很多。數據連線會使用一種稱之為「基地台」的特定收發器來連接您的流動裝置與網絡。

第二部分

講授內容

Wi-Fi 有什麼益處？

Wi-Fi 有什麼缺點？

比起使用連線互聯網，使用 Wi-Fi 可能會有什麼樣的安全性疑慮？

為什麼離開建築物之後，手機就會失去 Wi-Fi 連線？

選擇 Wi-Fi 網絡

第一部分

講授內容

所有 Wi-Fi 網絡都是安全的嗎？為什麼是 / 不是？

講授內容

有時候您必須選擇使用某一個 Wi-Fi
網絡。請千萬記得，如果連上錯誤的網絡，後患無窮。例如，不安全的 Wi-Fi 網絡是指那些不需要密碼就能登入的網絡。如果您連上不安全的網絡，其他使用同一個網絡的人就有機會偷看您的資訊。他們有可能竊取您在網絡上傳輸的資訊，或監測您的活動。

另一方面，安全與受信任的 Wi-Fi 網絡是指那些需要密碼才能登入、啟用加密功能，以及您確信登入網絡名稱與實際名稱相符的網絡。舉例來說，如果您不小心登入假冒學校網絡名稱的網絡，就可能導致帳戶資訊外流。因此，使用安全且受信任的網絡才能獲得最大的保障。

另一點值得注意的是 Wi-Fi 網絡的內容或地點。舉例來說，如果您人在戲院搜尋 Wi-Fi 網絡，卻在手機上看到學校的網絡名稱，這個網絡很可能是在模仿或假冒您的學校網絡，無戒備之心的學生很可能就會上當並交出密碼。

建立受密碼保護的 Wi-Fi 網絡時，持有人必須選擇啟用路由器的加密協定。常見的加密協定包含「有線等效加密」(Wired Equivalent Privacy, WEP)、「Wi-Fi
保護協定」(Wi-Fi Protected Access, WPA) 或
WPA2。這些協定可以將您在無線網絡上傳輸的資訊加密（或「雜湊」）。

加密功能的存在是為了讓駭客無法輕易看到您傳送的資訊。但其實所有的加密協定（WEP、WPA 和 WPA2）都曾經被破解。因此大家在網上傳輸資訊時，一定也要使用安全的網絡連線。

HTTPS 是一種網站用來加密網上傳輸資料的標準。加密作業可以防止任何一個第三方直接在您的連線中窺探您的資料。這個標準可以提供額外的一層防護，而且只要在網址前加上「https://」即可用於各種瀏覽器（例如：https://www.mysite.com）。但並非所有的網站都支援 HTTPS。

1. 您應該選擇只在擁有 HTTPS://
   前綴的網頁中輸入敏感資訊（例如：密碼、信用卡資料）。

2. 大部分主要的瀏覽器在網址列附近都會有類似鎖頭符號的安全性指標，用以顯示 HTTPS 連線。

3. 可惜的是，HTTPS 無法保證您的安全，因為有些惡意網站也會支援

HTTPS。HTTPS 可以確保連線的安全性，但無法確保網站的意圖。

講授內容

安全通訊協定 (SSL) / 傳輸層安全性協定 (TLS) 是負責維護 HTTPS 安全的技術名稱。SSL/TLS 會使用數碼加密金鑰，這些金鑰的作用與實際的鑰匙很類似。如果您在一張紙上寫下您要給朋友的秘密，任何找到這張紙的人都能看到您的秘密。但想像如果您親自將一個複製鑰匙交給朋友，然後再把秘密放在對應的鎖盒中轉交給他。就算有人攔截了鎖盒，在沒有鑰匙的情況下，他們也很難看到您的秘密。如果有人嘗試以外觀類似的鎖盒來替換，您就會發現鑰匙無法正常打開盒子。SSL/TLS 的運作原理也是這樣，只是把鎖盒換成了網站。

瀏覽器的安全性指標也會交流擴充驗證 (EV) 憑證資訊。獲得 EV 憑證的網站必須向認證機構證明自己的身分。在瀏覽器中，有時候 EV 指標會以網站名稱的形式顯示，或是網址列旁的註冊實體。
如果您對特定網站的內容有所懷疑，您可以點擊「View Certificate」（查看憑證）以檢查憑證上的網址是否符合瀏覽器上顯示的網址。[可以考慮在投影畫面中向學員示範如何尋找「View Certificate」。]
每個瀏覽器導覽至這個功能的方法都不太一樣。舉例來說，在 Chrome 瀏覽器中依序點擊「檢視」、「開發人員選項」與「開發人員工具」。
在「開發人員工具」中，依序點擊「Security」標籤與「View Certificate」。

講授內容

在連接新的網絡時，應該考慮哪些事？

1. 可能的答案包含：地點（或擁有這個網絡的人）、存取（或誰也在使用這個網絡），以及活動（或您要利用這個網絡做些什麼事）。

誰是您家用 Wi-Fi 網絡的持有人？學校的呢？咖啡室的呢？

1. 您的家長 / 照護者擁有家用的 Wi-Fi 網絡、行政主管和 / 或區域擁有學校的網絡，而咖啡室老闆擁有咖啡室的網絡。

這些人您都認識嗎？您信任這些人嗎？

1. 邀請學員討論他們對於這些對象的信任有何不同。

講授內容

您應該要認識並信任 Wi-Fi 擁有網絡的人。有時候您可以透過網絡的 SSID 瞭解擁有人的身分。

服務設定識別碼 (Service Set Identifier, SSID) 是持有人賦予 Wi-Fi 網絡的名稱，您嘗試連結的時候就能看到。SSID 通常會用於表達網絡持有人的身分，以及其他與網絡相關的細節。但別掉以輕心，幾乎所有人（我是不知道怎麼做啦）都可以創建 SSID。例如有人可能會建立和您的學校網絡一模一樣的 SSID。這種例子是為了假冒已知且受信任的網絡，藉此竊取他人的用戶名稱與密碼。

知道網絡的持有人身分可以幫助您判斷這個網絡是否安全。如果網絡屬於您信任的對象或組織，那麼您就可以安心連線。但如果是未知的網絡，建議最好不要連線，因為您不知道誰是路由器的主人。因為網絡上的所有流量都會通過路由器，路由器的持有人可能會監測或記錄您的網站流量。

連線 Wi-Fi 時，您的裝置會連上當地的裝置網絡，然後該網絡又會連到一個更大的互聯網。因為您的裝置會和這個網絡互換資訊，所以您一定要能夠信任其他共同連線的裝置，也就是這個網絡上的所有裝置。就如同是您在學校做分組作業，您一定會希望能夠信任其他同組的組員！

在網絡上套用密碼可以限制連結這個網絡的對象。這就表示比起完全開放的網絡，您可以更清楚有誰在使用這個網絡，例如您的家人、朋友或咖啡室的其他顧客。

無論您是否決定要連上看似可疑的網絡，最終還是要取決於您願意為保護網絡安全做出多少犧牲。您可能會不知道如何權衡「帳戶可能被入侵」與「使用網絡的便利性」，哪一個比較重要？

講授內容

您可以使用家用 Wi-Fi 網絡閱讀網上新聞 / 網誌嗎？學校的呢？咖啡室的呢？

1. 說明該網頁上的內容通常都不是敏感資訊。使用哪一個網絡應該都沒有關係。

您可以使用家用 Wi-Fi 網絡傳送信用卡號碼嗎？學校的呢？咖啡室的呢？為什麼？

1. 鼓勵大家參與討論：為什麼使用家用 Wi-Fi 從事這類行為最保險，而絕不要使用咖啡室的 Wi-Fi。另外順便討論：雖然學校的網絡比較值得信任，但最好不要冒險嘗試，因為信用卡屬於極度敏感的資訊。

您可以使用家用 Wi-Fi 網絡查看個人的電郵嗎？學校的呢？咖啡室的呢？

1. 鼓勵大家討論：取決於電郵帳戶的內容，使用家用 Wi-Fi 從事這類行為可能還是最保險的選項。舉例來說，有人可能會針對不同的用途而使用多個電郵帳戶（例如：一個帳戶是存放營銷 / 推廣電郵；另一個存放親朋好友的電郵）。

講授內容

包含密碼與銀行資訊等等的敏感資訊，最好是利用私人且安全的網絡傳送 / 檢視資料

，瀏覽網站時也要使用 SSL/TLS，絕對不要使用共用的公共網絡。如果有其他您不認識或不信任的對象也在使用這個共用的公共網絡，那麼您提交或存取的私密資訊將有外流的風險。

有時候敏感與非敏感資訊之間的界線並不明確，因為私隱是您個人必須自行判斷並做出的抉擇。所以一定要考慮每一種可能發生的後果，然後才決定是否應該連接網絡。在決定連線之前，請詢問自己是否信任網絡的持有人、其他共用網絡的對象、您要從事的網上活動以及您要分享的資訊。

安全與不安全的網絡

第一部分

課堂互動

請注意：這個活動的部分內容在「活動 #2：選擇 Wi-Fi 網絡。」
您可以自行判斷是否要再次討論這些資料或選擇跳過。

講授內容

我們之前已經介紹過所謂不安全的 Wi-Fi 網絡就是指那些不需要密碼就能登入的網絡。使用不安全的網絡會對您在網上傳輸與接收的資料造成風險。

安全的 Wi-Fi 網絡是指那些需要密碼且啟用加密功能的網絡。配置網絡的用戶可以選擇是否要啟用加密功能。加密功能會雜湊您在網絡上傳送與接收的資訊，讓使用同一個 Wi-Fi 網絡的駭客難以窺探您傳送或接收的資訊。

即使網絡是安全的，也不代表您的資料就是安全的。雖然一定比使用不安全的網絡更加保險，但有決心的駭客依然可以找到其他方式來存取您的資訊。

Wi-Fi 網絡有三種常見的加密協定：「有線等效加密」(Wired Equivalent Privacy, WEP)、「Wi-Fi 保護協定」(Wi-Fi Protected Access, WPA) 或 WPA2。WEP 與 WPA
都已經過時，使用這兩種保護協定的網絡都應該被視為不安全的網絡。此外，WPA2 也已經被證實有安全漏洞。

為了盡可能確保資訊的安全，請檢查您使用的網站是否有使用 SSL/TLS 進行加密。

講授內容

有沒有人可以舉出曾經用過以密碼保護的網絡範例？

1. 部分範例包含自家的 Wi-Fi、學校的 Wi-Fi 以及部分公共地點的 Wi-Fi 網絡，例如咖啡室。

有沒有人可以舉出曾經用過不安全的網絡範例？

有沒有安全的網絡範例？

講授內容

您可以檢視裝置的網絡或無線設定，以查看 Wi-Fi 網絡是否加密。

第二部分

課堂互動

開始教學這個部分之前，請先上網研究，查看不同的作業系統如何檢查 Wi-Fi 網絡的加密類型。然後向學員展示如何查看網絡使用的加密類型。例如，在 MacOS 上點擊系統偏好設定 -> 網絡 -> 選擇 Wi-Fi -> 選擇適當的網絡名稱。在「Wi-Fi」標籤中，會出現一串已知網絡的清單，以及一個顯示加密類型的欄位。

講授內容

並非所有的連線都一樣。如果是不安全的網絡，任何人都可以連上該網絡，但我們不清楚是誰在控制這個網絡。使用不安全的網絡會讓自己冒很大的風險，因為如果您沒有使用 SSL/TLS 連線，您傳送與接收的資訊（例如您的網站流動：網頁、密碼等等）很可能就會被其他使用相同網絡的人看到。

課堂互動

取決於學員的技術背景知識，您可以嘗試討論使用 VPN（虛擬私人網絡）作為使用 Wi-Fi 的另一層保護措施。請在「資源」區塊參考 VPN 連結以獲得更多的資訊。

認識網絡安全

標題部分

課堂互動

將學員分成 2-3
人一組。分發「網絡安全：學員講義」，然後為各組指定一個情境。給各組 5 分鐘的時間討論自己的情境。之後要求各組分享他們的回應。講義上的答案會以綠色字體顯示。

作業

第一部分

作業

要求學員：

1. 畫一條日常生活的時間軸，然後標記他們連線的 Wi-Fi 網絡。

2. 透過時間軸上標記的網絡，讓學員選擇其中兩個，然後以簡短的段落分別描述這兩個網絡，還有誰也連結這些網絡？這些網絡安全性多高？

3. 此外，針對學員剛剛選擇的那兩個網絡，要求學員描述連線時所產生的機會與風險。