公共 Wi-Fi

學員將可瞭解什麼是公共 Wi-Fi
網路，及其優點和風險。更明確來講，他們可以學到如何在提供 Wi-Fi
服務的場所，識別該 Wi-Fi 網路是否安全；瞭解使用不安全的 Wi-Fi
會伴隨哪些利弊得失；並針對何時該連線和使用不安全的 Wi-Fi 做出正確決定。

教材

「上網安全」講義

資源

無線數據機圖像

什麼是 Wi-Fi？

第一部分

講授內容

您使用哪些裝置上網？

這些裝置是透過什麼方式上網？

Image Class Interaction

Wi-Fi 是裝置連上網路常用的方法之一，它利用無線電訊號來連結裝置，讓裝置無需透過實體連線或有線網路即可上網。

假設您想利用家裡的三部筆記型電腦上網，這時您需要有下列設備才能順利連上網路：

1.存取點（AP）：任何可傳輸（或廣播）Wi-Fi 訊號和提供網路存取服務的裝置即為存取點。您的裝置必須接收到這些訊號才能連線到網際網路。有時，您可能需要取得特殊權限（例如用戶名稱和密碼），才能登入使用 AP 廣播的無線訊號。

2.路由器：路由器這種裝置可以建立區域網路，供特定地點（例如學校、圖書館或住家）的所有裝置（例如電腦、平板電腦、手機）使用。一般來說，路由器會內建 AP（見上方圖表）。

> 路由器有覆蓋範圍限制，距離通常不會太遠，因此如果您的裝置離路由器太遠，您收到的 Wi-Fi 訊號就會很微弱，甚至收不到訊號。此外，如果您和路由器之間受到某物（例如建築或磚牆）阻隔，也會使訊號強度減弱。
>
> 雖然連線到路由器可以連上區域網路，但不代表可以使用網際網路。若要讓區域網路中的多個裝置可以連上網際網路，路由器必須連接到數據機。

3.數據機：數據機這種裝置可與網際網路服務供應商（ISP）建立並保持連線，以便讓用戶連上網際網路。數據機可將外來訊號轉換成電腦和其他數位裝置可讀取的訊號。

> 一般常見的配置是，AP 和路由器為同一裝置，並透過乙太網路線這種特殊傳輸線連接到數據機，這就是所謂的「有線」網際網路連線。
>
> 行動裝置若無法連上學校、圖書館或住家的區域網路，也可以使用行動數據連線來上網。行動數據連線是一種無線電訊號，其覆蓋範圍比路由器要大上許多。行動數據連線會透過無線電收發機，也就是基地台，將用戶的行動裝置連線到網際網路。

第二部分

講授內容

Wi-Fi 有什麼優點？

Wi-Fi 有哪些缺點？

比起有線網際網路連線，使用 Wi-Fi 會有哪些安全疑慮？

為何離開特定地點後，手機的 Wi-Fi 連線會中斷？

選擇 Wi-Fi 網路

第一部分

講授內容

所有的 Wi-Fi 網路都安全嗎？為什麼？

講授內容

有時，您可以選擇想要使用哪一個 Wi-Fi 網路。切記，如果您連線到不安全的網路，可能會為自己招來巨大風險。舉例來說，無需密碼即可登入者就是不安全的 Wi-Fi 網路。如果您使用不安全的網路，該網路上其他人可能會擷取您的資訊，例如竊取您透過網路傳送的資訊，或監視您的一舉一動。

另一方面，如果網路需要密碼才能登入、已啟用加密功能，或是您登入的網路確實與網路名稱相符，就是安全可信任的 Wi-Fi 網路。比方說，如果您不小心登入假冒您學校網路名稱的網路，可能會導致帳號資訊洩漏。所以說安全可信任的 Wi-Fi 網路，才能為用戶提供最嚴密的防護。

使用 Wi-Fi 網路時要考慮到環境或地點。舉例來說，某天您在電影院搜尋 Wi-Fi 網路連線，結果手機出現您學校的網路名稱，您應該要想到這個網路企圖透過模仿或「假冒」您學校的網路，以便從沒有警覺心的學生身上收集密碼。

設定使用密碼保護的 Wi-Fi 網路時，擁有者應選擇開啟路由器的加密協定。常見的加密協定包括有線等效加密（WEP）、Wi-Fi 保護存取（WPA）和 WPA2。這些協定可為透過無線網路傳送的資訊加密或「加擾」。

為資訊加密後，會增加駭客破解您傳送內容的難度。不過，事實證明這些協定（WEP、WPA 和 WPA2）也無法完全抵禦駭客入侵。因此，透過網路傳送資訊時，還是要使用安全的網路連線才有保障。

HTTPS 是一種標準，可讓網站將資料加密，再將加密後的資料透過網路傳送。將資料加密可防止任何第三方輕易查看來自您網路連線的資料，只要在您使用的網址前面加上「https://」，即可提供額外的安全保障，且適用於任何瀏覽器，例如 https://www.mysite.com。然而，不是所有網站皆支援 HTTPS。

1. 您應該只在開頭是 HTTPS:// 的網頁輸入敏感資料（如密碼、信用卡資料）。

2. 大部分的瀏覽器在網址列附近會顯示一個安全標誌，表示該網頁使用 HTTPS 連線。

3. 不過有些惡意網站也支援 HTTPS，因此 HTTPS 並無法完全保障您的安全。此外，HTTPS 可以確保網路連線的安全，但無法保證網站不會做出意圖不軌的舉動。

講授內容

用於確保 HTTPS
安全無虞的技術，稱為安全通訊端層（SSL）/ 傳輸層安全性（TLS）。SSL / TLS 使用數位加密金鑰，其作用類似真正的鑰匙。如果您把祕密寫在紙上再交給朋友，那麼只要是發現這張紙的人，都會看到您的祕密；不過想像一下，如果您先將鑰匙親自交給朋友，再將祕密鎖在那把鑰匙才能打開的盒子裡，然後將盒子寄給朋友，那麼就算有人攔截了盒子，只要他們沒有鑰匙，就無法窺見您的祕密。此外，如果有人把您的盒子調包成另一個類似的盒子，但是因為您的鑰匙開不了假盒子，您就能知道這不是您原本的盒子。SSL / TLS 的運作方式也是同樣的道理，只是應用在網站上。

瀏覽器安全標誌也能提供延伸驗證（Extended Validation，EV）憑證資訊。網站必須先向憑證機構證明自己的身分，才能取得延伸驗證憑證。在瀏覽器上，延伸驗證憑證有時會以網站名稱或註冊實體顯示在網址列旁邊。 若您不確定某個網站的內容是否安全，可以點擊「檢視憑證」，檢查瀏覽器顯示的網址是否與憑證上的網址相符
[建議使用投影布幕向學員示範找到「檢視憑證」的操作步驟]。
各家瀏覽器前往「檢視憑證」的路徑不一樣。以 Chrome
為例，請點擊「檢視」下方的「開發人員」，然後點擊「開發人員工具」。
進入「開發人員工具」後，依序點擊「安全性」頁籤和「檢視憑證」。

講授內容

連線到任何網路時，應考慮哪些事項？

1. 可能的答案包括：地點（即網路擁有者）、存取權限（即還有誰也連線到這個網路），以及活動（即您會在網路上做什麼事）。

家裡的 Wi-Fi 網路歸誰所有？學校和咖啡廳的 Wi-Fi 網路又各是歸誰所有？

1. 您家裡的 Wi-Fi 網路歸父母 / 照顧者所有，學校網路是歸管理員和 / 或校區所有，咖啡廳的網路則歸店家老闆所有。

您認識這些人嗎？您信任這些人嗎？

1. 請學員討論他們對這些人的信任程度會有何不同。

講授內容

您應該要認識並信任 Wi-Fi 網路擁有者。有時，您可以利用網路的 SSID
來識別擁有者是誰。

服務組識別元（SSID）是擁有者為 Wi-Fi
網路指定的名稱，當您嘗試連線到網路時就會看到這項資訊。我們通常可透過 SSID 來辨識網路擁有者，並可獲得其他相關詳細資料。但請小心，只要知道方法，幾乎任

何人都能建立 SSID。例如，有人可能會建立與您學校網路完全一致的 SSID。這就是假冒已知可信任網路的例子，為的是收集用戶名稱和密碼。

知道網路擁有者是誰，有助於您判斷網路是否安全。如果網路為您所信任的人或組織所有，那麼您就能安心地連線。但如果是未知網路，便無從得知自己連上的路由器是為誰所有，因此建議您不要連線，因為該網路所有流量都會經過路由器，擁有者可能正在監視或記錄您的網路流量。

連線到 Wi-Fi 時，您的裝置會連線到裝置共用的區域網路，而該區域網路則會連線到更寬廣的網際網路。由於您的裝置會與這個網路交換資訊，因此一定要能夠信任與您相連結的所有其他裝置才行。這就像是在學校進行團隊合作，您必須信任其他合作夥伴，才有辦法互相配合！

為網路設定密碼，可以限制誰有權限連線到網路。這樣比起完全開放的網路，您會比較清楚有哪些人（例如家人、朋友或咖啡廳的客人）連線到網路。

要不要加入有安全疑慮的網路，全看您權衡是否願意犧牲網路安全。您可以權衡一下是否該為了上網方便，加入可用的網路，讓自己暴露在帳號被盜的風險之中。

講授內容

您應該使用家中 Wi-Fi 網路閱讀網路新聞 / 部落格嗎？用學校的 Wi-Fi 可以嗎？用咖啡廳的 Wi-Fi 網路呢？

1. 解釋說一般的網頁內容並非敏感資訊，因此基本上可以在任何網路上閱讀這些內容。

您應該使用家中 Wi-Fi 網路傳送信用卡卡號嗎？用學校的 Wi-Fi 可以嗎？用咖啡廳的 Wi-Fi 網路呢？為什麼？

1. 請學員一起討論為什麼想要透過網路傳送這類敏感資訊時，最安全的方式是使用家中 Wi-Fi 網路，而非咖啡廳 Wi-Fi 網路。另外，儘管學校網路可能值得信任，但仍不值得冒險傳送這類高度敏感的資訊，請討論其中的原因。

您應該使用家中 Wi-Fi 網路查看個人電子郵件嗎？用學校的 Wi-Fi 可以嗎？用咖啡廳的 Wi-Fi 網路呢？

1. 討論為何查看個人電子郵件時，最安全的方法可能是使用家中網路，不過這還得視電子郵件帳號內容而定。舉例來說，有些人會因應不同用途使用多個電子郵件帳號，例如有個帳號是專門接收行銷 / 促銷訊息，而與家人朋友聯絡時則用另一個帳號。

講授內容

傳送 / 查看敏感資訊（包括密碼和銀行資訊）時，最好使用安全的私人網路，以及使用 SSL / TLS 加密協定的網站，千萬不要使用共用的公共網路。使用公共網路傳送或查看這類私人資訊會伴隨一定風險，因為還有其他您不認識且不信任的人正在使用這個網路。

我們很難明確定義某項資訊的敏感程度，因為保護隱私的決定權掌握在您自己手裡。每個情況都必須各別去考慮，以決定是否應該連線使用網路。您可以先問問自己是否信任網路擁有者、其他網路共用者、您會透過網路做哪些事情，以及您會分享哪些資訊，再決定是否連線到網路。

安全與不安全的網路

第一部分

課堂互動

請注意：本活動部分內容與「活動 2：選擇 Wi-Fi 網路」有所重複。
您可自行評估，決定要使用本教材或略過。

講授內容

我們先前提過，無需密碼即可登入者就是不安全的 Wi-Fi
網路。使用不安全的網路，將使您透過網路傳送和接收的資料暴露在風險之中。

安全的 Wi-Fi 網路不僅需要使用密碼登入，而且會啟用加密功能。設定該網路的人可以選擇是否啟用加密功能。加密功能會對您透過網路傳送和接收的資料進行加擾，因此使用同一個 Wi-Fi 網路的駭客較難看出您傳送或接收哪些資料。

但使用安全網路不代表您的資料就安全無虞。這當然比使用不安全的網路更為安全，不過只要駭客鍥而不捨，仍會有辦法取得您的資訊。

Wi-Fi 網路有三種常見的加密協定：分別是有線等效加密（WEP）、Wi-Fi
保護存取（WPA）和 WPA2。WEP 和 WPA
已過時，因此使用這兩種協定的網路應視為不安全的網路。此外，我們發現 WPA2
也無法完全抵禦駭客入侵。

為確保您的資訊受到最嚴密的保護，請查看您造訪的網站是否使用 SSL / TLS
加密協定。

講授內容

誰有印象自己曾使用過哪些受密碼保護的網路？請舉例。

1. 比方說自家 Wi-Fi、學校 Wi-Fi 和咖啡廳等公共場所的 Wi-Fi 網路。

誰有印象自己曾使用過哪些不安全的網路？請舉例。

又有哪些是安全的網路？請舉例。

講授內容

您只要查看個人裝置上的網路或無線網路設定，就能知道特定 Wi-Fi 網路是否加密。

第二部分

課堂互動

進入這部分學習課程之前，請進行網路搜尋，為學員複習如何查看不同作業系統的 Wi-Fi 網路加密類型。然後，示範如何查看網路使用的加密協定類型。比方說，如果是 MacOS 裝置，請依序按一下「系統偏好設定」->「網路」，然後依序選擇 Wi-Fi 和適當的網路名稱。「Wi-
Fi」頁籤之下會列出已知的網路，而且會有一列指出各個網路所用的加密類型。

講授內容

並非所有網路連線都同樣安全。如果是不安全的網路，任何人都能連線到這個網路，而且難以確定此網路是由誰管理。加入不安全的網路會使您暴露在危險之中，因為如果您不是使用 SSL / TLS 連線，您傳送和接收的資訊（例如粉絲專頁、密碼等網路流量）有可能會被該網路上任何人看到。

課堂互動

如果學員具備足夠的科技知識，您可以和他們討論如何在使用 Wi-Fi
時，利用虛擬私人網路（VPN）多加一道安全防護。請參閱「資源」部分的 VPN
連結，取得更多資訊。

認識上網安全

第一部分

課堂互動

將學員分成 2-3
人一組。將上網安全講義發下去：發講義給學員，並為各組指派一個情境題。給學員 5 分鐘針對情境題進行討論，時間到了之後，請各組分享他們的討論結果。答案會在講義上以綠色標示。

作業

第一部分

作業

要求學員完成以下作業：

1. 請學員畫出平常一整天的行程時間表，並標記他們所連線的 Wi-Fi 網路。

2. 請學員從日常選用的網路中選出兩個網路，並簡短說明他們使用的網路，例如還有哪些人會連線到這個網路。這個網路是否安全？

3. 另外，請學員針對所選的兩個網路，說明在什麼機會下會連線到這些網路，及其可能伴隨的風險。