

CHAPTER 13

資訊安全與網路議題



INTERNET

本章摘要

13-1 資訊安全基本概念

- 13-1-1 資訊安全三要素
- 13-1-2 資訊安全管理系統
- 13-1-3 資訊安全的種類



INTERNET

13-2 惡意程式的威脅與防範

- 13-2-1 惡意程式的威脅
- 13-2-2 惡意程式的防範



INTERNET

13-3 駭客的威脅與防範

- 13-3-1 認識駭客
- 13-3-2 常見的駭客攻擊手法
- 13-3-3 預防駭客入侵的措施
- 13-3-4 零信任架構



INTERNET

35

13-4 網路交易安全

- 13-4-1 資料加解密技術
- 13-4-2 SSL與SET
- 13-4-3 FXML憑證
- 13-4-4 零知識證明



INTERNET

13-5 網路帶來的影響與衝擊

- 13-5-1 資訊超載與資訊焦慮
- 13-5-2 網路謠言及假訊息
- 13-5-3 網路犯罪
- 13-5-4 區塊鏈的隱憂
- 13-5-5 暗網



INTERNET

13-1 資訊安全基本概念

13-1-1 資訊安全三要素

13-1-2 資訊安全管理系統

13-1-3 資訊安全的種類

INTERNET

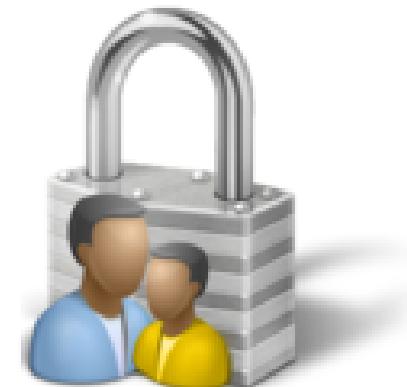
13-1-1 資訊安全三要素

- 資訊安全的組成主要包含了機密性、完整性及可用性等三要素，這三要素為資訊安全的三個原則，簡稱為CIA。
- 任何違反三原則的事件行為，都會造成資訊安全的問題，而對企業資產或機密資料造成威脅。

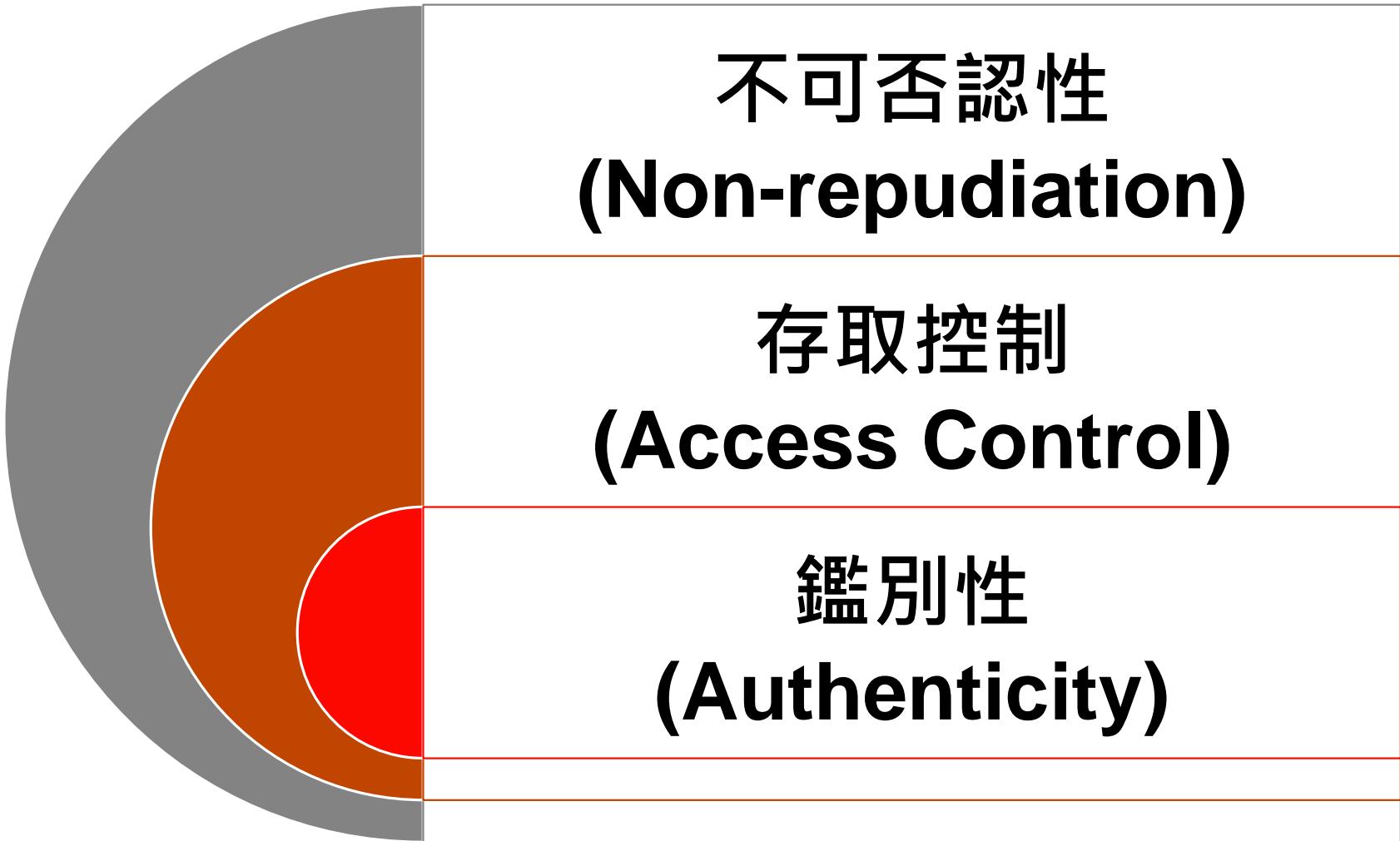


13-1-1 資訊安全三要素

- 資訊安全三要素關係是互相影響的，例如機密性越高，就會造成完整性與可用性的降低，若需要高可用性的系統，則會讓機密性與完整性降低，因此如何在有限資源下，讓三者保持平衡是每個企業需要面對的議題。
- 另外還衍生出不可否認性、存取控制、鑑別性三個安全性要素，讓資訊安全更完善。



13-1-1 資訊安全三要素



13-1-2 資訊安全管理系統

- 資訊安全管理系統 (Information Security Management System, ISMS) 目的在於保護資訊資產的機密性、可用性及完整性。
- 是一套有系統地分析和管理資訊安全風險的方法。
- 目標是透過控制方法，把資訊風險降低到可接受的程度內，遭受攻擊時，系統仍可維持正常運作的能力。

13-1-2 資訊安全管理系統

ISO 27001

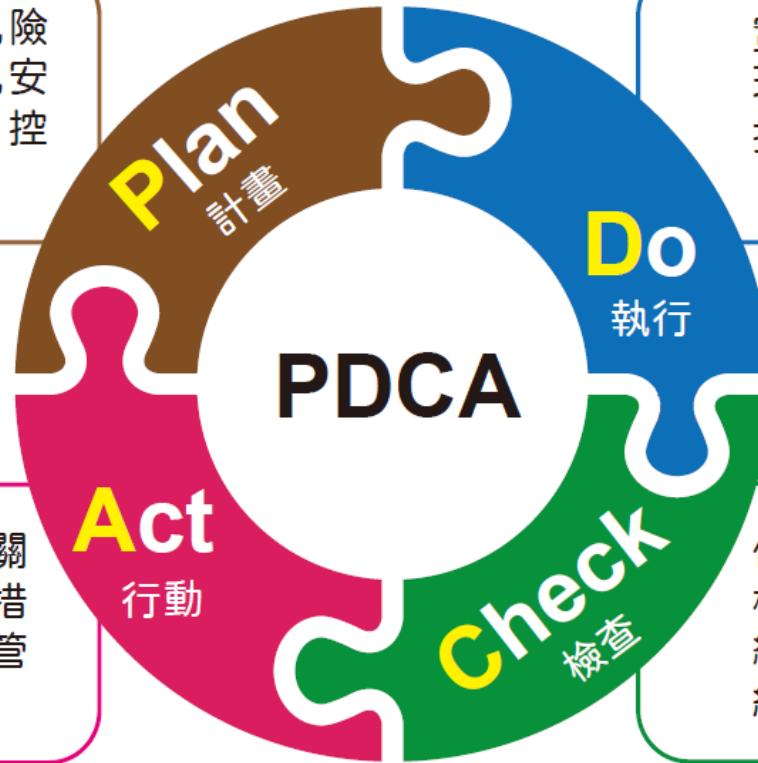
- ISO 27001 是一套經過國際標準組織(ISO)認證，且通用的資訊安全管理制度標準。
- 中文完整名稱為「資訊科技—安全技術—管理系統—要求事項」。
- 因為它是由國際標準組織與國際電工委員會聯合發布，因此有時也會寫作ISO/IEC 27001。

13-1-2 資訊安全管理系統

- ISO 27001採用PDCA (Plan-Do-Check-Act)流程建構ISMS系統的準則，透過不斷的審視與改進，能夠及時發現資安系統的缺陷與不足，並做出修補，將資訊安全風險降至可接受的範圍，保護資訊的機密性、完整性與可用性。
- PDCA是指「計畫—執行—檢查—行動」的過程，在一開始的計劃階段，組織必須要建立符合營運目標的ISMS政策，並說明資訊安全的目標、需要透過哪些指標去衡量成效，以及管理階層應該擔負的責任。

13-1-2 資訊安全管理制度系統

建立管理資訊安全風險的目標，及改進資訊安全系統的相關政策、控制措施。



實際執行資訊安全管理系統的政策及控制措施。

依據審查結果，或相關資訊採取矯正與預防措施，以達成資訊安全管理系統的持續改進。

依據ISMS政策及目標，評鑑及測量實行績效，並將結果回報給管理階層審查。

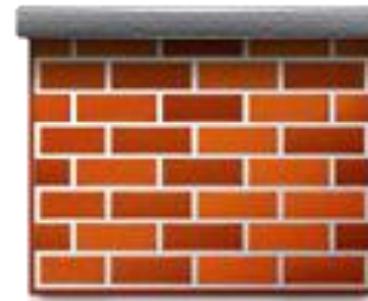
13-1-2 資訊安全管理系統

- 資訊安全是一個管理過程，而不是一項技術導入過程。
- 維護資訊安全並不單只是資訊人員的責任，還牽涉到企業流程和員工資安意識，員工若沒有資安概念會威脅到整個組織。
- 資訊安全要成為所有人員必須遵守的規範，建立員工資訊安全意識。
- 唯有人員都具備了資訊安全的警覺與防護意識，才能降低資安事件發生的可能。

13-1-3 資訊安全的種類

硬體安全

- 硬體的安全包含對於硬體環境的掌握以及設備管理，如建築物與週遭環境的安全考量、硬體環境控制、天然災害控制、人為破壞管理控制等。
- 電腦應設置於通風良好、乾燥之冷氣房中，勿直接曝曬陽光，機房應選用耐火、絕緣、散熱性良好的材料，並擺放防火滅火設備，嚴禁易燃易爆物品。



13-1-3 資訊安全的種類

- 天然災害可能會造成軟、硬體的損壞，導致整個資訊系統失靈。
- 預防資料被毀損最好的方法就是時常將電腦中的資料進行備份，而這些備份的資料，最好做到異地備份，儲存於不同媒體中或是別的地方。

完整備份 (Full Backup)

- 將所有的程式、檔案及資料全部進行備份。

差異備份 (Differential Backup)

- 只針對上一次完整備份後有變更的檔案進行備份。

增量備份 (Incremental Backup)

- 只針對上一次完整備份或增量備份後有變動的資料進行備份。

13-1-3 資訊安全的種類

軟體安全

- 包含資料軟體安全和通訊管道的安全性。
- 現今在工作及生活中，都非常依賴各種軟體來完成工作，因此當軟體環境被入侵或因感染病毒等異常狀況時，對使用者或企業都影響很大。
- 軟體安全在防護上要防止被入侵及資料被竊，定期更新軟體、安裝防毒軟體等，都是防護的必要措施。

13-1-3 資訊安全的種類

資料安全

- 對於各種的資料處理，應該抱著謹慎態度去面對，切勿在網路上分享或是存放機密資料。
- 各項資料在進行輸入輸出時，最好能設定密碼管理制度，並時常更新密碼，以確保資料不會外流。對於重要性及機密性較高的資料，應加設資料存取控制，以防止資料外流。
- 若資料輸入須委外處理時，可以將資料分成數部分交給多人繕打，以提高安全性。

13-2 惡意程式的威脅與防範

13-2-1 惡意程式的威脅

13-2-2 惡意程式的防範



INTERNET

13-2-1 惡意程式的威脅

- 惡意程式(Malicious Code)是指所有不懷好意的程式碼。



13-2-1 惡意程式的威脅

電腦病毒(Computer Virus)

- 是由意圖不軌的人所撰寫的程式。
- 電腦中毒後所遭受的破壞也會有所不同，輕則損失一些檔案，重則損毀整個硬碟，導致無法再啟動電腦。
- 電腦病毒在發作前都會有一些徵兆，例如：程式執行速度突然變慢了、檔案的大小、日期改變了、出現一些奇怪的錯誤訊息或快顯視窗、出現不明的常駐程式或檔案、無故佔用記憶體、使程式無法被載入執行等。

13-2-1 惡意程式的威脅

- 電腦病毒的傳播途徑主要有：



經由來路不明的儲存裝置



經由電子郵件



點擊廣告網頁或連結



任何可以儲存資料、傳輸資料的地方都有可能是病毒傳播的途徑

13-2-1 惡意程式的威脅

電腦蠕蟲(Worm)

- 可以自我複製出許多「分身」，並透過網路連線或電子郵件等方式進行散播。
- 與電腦病毒不同的是，它通常不會感染其他檔案，其主要危害在於引發一連串的指令或動作，佔用大量電腦資源或網路頻寬，進而癱瘓電腦主機、網路或郵件伺服器。



13-2-1 惡意程式的威脅

特洛伊木馬(Trojan Horse)

- 是一種透過網路的遠端遙控程式。
- 通常潛伏在惡意網頁中，或是偽裝成有趣的小程式，吸引使用者下載或執行，然後伺機在受害者電腦中安裝惡意程式，使入侵者具有與電腦使用者相同的權限，並藉此執行一些惡意行為，像是刪除檔案、竊取密碼與機密資料、或利用受害電腦進行非法行為等。

13-2-1 惡意程式的威脅

間諜程式(Spyware)

- 是在使用者不知情、且未經使用者同意的情況下，自行將軟體安裝在使用者電腦中，並觀察使用者的使用行為與監督電腦活動。
- 有些間諜軟體則會取得使用者的帳號、密碼等資訊，進行不法勾當。若電腦中被安裝了間諜程式，可能會出現以下的徵兆：
 - 電腦運作的速度變慢。
 - 常常不定時會出現快顯廣告視窗。
 - 電腦中的設定突然更改，且無法改回原來設定。
 - 網頁瀏覽器突然安裝了不明附加元件。

13-2-1 惡意程式的威脅

邏輯炸彈(Logic Bombs)

- 是特洛伊木馬的一種，它會因某特定事件而進行攻擊。
- 例如：某程式設計師在某系統中植入了邏輯炸彈，若該程式設計師被公司資遣，便會啟動破壞行為。



13-2-1 惡意程式的威脅

無檔案病毒(Fileless Malware)

- 是潛藏在電腦記憶體內的惡意軟體，因此不容易被察覺。
- 在不被察覺下透過特製的PowerShell腳本直接寫入電腦記憶體，一旦取得存取權限，會讓系統偷偷執行命令。
- 由於是在記憶體中執行，只要受害者的電腦重新開機，記憶體中的惡意軟體和所有可供偵測及入侵後鑑識調查的證據都會隨之遭到清除。

13-2-1 惡意程式的威脅

垃圾郵件(Spam)

- 是指未經電子郵件收信者同意或訂閱而大量寄發的電子郵件，郵件內容通常是一些無用的商業廣告、販賣盜版光碟或色情光碟、網路賭博，甚至其中還可能夾帶病毒。
- 當收件者一開啟電子郵件收件匣，收到大量不具參考價值的郵件，不但耗用網路資源，也對收件者造成困擾。



13-2-1 惡意程式的威脅

勒索軟體(Ransomware)

- 引誘受害人前往來歷不明的網站或程式，會將受害者電腦的檔案加密，並持有解鎖所需的密鑰，導致檔案無法存取，讓受害者無法自行復原，受害人要付款才可復原，否則將毀損解密金鑰。
- 常見的勒索軟體有**CryptoLocker**、**Locky**、**Petya**、**Cerber**、**GoldenEye**、**SMSLocker**、**KeRanger**、**Cuba**、**ALPHV**（又名**BlackCat**）、**Conti**、**Pysa**、**Maze**、**Hive**及**Vice Society**等。

13-2-1 惡意程式的威脅

- 勒索軟體的攻擊會迅速蔓延到整個企業，有些企業為了復原重要系統不得不付錢給攻擊者。



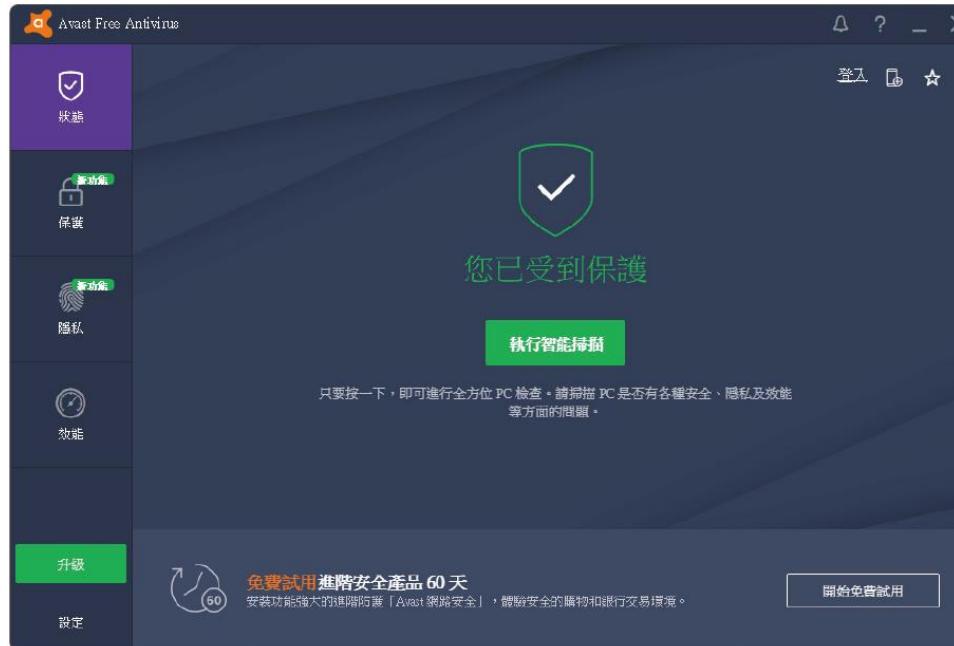
13-2-2 惡意程式的防範

防毒軟體

- 為了保障自己電腦的安全，最好在電腦中安裝一套防毒軟體，可用來檢測電腦是否遭受病毒感染，並清除已偵測到的病毒威脅。
- 防毒軟體掃毒的方式，是透過比對電腦中的檔案及防毒軟體中已登錄的病毒碼，來確認檔案是否遭到感染，因此必須常常要進行掃描引擎與病毒碼的更新，才能讓電腦得到最佳的保護。

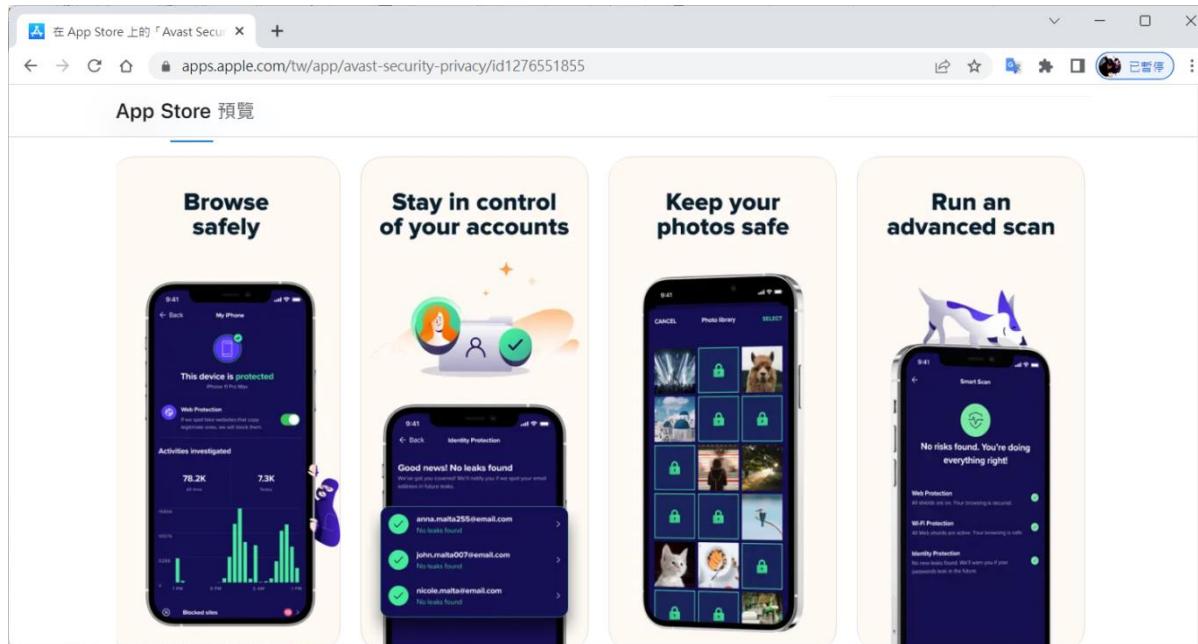
13-2-2 惡意程式的防範

- 防毒軟體有 PC-cillin 、 Norton AntiVirus 、 Kaspersky Anti-Virus 等，亦有免費的防毒軟體 ClamWin 及 Avast 可供下載使用。



13-2-2 惡意程式的防範

- 行動裝置防毒軟體，如 Lookout Mobile Security、Avast、ESET Mobile Security、AVG AntiVirus 等防毒App。



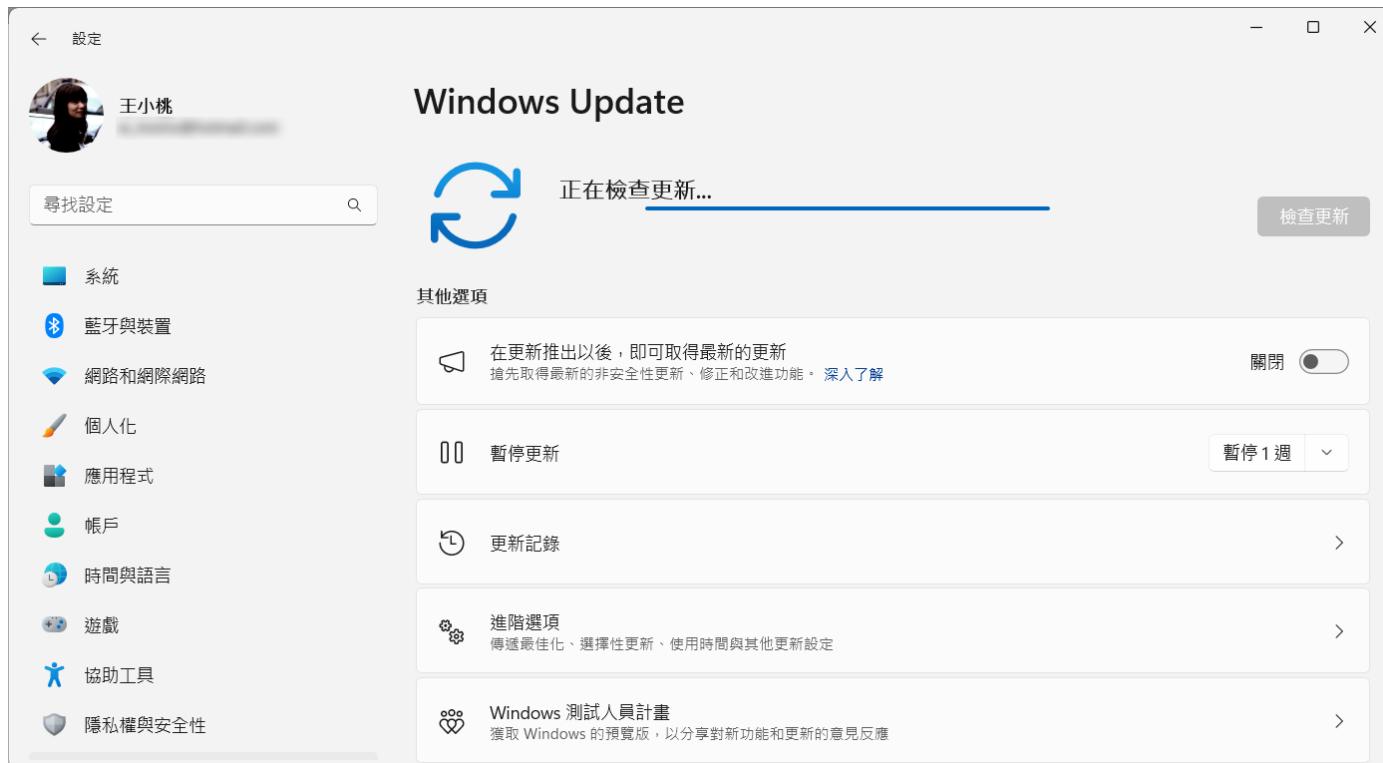
13-2-2 惡意程式的防範

作業系統與軟體更新

- 透過作業系統和軟體的更新，才能把系統的漏洞修補起來，減少被惡意程式入侵的機會。
- 以Windows作業系統為例，為了加強防範網路安全問題的發生，微軟會即時在發現Windows作業系統的安全性漏洞後，透過Windows Update的更新機制，提供使用者下載更新安全性修正程式。

13-2-2 惡意程式的防範

- 使用者也可以進入「Windows Update」項目視窗中，來檢查並執行系統的更新。



13-2-2 惡意程式的防範

勒索軟體的預防

四大症狀

- 出現不明對外連線。
- 各目錄下開始出現奇怪副檔名的檔案，例如 .crypt 、 .ECC 、 .AAA 、 .XXX 、 .ZZZ 等。
- 突然出現很多 Ransom Note 檔案(支付贖金的說明檔案)或捷徑，通常是 .txt 檔或是 .html 檔。
- 在瀏覽器工具列發現奇怪的捷徑。

緊急措施

- 立即切斷網路，避免將網路磁碟機或共享目錄上的檔案加密。
- 立即關閉電腦電源，不讓勒索病毒繼續加密電腦中的檔案，關機時間愈快被加密的檔案愈少，建議強制關閉電腦電源。
- 保留電腦，通報專業資安人員。
- 不要付錢。

預防方法

不

不上鉤

標題特別吸引
人的郵件務必
小心上鉤

不

不打開

不隨便開啟郵
件所附加的檔
案

不

不點擊

不隨便點擊郵
件附加的連結
網址

要

要備份

重要資料務必
要備份

要

要確認

開啟郵件請務
必確定寄件者
身分

要

要更新

一定要隨時更
新病毒碼

13-2-2 惡意程式的防範

養成良好的使用習慣

- 隨時注意特殊的檔案的長度與日期，以及記憶體使用情形，並重視電腦系統所發生的異狀。
- 不使用來路不明的檔案或盜版軟體。
- 不要隨便開啟來路不明的電子郵件。
- 任何可以儲存資料、傳輸資料的地方都有可能是病毒傳播的途徑，從網路上下載檔案也是電腦病毒的傳播途徑，下載檔案時，請確認該檔案是沒有病毒的。

13-3 駭客的威脅與防範



13-3-1 認識駭客

13-3-2 常見的駭客攻擊手法

13-3-3 預防駭客入侵的措施

13-3-4 零信任架構

INTERNET

13-3-1 認識駭客

- 駭客(Hacker)指的是非法入侵他人電腦系統中，竊取他人資料或篡改資料的人。



13-3-2 常見的駭客攻擊手法

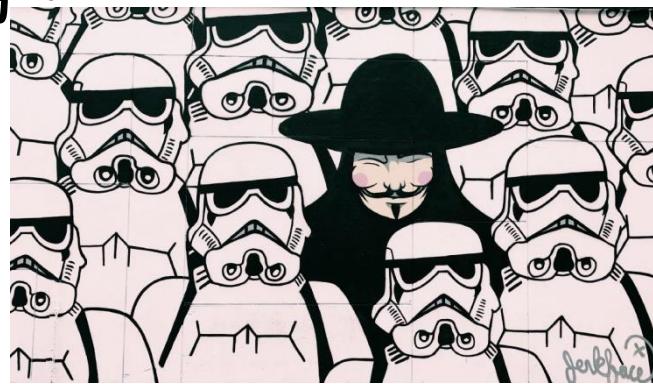
中間人攻擊(Man-in-the-Middle Attack)

- 簡稱MitM攻擊，是一種從中「竊聽」兩端通訊內容的攻擊手法，攻擊者能在客戶端與網站之間分別建立獨立的網路，並交換兩端所接收到的資訊，通訊的兩端以為雙方在直接對話，但事實上整個通訊的過程完全被攻擊者控制。
- 記得不隨意點擊來路不明的信件，並隨時注意網頁是以https進行連線。

13-3-2 常見的駭客攻擊手法

入侵網站

- 電腦駭客透過網路入侵他人的網站或電腦系統，篡改或盜取其中的資料或紀錄。
- 例如駭客非法入侵購物網站，竊取網站會員的個人資料或購物明細，再將這些資料轉手販賣或用以從事不法行為。



此相片 (作者: 未知的作者) 已透過 [CC BY-SA-NC](#) 授權

13-3-2 常見的駭客攻擊手法

殭屍網路

- 電腦駭客透過網路散播木馬程式，待集結大批受感染的電腦，形成殭屍網路(BotNet)之後，再遠端操控這些被控制的電腦，使其成為犯罪工具，進行惡意的攻擊行為，例如癱瘓他人電腦、濫發垃圾郵件，或竊取他人機密資料等。

13-3-2 常見的駭客攻擊手法

阻斷服務攻擊

- 阻斷服務(Denial of Service, DoS)攻擊主要目的是癱瘓系統主機或網站，使其無法正常運作。
- 電腦駭客會在同一期間發送大量且密集的封包至特定網站，迫使網頁伺服器因為一時無法處理大量封包而導致癱瘓，進而造成網路用戶無法連上該網站，而被阻絕在外。
- 分散式阻斷服務 (Distributed Denial of Service, DDoS) 它是透過網路上的多部電腦主機同時發動DoS攻擊，以分散攻擊來源。

13-3-2 常見的駭客攻擊手法

零時差攻擊(Zero-day Attack)

- 是指電腦駭客利用尚未被發現或公開的軟體安全漏洞，進行植入惡意程式等攻擊行為。
- 使用者應即時更新由軟體公司所提供的修補程式，避免讓駭客有機可乘。



13-3-2 常見的駭客攻擊手法

網站掛馬攻擊

- 電腦駭客會設立一個網站或部落格，以各種方式吸引民眾瀏覽，或是在一般正常網站中植入隱藏性的惡意程式，使用者若是瀏覽這些隱含惡意程式的網站，就有可能自動下載惡意程式到電腦中。



13-3-2 常見的駭客攻擊手法

網域名稱伺服器攻擊

- 電腦駭客會擅改網域名稱伺服器上的資訊，達到誤導使用者的目的。
- 例如駭客入侵某網站的DNS管理伺服器，篡改該網站的首頁紀錄，使得網友在登入網站時，被定向到另一個不知名的網址，而無法正常登入該網站。

13-3-2 常見的駭客攻擊手法

跨站腳本攻擊(Cross-Site Scripting, XSS)

- 是一種網頁漏洞攻擊方式，電腦駭客利用合法網站上的漏洞，在某些網頁中插入惡意的HTML與Script語言，藉此散布惡意程式，或是引發惡意攻擊。
- 當不知情的使用者在觀看這些網頁的同時，便引發這些惡意網頁程式的執行，導致瀏覽器自動下載網頁中隱含的惡意程式。

13-3-2 常見的駭客攻擊手法

鍵盤側錄程式(Key-logger)

- 是一種會記錄使用者所敲擊的鍵盤按鍵，竊取網路帳號密碼或機密檔案。
- 當受害者在電腦中輸入網路帳號及密碼時，鍵盤側錄程式會自動記錄鍵盤的鍵入及操作過程，並儲存在電腦中，再結合木馬程式將紀錄回傳給不法駭客集團。



13-3-2 常見的駭客攻擊手法

網路釣魚(Phishing)

- 是指不法人士透過E-mail或網路廣告，假冒知名網站的超連結來進行誘騙，將不知情的使用者引誘到他們所製作的冒牌網站，也就是所謂的「釣魚網站(Phishing Site)」。
- 釣魚網站的類型大多是知名的拍賣網站、網路銀行等，大多會設計得與合法網站幾乎一模一樣，讓使用者信以為真，然後藉由讓使用者在假冒的釣魚網站中輸入個人資料的同時，竊取帳號、密碼、信用卡號碼、身分證字號等個人機密資料。

13-3-2 常見的駭客攻擊手法

電子郵件炸彈(E-mail Bomb)

- 是指透過機器或程式碼，在短時間內不斷向同一郵件地址連續發送大量電子郵件，以癱瘓受害者的網路頻寬或郵件系統。



13-3-2 常見的駭客攻擊手法

密碼噴灑(Password Spraying)

- 指的是駭客用一個強度較弱的密碼去配對多個不同員工帳號，進而攻破帳戶入侵內部網路。



[此相片](#) (作者: 未知的作者) 已透過 [CC BY](#) 授權

13-3-2 常見的駭客攻擊手法

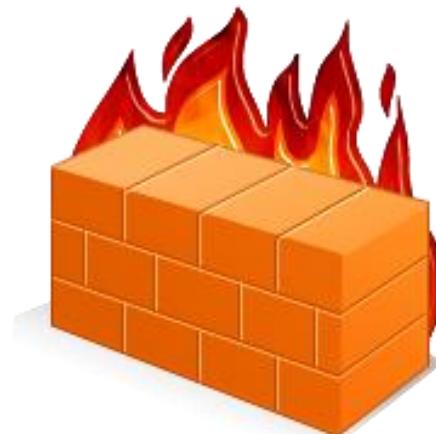
竊密軟體(RedLine Stealer)

- 主要是透過釣魚郵件或偽裝成安裝檔案的惡意軟體進行散布。
- 竊密駭客透過AI自動產生含惡意軟體連結的影片在YouTube散布，使用者一旦點擊影片說明欄偽裝成好康破解資源的惡意連結，就有可能被植入 Vidar 、 Redline 、 Vector Stealer 、 Titan Stealer 等竊密軟體，造成個資外洩。

13-3-3 預防駭客入侵的措施

防火牆(Firewall)

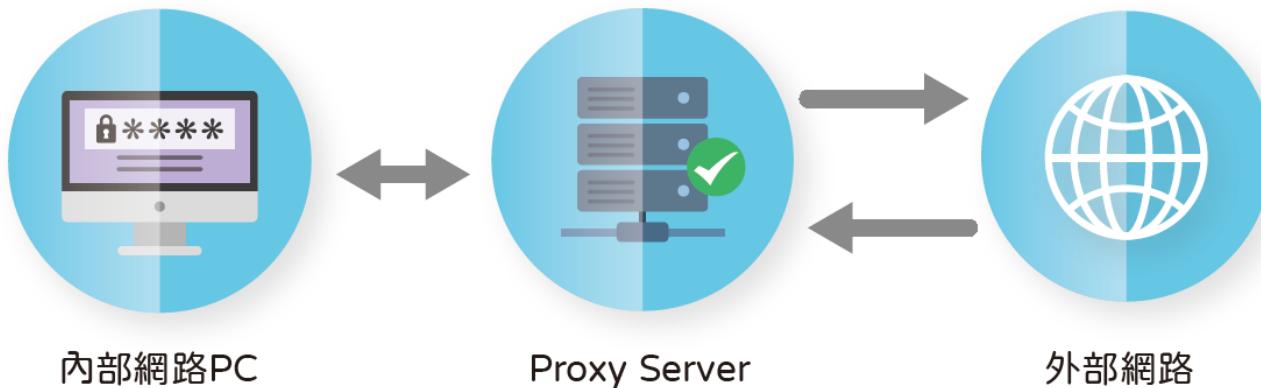
- 是網路安全的防護設備，可能是軟體也可能是硬體，它是內部網路和外部網路之間的橋樑。
- 防火牆可以管制資料封包的流向，並限制外界僅能存取指定的內部網路服務，藉此可以保護主機中的資料。



13-3-3 預防駭客入侵的措施

代理人伺服器

- 位於網際網路和內部網路之間，會統一代替內部網路中的所有個人電腦，向外部網路傳輸資料。
 - 因為連外網路都需通過代理人伺服器，因此它可同時過濾網站內容，能在個人電腦讀取網頁之前，就預先偵測和移除網頁中的惡意程式。



13-3-3 預防駭客入侵的措施

入侵偵測系統(**Intrusion Detection System, IDS**)
入侵防護系統(**Intrusion Prevention System, IPS**)

- 企業用來防禦網路攻擊的安全設備，位於防火牆與內部網路之間，可做為防火牆的第二道防線。
- 入侵偵測系統可對網路或系統的運作狀況進行監視與資料檢測，當發現各種異常情況或攻擊行為時，便會即時向網路安全管理人員或防火牆系統發出警報。

13-3-3 預防駭客入侵的措施

主機型IPS

- 是安裝在使用者電腦上的防護系統，用來阻絕外來網路的攻擊，或中斷系統內容的非法程序存取，以避免主機遭受破壞。

網路型IPS

- 是裝設在網路骨幹上的防護設備，用來監控網路的所有進出流量，阻絕網路中所傳送的異常資料封包。

13-3-3 預防駭客入侵的措施

虛擬私有網路(Virtual Private Network, VPN)

- 企業在組織內傳送電子商務訊息時，為了安全上的考量，可能會建構一個屬於企業私用的私有數據網路，以專線連接各地分公司，來保障資料的傳輸安全。
- 虛擬私有網路是指在開放的網際網路上，使用通道技術、加密、認證等安全技術，以期建立一個與專屬網路具有相同安全性的私人網路。

13-3-3 預防駭客入侵的措施

軟體式VPN

- 是指架設在伺服器或作業系統上的應用程式，提供較具彈性的功能設定，但由於它使用電腦設備原有的CPU進行加解密資料處理，可能會影響到傳輸效能，因此較適合於資料傳輸量小的公司或個人使用。

硬體式VPN

- 具有一個專門處理VPN加解密工作的硬體設備，因此能提供較佳的效能，較適合資料傳輸量大的企業。

13-3-3 預防駭客入侵的措施

- 現今的網路安全設備通常一併結合了防火牆、IPS、VPN等多重防護功能。



13-3-3 預防駭客入侵的措施

帳號與密碼的使用

- 設定密碼時，最好不要使用懶人密碼，定期更換密碼。
- 設定密碼時，可設定不同組合的字母串，最好是12位數以上來加強密碼強度。
- 不使用重複性、連續性或過於簡單的密碼。
- 密碼不要儲存在電腦檔案中或是寫在某個地方。
- 不要透過任何通訊軟體傳送密碼。

13-3-3 預防駭客入侵的措施

行動上網安全守則

- 當使用行動裝置時，若發現電池壽命變短、通話經常不尋常中斷、電信費用異常、自動下載軟體、效能變差等問題時，可能是在提醒你該檢視行動裝置的資安情形了。
- 無線網路設密碼
 - 行動上網工具是靠著無線網路系統與網際網路連線，家中裝有無線網路設備時，請記得為它設定連線密碼，以保障全家人的網路資料安全及網路頻寬品質。

13-3-3 預防駭客入侵的措施

- 公眾無線網路安全性
 - 在公共場合使用免費的Wi-Fi時，盡量不要進入那些需要輸入帳號、密碼、金融卡、信用卡或其他敏感資料的網站，以避免這些資料在傳輸過程中，被不懷好意的人竊取，造成重大損失。當不需要上網時，記得關閉與無線網路的連線。
- 下載App的潛在風險
 - 下載App之前，務必檢查該App要求的權限是否與該App的功能相關。

13-3-3 預防駭客入侵的措施

● LINE安全

- LINE幾乎已成為智慧型手機必備的App，使用者重要的通訊工具，但也成為了詐騙及散播假消息的溫床，非LINE好友傳訊息時，注意是否有不明連結，該訊息上方有「您尚未將本用戶加入好友名單」警告，用此判斷為是否為名單內好友。不要點開訊息中的短網址連結(goo.gl、bit.ly等)或IP連結，建議可先向發送訊息的朋友查證。

13-3-3 預防駭客入侵的措施

- **Facebook安全**
 - Facebook提供雙重驗證功能，讓用戶可透過行動裝置設定安全性金鑰登入Facebook，以防止駭客竊取資訊。雙重驗證是一項確保用戶帳號安全的機制，當用戶從未知的裝置登入Facebook時，必須同時提供密碼與登入碼。
 - 當有心人士試圖從未經認可的瀏覽器或行動裝置登入用戶的Facebook帳號時，用戶即會收到通知，並要求登入者使用金鑰確認為用戶本人。

13-3-4 零信任架構

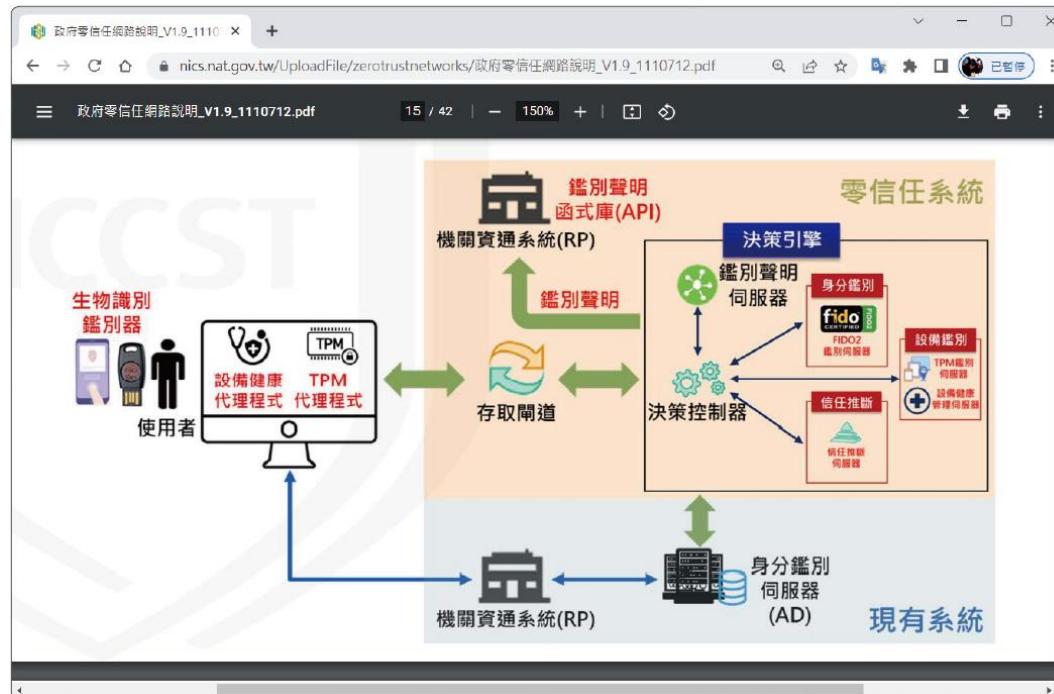
- 零信任架構(Zero Trust architecture, ZTA)是2010年由Forrester Research前副總裁John Kindervag提出的，他認為裝置不再有信賴與不信賴的邊界，以及不再有信賴與不信賴的網路與使用者。
- 零信任架構有別於傳統網路資安防護，任何資料存取依循「永不信任，一律驗證」的原則。

13-3-4 零信任架構

- 傳統的安全性架構是使用者在工作崗位上登入帳號後，便可以存取整個公司的網路，這種架構僅能保護公司的外圍環境，會讓公司暴露在風險之下，因為當有心人士竊取密碼時，對方便能夠存取所有內容；而零信任架構不只會保護公司的外圍環境，還會透過驗證每個身分和裝置，來保護各項檔案、電子郵件和網路。
- 零信任的主要目標在於降低大多數公司在現代環境內遭受網路攻擊的風險，Google等大型企業也都有建構自己的零信任模型，美國眾議院也建議政府機構採用零信任框架來防禦網路攻擊。

13-3-4 零信任架構

- 我國政府也推動零信任網路的計畫，將採門戶部署方式，逐年導入零信任網路的3大核心機制：身分鑑別、設備鑑別以及信任推斷。



13-4 網路交易安全



13-4-1 資料加解密技術

13-4-2 SSL與SET

13-4-3 FXML憑證

13-4-4 零知識證明

INTERNET

13-4-1 資料加解密技術

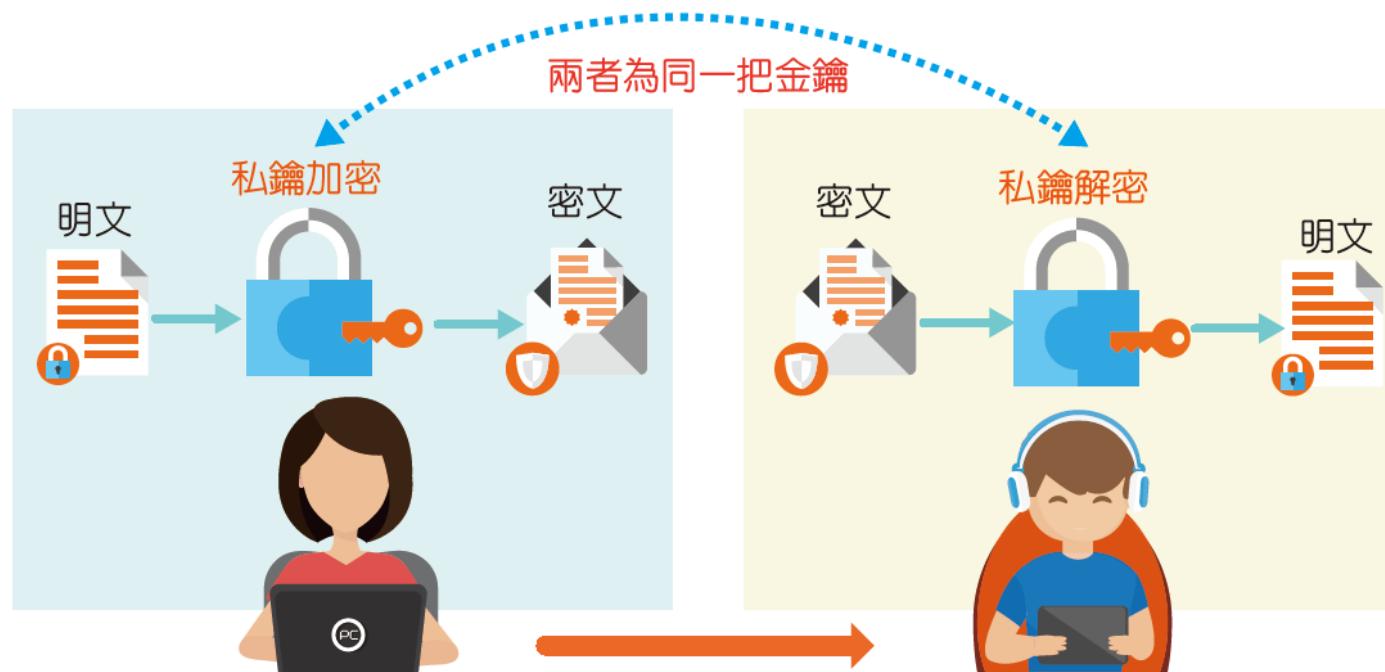
- 資料加密(Data Encryption)是指將原本容易被讀取的原始資料(原文)，透過數學演算法加以編碼，轉換為不可讀取的格式(密文)；而指定的收件者收到密文後，再經由特定的解碼規則，將密文還原為原本正常可讀取的內容，則為資料解密(Data Decryption)。



13-4-1 資料加解密技術

私密金鑰加密法(Secret_key Cryptography)

- 也稱為對稱式加密法，此種技術所使用的加密解密的金鑰是相同的。



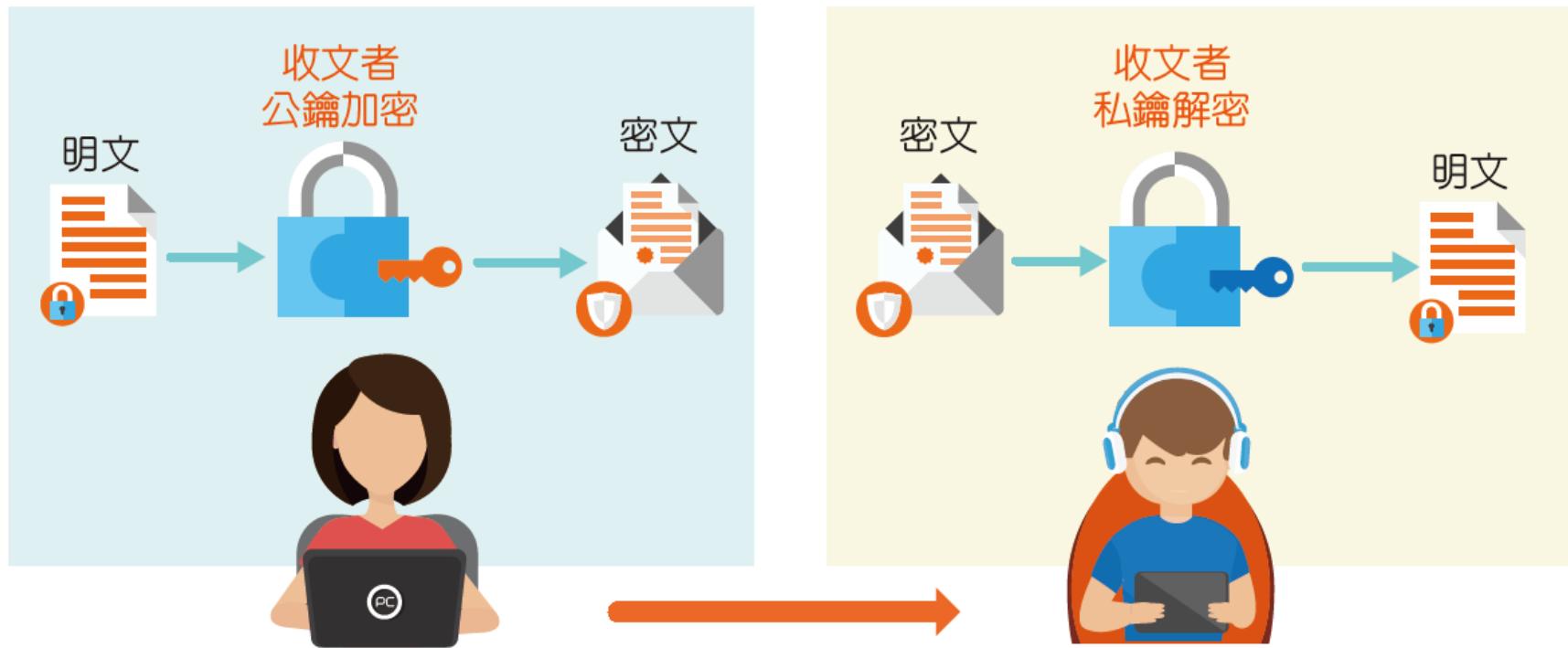
13-4-1 資料加解密技術

公開金鑰加密法(Public_key Cryptography)

- 也稱為非對稱式加密法，此種技術所使用的加密解密的金鑰是不相同的，分別是公開金鑰和私有金鑰。
- 公開金鑰是每個人都可以取得的，而私有金鑰則是由個人所擁有並保存。而以某人的公鑰加密，就必須以同一人的私鑰解密；反之，以其私鑰加密，就必須以其公鑰解密。以這兩種不同的金鑰進行加解密，就可以達到資料的私密性與身分認證的功能。

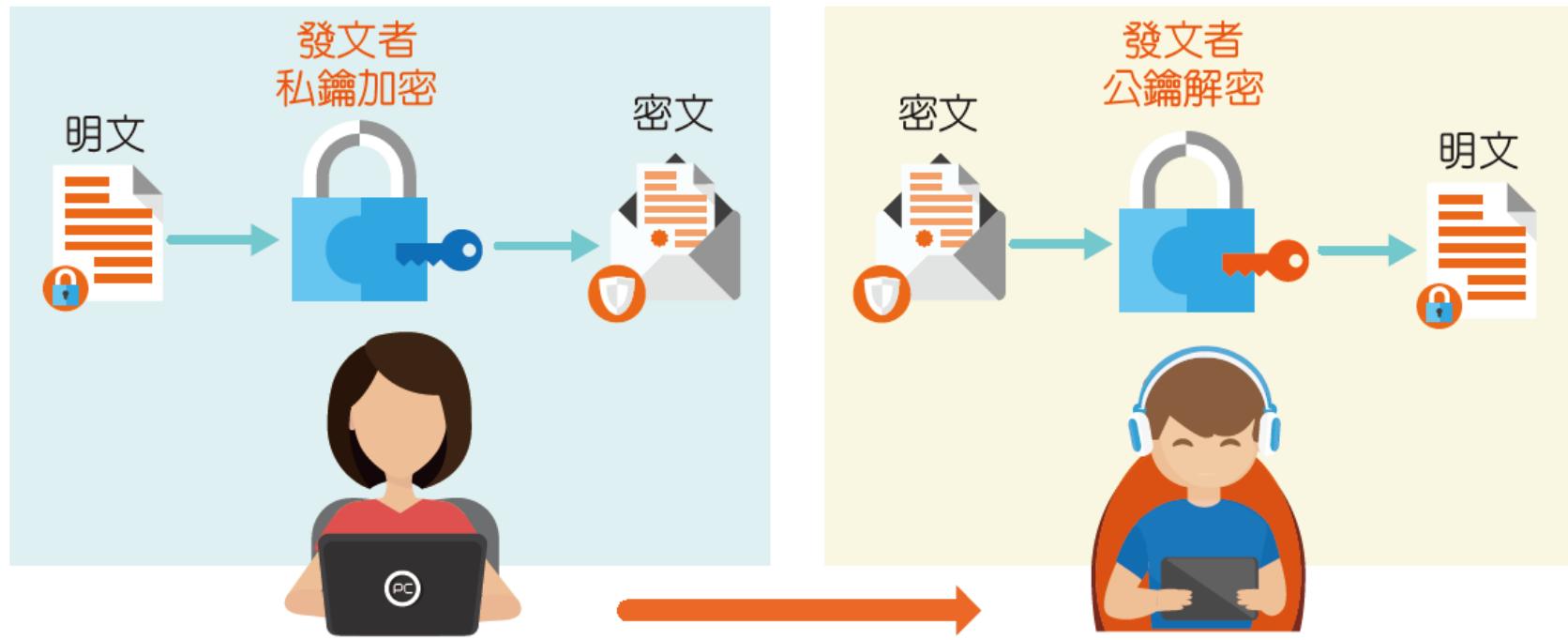
13-4-1 資料加解密技術

- 傳送機密資料給接收者



13-4-1 資料加解密技術

- 接收者可確認發文者身分



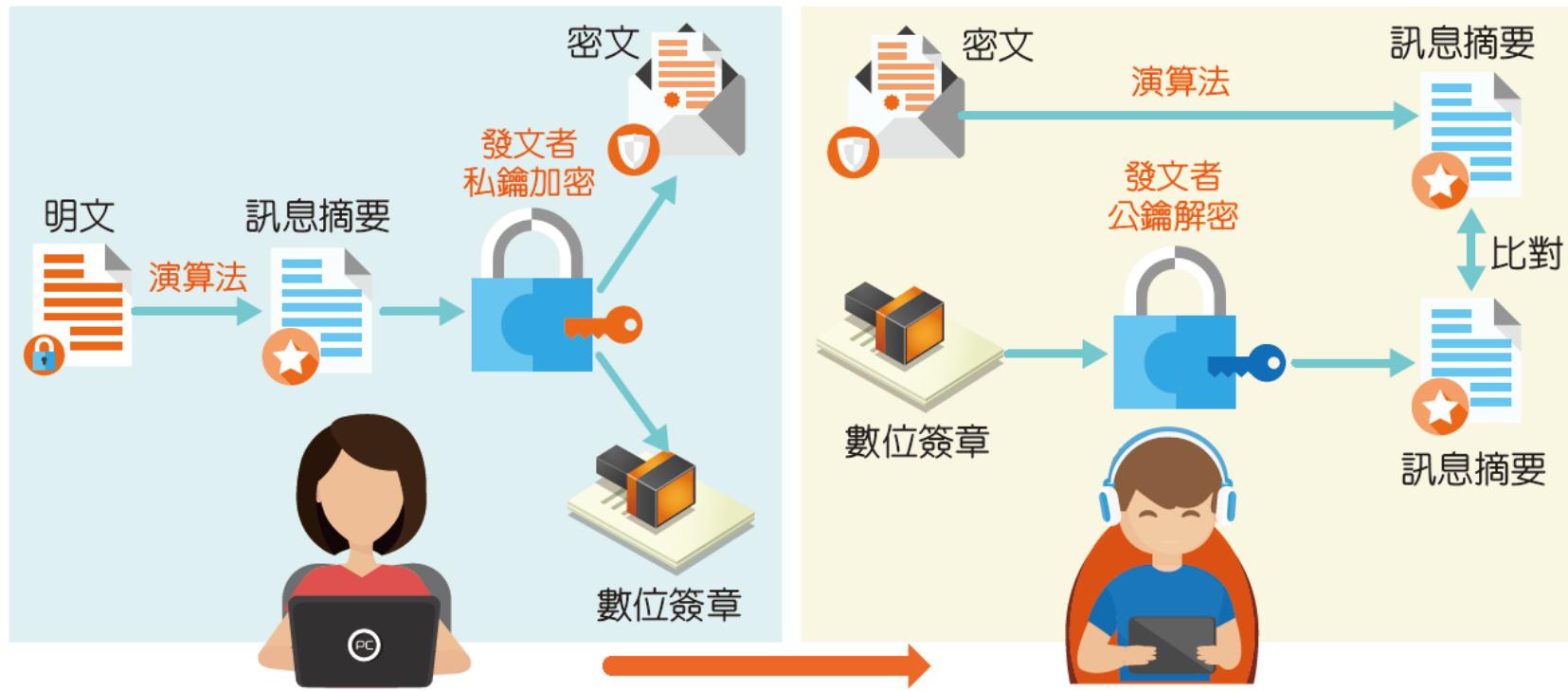
13-4-1 資料加解密技術

數位簽章(Digital Signature)

- 是一種利用公開金鑰加密技術所延伸出的電子安全交易要件，是一項依附於電子文件中，用以辨識及驗證電子文件簽署者的身分與電子文件真偽的資訊。
- 數位簽章就是實際簽章的數位電子表示法，用來防止資料內容在傳輸時被篡改或被冒名傳送假資料。數位簽章與傳送者及傳送內容完全相關，傳送者不可否認，他人也無法偽造，並可由第三者認證。

13-4-1 資料加解密技術

- 按照公開金鑰加密法的原則，數位簽章同樣是以一組公鑰及私鑰來進行簽署者的身分驗證。



13-4-1 資料加解密技術

- 數位簽章必須能提供以下四種資訊安全上的保障：



資料完整性(Integrity)



資料來源辨識(Authentication)



資料隱密性(Confidentiality)



不可否認性(Non-repudiation)

13-4-1 資料加解密技術

數位憑證(Digital Certificate)

- 就如同網路身分證，是由具公信力的憑證管理機構利用公開金鑰密碼技術所核發的一組資料，用以提供網路身分證明的工具，可在網路上代表憑證持有人進行電子交易。
- 其資料內容包含有憑證持有人的身分及公開金鑰、金鑰的有效期限、憑證管理機構及其數位簽章等訊息。

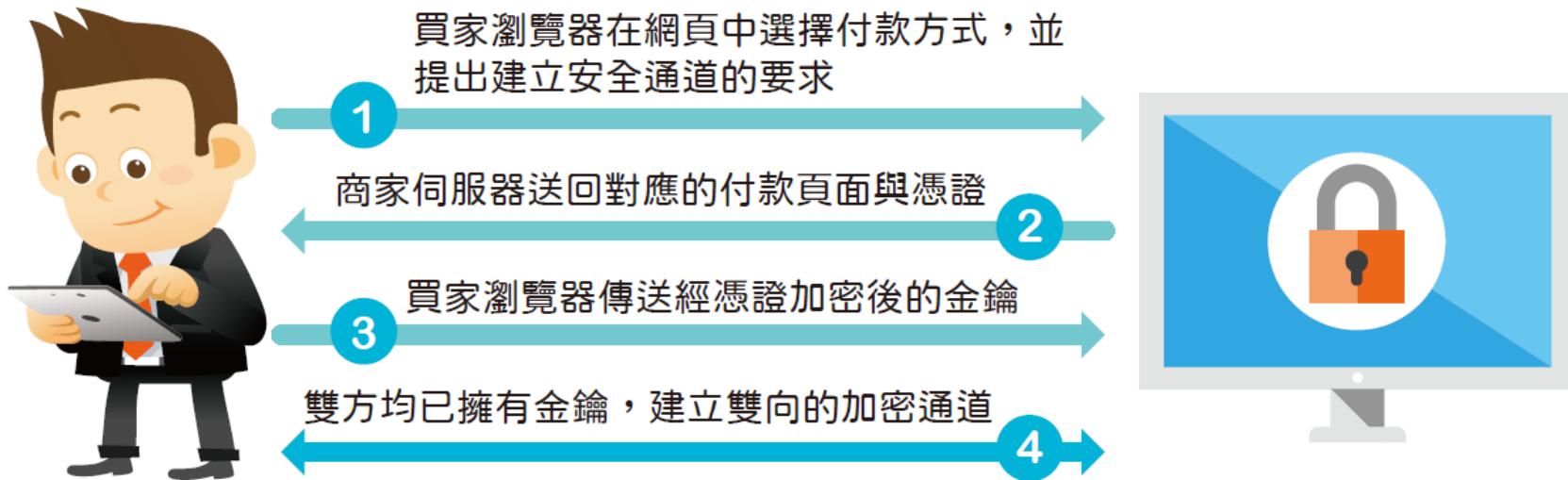
13-4-2 SSL與SET

安全通道層(Secure Sockets Layer, SSL)

- 它介於HTTP和TCP之間，在瀏覽器和伺服器之間建立加密的連接，確保資料能夠安全地傳輸。
- 有採用SSL安全機制的網站，該網站位址都是以「**https**」為開頭。由於SSL是內建於客戶端的瀏覽器上，當客戶端進入有SSL保護的網站中進行查詢或交易時，只要輸入使用者帳號及密碼，不需事先取得認證，就能夠執行相關作業，是目前多數網路交易所使用的線上安全機制。

13-4-2 SSL與SET

- SSL安全協定是在買賣雙方之間建立一個安全通道，來確保線上信用卡資料傳輸安全。



13-4-2 SSL與SET

安全電子交易標準 (Secure Electronic Transaction, SET)

- 是一種應用於網際網路上，以信用卡付款的電子付款系統規範，SET主要是希望能確保網路上信用卡交易的安全性。
- 有了安全電子交易標準，不但在網路上傳遞的資料不易被竊取，也保障了我們交易的安全。
- SET的架構主要是由電子錢包(信用卡)、商店端伺服器(商店)、付款閘道(銀行)和憑證管理機構(政府)等成員共同組合起來的。

13-4-2 SSL與SET

- 就安全層面上的考量，SET機制是比SSL機制略勝一籌。SSL架構下的消費行為，直接由支援SSL的瀏覽器處理，不需另外申請認證；SET機制就必須另外向認證公司取得認證，並且必須配合信用卡業務來進行線上交易。

	SSL	SET
認證機制	只有商店端的伺服器需要認證，客戶端認證則是選擇性的。	所有參與SET交易的成員(持卡人、商家、付款轉接站等)都必須先申請數位憑證來識別身分。
設置成本	較低	較高(客戶端需電子錢包)
安全性	部分(只限客戶端至特約商店，客戶個人資料會在特約商店被解開)。	全部(特約商店無法得知客戶個人資料，銀行無法得知客戶購買內容為何)。
方便性	較高	較低
採用率	較高	較低

13-4-3 FXML憑證

- FXML (金融XML)就是俗稱的「金融憑證」。是應用於金融交易之XML，為國內金融機構間進行網際網路交易所訂定的安全機制。
- 金融憑證中內含網路銀行憑證、證券網路下單憑證、網路保險憑證等三種憑證。
- 使用於銀行、證券、保險等金融領域之電子憑證，除既有之業務範圍外，亦可使用於查詢下載所得資料及進行網路報稅作業。

13-4-4 零知識證明

- 零知識證明(Zero-knowledge proof, ZKP)是一種加密協議，可以在不透露任何資訊的情況下驗證真偽，讓證明者向驗證者確認資料真實性，但卻無需透露任何其他訊息。
- 主要應用在區塊鏈加密貨幣、去中心化金融(DeFi)及Web3中，例如：在加密貨幣的交易中，讓用戶之間可以正常交易、確認錢包內資金安全性，但仍然可以隱藏交易兩方在真實世界中的真實身分。

13-4-4 零知識證明

零知識證明的類型

- **zk-SNARK (簡明非交互零知識證明)**
 - 是一種簡潔的非交互式零知識證明，被廣泛使用於基於區塊鏈的支付系統，它允許在不透露任何資訊的情況下進行驗證。幣安、Zcash與摩根大通等就是使用該驗證方式。
- **zk-STARK (零知識可擴展透明知識論證)**
 - 使用的是公開透明的算法，不需要使用可信任的設置來儲存秘密參數。OKX升級儲備金證明POR系統就是採用該方式。

13-4-4 零知識證明

零知識證明的應用

- 數位身分驗證
 - 零知識證明可以用來驗證使用者的身份，而無須透漏任何敏感個人資料。例如：在數位投票系統中，投票者的身分可以在不透露任何個人資料的前提下被驗證。
- 隱私保護交易
 - 荷蘭國際銀行(ING Bank)將零知識證明改編成一種在銀行使用的零知識範圍證明(Zero-Knowledge Range Proofs)，可以證明數字是在某一特定範圍內的，例如：貸款申請人可以證明他們的薪資在一定範圍內，而不用洩露確切的金額。因此，範圍證明在計算上比零知識證明更簡便，在區塊鏈上運行速度也更快。

13-5 網路帶來的影響與衝擊



13-5-1 資訊超載與資訊焦慮

13-5-2 網路謠言及假訊息

13-5-3 網路犯罪

13-5-4 區塊鏈的隱憂

13-5-5 暗網

INTERNET

13-5-1 資訊超載與資訊焦慮

資訊超載(Information Overload)

- 因為人類從環境接受輸入的容量是有限的，當人類所具有的內在過濾或選擇程序無法處理增加的資訊時，就會發生資訊超載。
- 資訊超載會帶來各種負面影響，如錯失恐懼症、壓力過大等，而導致拖延，以及對工作與生活無感等。

13-5-1 資訊超載與資訊焦慮

- 如何有效的管理資訊，是許多人共同面臨的難題，為避免資訊超載，可以試試以下的方法：
 - 允許自己忽略某些訊息，善用資訊管理工具過濾資訊。
 - 視需求快速瀏覽摘要與評論，抓住重點，將能有效篩選出需要精讀的內容，節省時間與精力。
 - 減少社交互動、資訊豐富的社群網站及軟體的使用。
 - 與團隊成員分工合作，決定好各自應掌握的訊息範疇，然後彼此分享。

13-5-1 資訊超載與資訊焦慮

資訊焦慮(Information Anxiety)

- 藍斯·蕭(Lance Shaw)表示：「在我們這個對資訊狂熱，而且充分飽和的社會，已經開始出現一種病症，症狀是：一種偏執的迫使自己遍讀一切可讀之物，當吸收的閱讀量超過消化所需的能量時，超出的部分日積月累，最後因壓力與過度刺激轉化為所謂的資訊焦慮症。」

13-5-1 資訊超載與資訊焦慮

- 限制新聞數量，留意閱讀內容，試著在特定時間查看新聞。
- 中斷社交媒體或關閉訊息提醒，如果你對社群媒體上的訊息不堪負重，請將其靜音，或者隱藏相關貼文。
- 安排例行活動並與周圍的人保持聯繫。
- 不要轉傳或散布恐慌性的資訊與照片。
- 以閱讀書籍、手寫創作取代使用各類的電子產品。

13-5-2 網路謠言及假訊息

- 趨勢科技指出，因COVID-19帶起的詐騙、假訊息及謠言層出不窮，光是在疫情傳播最高峰，所偵測到的數量即高達20萬則，暴增了203%。
- 網路謠言與假訊息都是一種未經證實的訊息，它可能引起相當可怕的效應。
- 一般民眾在收到訊息時，可能沒有深入追查其來源與真實性，而又流傳給更多人知道，無心成為散布謠言的幫凶。若是錯誤的訊息透過口耳相傳一再散播，就可能造成他人權益的損害，甚至影響社會秩序。

13-5-2 網路謠言及假訊息

假訊息的手法

諷刺揶揄與惡搞迷因

圖文不符與錯誤敘事

標題殺人與流量霸權

機器帳號與大量訊息

AI生成

13-5-2 網路謠言及假訊息

網軍

- 網軍是泛指在各大社群散播訊息的人，通常是受雇於特定政治背景的個人或組織，並為其刺探網路情報、輿論顛覆、帶動輿論風向者；另一種則是受雇於特定的民間企業，透過各種方式行銷、推廣特定人、事、物者。
- 網軍透過Facebook、LINE、Dcard、PTT等各大社群媒體及論壇進行發文宣傳。

13-5-2 網路謠言及假訊息

- 若網軍不能受控於一定的法律、職業道德規範下，那麼這種操控社群、操控人心的行為，很容易讓社會資源浪費，且導致憾事發生。
- 例如有網友在PTT中散播臺灣旅客靠中國駐日使館脫困的假消息，並指責我國駐外人員態度差，間接造成駐外人員不堪輿論壓力選擇輕生以死明志。

13-5-2 網路謠言及假訊息

查證網路謠言

- 要有正確的認知，遠離虛假、垃圾訊息，並且看清楚真相。

1

誇張聳動、讓人忍不住想點閱的標題，可能為惡意「點擊誘餌」

3

內容出現拼字錯誤或網站版面不正常

5

沒有附註發布日期

2

可疑的網站地址，可能冒充真實的新聞網站

4

明顯經過刻意修圖的照片或圖片

6

未註明作者、消息來源或相關資料

13-5-2 網路謠言及假訊息

網站名稱	網址
MyGoPen 這是假消息	https://www.myopen.com
衛生福利部食品藥物管理署 - 食藥闢謠專區	https://www.fda.gov.tw
台灣事實查核中心	https://tfc-taiwan.org.tw
食力 foodNEXT	https://www.foodnext.net
Cofacts 真的假的	https://cofacts.g0v.tw
LINE 訊息查證	https://fact-checker.line.me
蘭姆酒吐司	https://rumtoast.com

13-5-3 網路犯罪

網路詐欺

- 網路詐欺是網路上最常見的犯罪行為，例如有些人會在網路上拍賣一些低價的物品，吸引消費者購買，而當消費者依指示將錢匯入對方帳戶後，卻沒有收到購買的商品，此行為可能涉及刑法第339條的詐欺罪。

13-5-3 網路犯罪

網路援交

- 網路援交是指透過網路散播訊息，以尋求提供性服務來換取金錢的援助交際行為，透過網路這個溝通媒介，讓有意援交的兩方人馬可以約見時間與地點以進行交易，而這樣的行為其實已經觸犯兒童及少年性交易防制法。
- 按照該條文之規定，只要有散布、播送或刊登足以引誘、媒介、暗示或其他促使人為性交易之訊息，無須以「實際發生性交易」為必要，仍然構成犯罪，且交易雙方均依該條例處罰。

13-5-3 網路犯罪

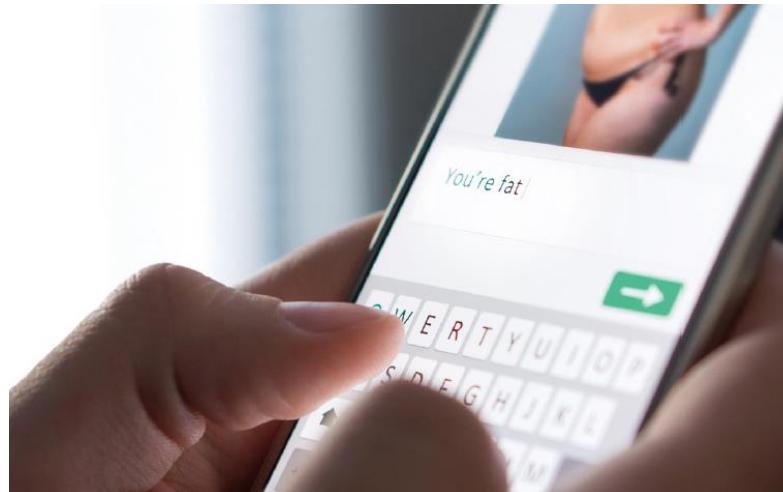
網路色情

- 常見的網路色情犯罪事件，是利用網路散播色情圖片，例如架設色情網站，並提供各種色情圖片、影片、利用電子郵件夾帶色情圖檔、利用網路相簿存放色情圖片等。
- 這些行為可能已觸犯刑法第234條的公然猥褻罪，以及刑法第235條之散布、販賣猥褻物品及製造持有罪等。

13-5-3 網路犯罪

網路不當言論

- 在網路上以公開或匿名方式發表不實報導、網路恐嚇、公然毀謗或辱罵他人、侵犯他人權益、妨害他人名譽或留言霸凌他人等，都可能觸犯刑法的公然侮辱罪、誹謗罪，或是恐嚇罪等。



13-5-3 網路犯罪

網路賭博

- 在網路上架設網頁，並提供賭博網站之功能，供群眾上網賭博財物者，就會觸犯刑法第268條的賭博罪。

入侵他人網站

- 未經過他人同意，非法入侵他人電腦系統，以竊取電腦內部重要或機密資料、偷取電玩虛擬寶物，或破壞或擅改電腦系統等，可能觸犯刑法第358條之入侵電腦或其相關設備罪，及第359條的破壞電磁紀錄罪。

13-5-3 網路犯罪

散布電腦病毒

- 在網路上散播電腦病毒，致使他人的電腦當機、檔案毀損或硬碟格式化等情形，可能觸犯刑法第360條之干擾電腦或其相關設備罪及第362條的製作犯罪電腦程式罪。

侵害他人智慧財產權

- 網路上有許多豐富的資源，包括文字、圖片、影音檔案等，這些資源雖然垂手可得，但它們仍然具有著作權，若是未經所有權人同意，是不能任意引用或改製的，以免不小心觸法。

13-5-3 網路犯罪

散布假消息

- 因行動裝置的普及，不實謠言及假消息的散布越來越迅速，已嚴重影響國人社交生活及社會安寧，而行政院為了「防堵假新聞」修法，納入禁止散播假新聞的規範和罰則，最嚴重的狀況下，可能被罰100萬罰金或無期徒刑。

13-5-4 區塊鏈的隱憂

- 區塊鏈分析公司Chainalysis在報告中指出，2022年非法加密貨幣活動總額超過6,000億元。Chainalysis發現不少DeFi的智慧合約與程式碼存在漏洞，只要有利可圖，駭客就會拼命鑽這些漏洞詐取虛擬貨幣。
- 在140億美元的犯罪活動裡有32億美元屬於被盜案件，而在這32億美元中又有72%的被盜資金來自DeFi相關事件。

13-5-4 區塊鏈的隱憂

- 因為區塊鏈特性，有不少犯罪集團採用虛擬貨幣作為主要的贖金，例如鴻海遭勒索攻擊，駭客威脅交付1,804枚比特幣贖金。
- 為避免虛擬貨幣淪為犯罪集團洗錢犯罪的工具，金管會正式實施「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」，規範虛擬貨幣業者需遵循嚴格的認證與反洗錢程序。

13-5-5 暗網

- 網路世界可以分為明網及深網兩大部分，可以被搜尋引擎找到的網站，就是屬於明網的一種，而無法被搜尋引擎找到的就都是深網的一部分。
- 暗網(Dark Web)是深網的一部分，在深網的最底層，需要特殊的權限、特殊的瀏覽器、甚至特殊的裝置才能進入。
- 要上暗網，必須要透過專屬的瀏覽器，如「洋蔥路由器(Tor)」，暗網的網址是以.onion結尾，用一般的瀏覽器是無法連上的。

13-5-5 暗網

- 暗網有不易被追蹤的特性，因此有許多不肖人士利用暗網的隱匿性，在暗網上從事非法活動，例如毒品、軍火、護照資訊買賣、發布非法色情內容等黑市交易。
- 暗網是否如傳說中的邪惡，完全取決於使用者的使用方式，而許多網路公司，如Facebook也開發出了暗網版本，讓注重隱私的用戶也能安心使用。在暗網的販售網站，幾乎都是釣魚網站或詐騙網站，許多內容也暗藏惡意軟體或病毒連結，建議不要造訪違法、不安全的暗網網站。