議題三

第一單元
資訊安全與可能危害

UNIT3

01

0101101001010110100110
0010110100101011010010
0010110100110110100 1

「一」葉知秋 – 學思並進

學習目標

核心素養

科 S-U-B2(普通高中)、科 V-U-B2(技術高中)、科 C-U-B2(綜合高中)

理解科技與資訊的原理及發展趨勢，整合運用科技、資訊及媒體，並能分析思辨人與科技、社會、環境的關係。

學習表現

設 k-V-3(普通高中、技術高中、綜合高中) 能分析、思辨與批判人與科技、社會、環境之間的關係。

運 a-V-1(普通高中、技術高中、綜合高中) 能實踐健康的數位公民生活。

學習內容

資 H-V-1(普通高中、技術高中、綜合高中) 資訊科技的合理使用原則。

資 H-V-2(普通高中、技術高中、綜合高中) 個人資料的保護。

資 H-V-3(普通高中、技術高中、綜合高中) 資訊科技對人與社會的影響與衝擊。

學習重點

1. 學生在學習完本章後，能夠理解數位資料的定義並懂得如何保護自己的重要數位資料。
2. 學生在學習完本章後，能夠因為理解資訊領域常見的攻擊手段而避免自身受險。
3. 學生在學習完本章後，能夠在不幸遭受資安危害後使用正確的方式降低自己的受害狀況。

引起動機

近年來因為勒索病毒流行，電腦中重要資料被加密後救不回來的消息時有所聞，這些病毒究竟是透過什麼樣的方式進入電腦大肆破壞，又有什麼樣的方法可以避免自己成為受害者之一呢？本章將從資料的重要性談起，然後說明可能對資訊安全造成危害的攻擊手法和避免方式。

「兩」全其美 – 觸類旁通

數位資產與資訊安全

隨著科技的進步、資訊產品和網路服務的普及，人們不僅大量地使用電腦、手機等資訊設備來協助處理工作和進行創作，也把許多生活中的點滴，透過各種數位記錄方式儲存在不同裝置或分享於社群網站上。

這些數位型態所記錄的資料和資訊，雖沒有可觸碰的實體，但對當事人來說具有獨特的意義和價值，甚至具有轉化為實體金錢收益的可能性，所以我們仍然將其視為資產的一種，也就是所謂的數位資產（Digital Property）。

美國學者 Samantha D. Haworth (2014) 以「資產形式的儲存模式」為標準，將數位資產的內容區分為：

1. 帳號資訊（Access Information）

指使用者所擁有用來登入各式系統的帳號、密碼資訊及帳號運作權限。雖然根據帳號申請的需求程度不同，帳號本身可能不具有資訊價值，但是它卻是獲取或管理、支配數位資產的管道或連結。

2. 有形數位資產（Tangible Digital Assets）

可轉化為有形物品之數位內容，例如 PDF 文件檔、影像圖檔、臉書或部落格上的文章…。這類內容大多可用非數位之方式呈現，或可轉為其他有體物之形式呈現，也是一般使用者最容易意識到的數位資產。

3. 無形數位資產（Intangible Digital Assets）

按讚紀錄、貼文回覆及問卷調查等個人在網路上的活動紀錄，一般又稱為「數位足跡（digital footprint）」。雖然看起來無法直接轉化為實體金錢，但隨著網路和生活的緊密結合，它隱含的經濟利益正在不斷增加，例如，粉絲團按讚、頻道追蹤的人數，越來越被視為影響力的一種，甚至可能可以轉為代言、業配資格等現實中的酬庸關係。

4. 後設資料（Metadata）

描述資料的資料，也有人翻譯成元數據、元資料、詮釋資料、中介資料、中繼資料。例如，cookie 紀錄、瀏覽歷史紀錄、暫存檔案…。隨著大數據技術的發展，這類數位資產的價值正在逐步提升。

除了明確可見的重要資料以外，隱藏在其中的個人資料，也往往是有心人士覬覦的目標。根據「個人資料保護法」，個人資料是指能夠直接或間接識別該個人之資料，例如自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、聯絡方式、財務情況等等。這些資料因為與個人息息相關，所以可能會被販售、或用於非法行為以獲取財富。

既然在生活中所創造的數位資訊是具有價值的資產，就有被竊取的風險和保護的必要性，那我們應該如何著手保護自己的資料呢？

數位的資料因為是由數字所構成，所以具有和實體物品完全不同的特性，我們可以從資訊安全的三個原則來檢視資料是否安全：

1. 機密性（Confidentiality）

採取適當的安全機制來保護資料及資源，避免無權限的人員或程式任意取用。

例如：將雲端分享的檔案加上存取權限，使用者必須登入具權限的帳號才能存取該檔案。

2. 完整性（Integrity）

在傳輸、儲存資訊或資料的過程中，確保資訊或資料不被未經授權的篡改或在篡改後能夠迅速被發現。

例如：在網路購物時，購物內容的品項、數量、買賣方資料等購物資訊，必須要維持正確一致，才能確保買賣雙方權益。

3. 可用性（Availability）

確保資訊與系統的正常運作，讓使用者能夠正常的使用。

例如：訂票網站中的網站資料庫、網站伺服器與訂票系統必須要正常運作才能提供服務；相反的，若是個人的檔案因為磁碟損壞等問題造成無法正常讀取，就是缺乏可用性。

簡單來說，資訊安全意為保護資訊及資訊系統不受未經授權的進入、使用、檢視、修改、洩漏、記錄、破壞及銷毀（維基百科）。

常見攻擊類別

所謂「知己知彼，百戰百勝」，在開始建立好防線保護自己的資料和資訊之前，先來看看目前常見的攻擊方式，用以協助我們針對可能的弱點進行補強。

圖 3-1　勒索病毒 Wana Decrypt0r 的中毒時顯示的勒索訊息

一、惡意程式（Malicious code）

任何蓄意對個人電腦、伺服器、智慧型裝置、電腦網路等設備或服務造成資訊安全上損害的軟體都可以被稱為惡意軟體（Malware, malicious software），包括電腦病毒、木馬程式、電腦蠕蟲、間諜軟體、廣告軟體或其混合型。以下分別加以介紹：

1. 電腦病毒（Virus）

就像現實中的病毒一樣，「電腦病毒」是指會將本身程式碼複製（感染）到其他檔案或開機區的程式。電腦病毒根據製作者的意圖不同，會對感染者的系統造成程度不一的損害，輕者可能僅顯示無法關閉的圖片或隱藏檔案，重者則有機會破壞電腦裡的資料，甚至整個系統。近年來流行的勒索病毒則是透過將電腦中的資料進行加密（如圖 3-1 中），並以此向受害者勒索贖金因而得名。

電腦病毒的作者為了讓自己的程式碼更難被破解及偵測，「變體引擎」（polymorphism）、「壓縮」（compression）、「加密」（encryption）

等各項技術都被大量運用在各種類型的病毒上。

2. 特洛伊木馬程式（Trojan horses）

特洛伊木馬程式（本文簡稱木馬程式）和神話中的特洛伊木馬一樣，會將自己包裝成一些無害的軟體來吸引使用者下載並執行，再啟動內藏的「士兵」來破壞或竊取重要資料（如：格式化磁碟、刪除檔案、竊取密碼等）或是進行大規模的「阻斷服務」（DoS , Denial of Service）攻擊行動。Keylogger 木馬程式便是一例，被植入 Keylogger 的電腦，會記錄使用者按了哪些鍵，駭客便有機會竊取機密資料。

和電腦病毒的主動傳染不同，木馬程式大多是透過垃圾郵件、惡意連結或駭客入侵的方式散佈，並且大多不會感染系統中其他檔案。

3. 電腦蠕蟲（Worm）

和電腦病毒相比，電腦蠕蟲不會感染其他檔案，但是會複製出很多「分身」，透過巨量的數據資料占用資源來使得系統或網路無法正常提供服務。

常用的方法是透過區域網路（Local Area Network , LAN）資料夾分享或是網際網路（Internet）E -Mail 來散布自己。歷史上曾有許多蠕蟲軟體對全球的電腦和網路造成的重大的癱瘓，如 2003 年的衝擊波（Blaster）和 2004 年的震盪波（Sassar）蠕蟲，甚至近年來有名的勒索病毒 WannaCry 也是蠕蟲的一種。

電腦病毒、木馬程式、電腦蠕蟲原都是各自獨立的程式，近年來單一型態的惡意程式愈來愈少了，大部份都以「電腦病毒」加「電腦蠕蟲」或「木馬程式」加「電腦蠕蟲」的型態存在以造成更大的影響，比率以前者居多。例如 2006 年至 2007 左右曾經在台灣肆虐的熊貓燒香病毒就是一種蠕蟲病毒，它會偽裝成遊戲吸引人下載安裝，當中毒後會感染電腦中副檔名為 exe 的執行檔們使其無法執行，並把被感染檔案的圖示改成熊貓舉著三根燒著的香的圖案。

其他常見的惡意軟體還有在使用者不知情的情況下收集使用者資訊的間諜軟體（Spyware）；在電腦上自動播放、顯示或下載廣告的廣告軟體（Adware）等等。

二、垃圾郵件（Spam mail）

根據世界知名的網路及軟體安全業者賽門鐵克公司 2009 年 2 月公布的報告，臺灣被列為全球第 9 大發出垃圾郵件的國家；根據統計，臺灣一年有 1053 億封垃圾郵件在網路流竄，平均每人每天收到 29 封，光是刪除垃圾信件這個動作，一年下來會讓民眾浪費 30 個小時，可見目前對於網路使用者而言，垃圾郵件相當的泛濫。

一般所稱的垃圾郵件是將一份內容相同的電子郵件，未經收信人許可就大量寄給不同的人，郵件內容多數是與收信人不相干的商業廣告。另一種垃圾郵件為大量轉寄未經篩選或處理的信件給通訊錄中的郵件群組，通常是你的親朋好友。垃圾郵件並不侷限於一般網際網路上的郵件，已擴及無線通訊中的短訊或簡訊。由於同時寄發大量郵件，常造成網路壅塞、郵件伺服主機負擔過重，收信人需花費金錢、時間去收這些垃圾郵件。

現在有許多的垃圾郵件是由詐騙或駭客集團所寄出，他們往往會透過聳動的標題或是偽裝寄件者來讓你相信你中了獎、或是交易失敗需要你輸入相關資料將你引導到釣魚網站或下載帶有病毒的軟體。

雖然目前大多數的電子信箱服務都有篩選垃圾信件的功能，但是還是有許多信被誤判，讓使用者有機會受到其中的騷擾或落入駭客的陷阱之中。

三、社交工程（Social engineering）

指利用人性弱點，使用溝通和欺騙的伎倆，以獲取帳號、密碼、信用卡密碼、身分證統一編號、姓名、地址、其他可確認身分或機密資料的方法，進而突破資訊安全防護，進行非法的存取及破壞行為。社交工程一般不使用高深的駭客技術（如植入後門、使用系統漏洞入侵），而是利用人性的弱點或與人互動的技巧來達到目的的方法。

常見的社交工程的攻擊方式如下：

1. 線上聊天 / 電話釣魚

利用電話或即時通訊軟體和被害者建立友好關係後，再乘機騙取帳號及密碼。

2. 等價交換（Quid pro quo）

攻擊者可能偽裝成技術支援人員，在「幫助」有困難的人解決技術問題的同時

圖 3-2　垃圾郵件大多為廣告或是隱含資安疑慮的詐騙信件

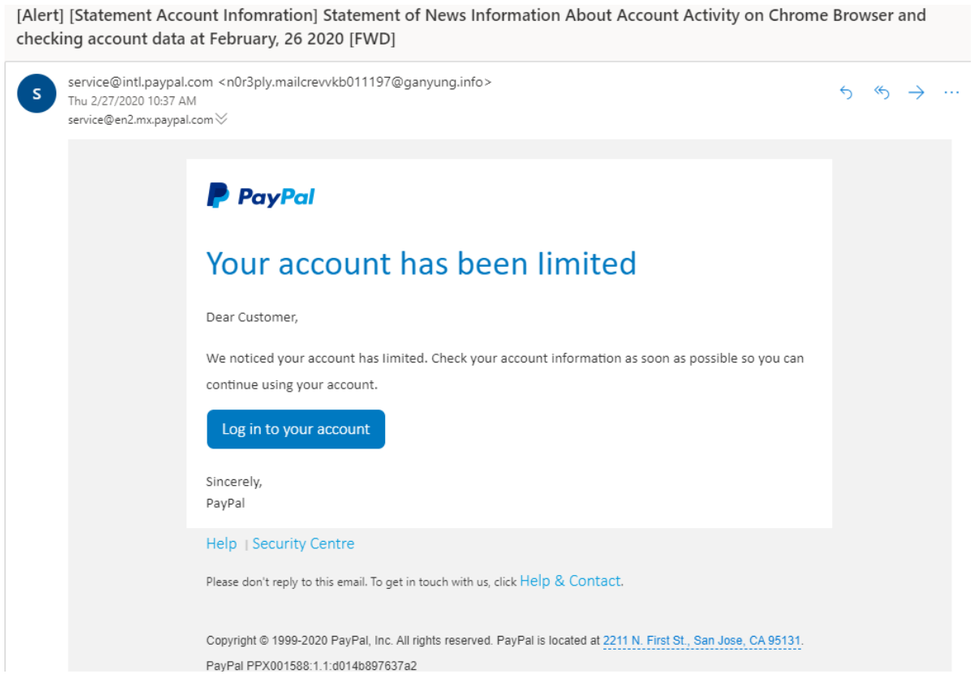


圖 3-3　偽裝成帳號警示等重要訊息的垃圾郵件是常見的社交攻擊手法

悄悄植入惡意程式或盜取資訊。或是偽裝成問券調查人員，藉由提供完成問卷的獎勵來誘使受試者完成填寫機密資料的問卷。

3.　網路釣魚（Phishing）

企圖利用電子通訊方式，透過偽裝成具公信力的組織，用以竊取如使用者用戶名稱、密碼、信用卡明細等個人敏感資訊的犯罪詐騙過程。通常是透過電子郵件或即時通訊的方式，引導被害者前往偽造成和本尊高度相似的網站進行登入或交易行為，在他們輸入帳號密碼或信用卡資訊時將其側錄，盜用這些資料。例如圖 3-3 中通知網站帳號遭到限制權限的電子郵件，若是仔細觀察可以發現寄件者所使用的電子信箱並非來自官方，從此可以判斷它應該是用於詐騙不知情受害者的垃圾郵件。

4.　利用人性慾望

透過中獎、色情彈出廣告或電子郵件的方式，引誘使用者點下有害的網站連結。亦有透過偽裝成線上掃毒宣稱發現電腦中毒，要求使用者下載假冒的防毒軟體。

5.　錯置或混淆連結

近年來因為二維條碼（QR-code）的普及和短網址服務的提供，越來越多的連結可以透過這類方式隱藏自己的網址（URL）藉此讓使用者無法在第一時間察覺所連向的目標。例如現在就常常有釣魚網站或病毒載點藉由短網址的功能隱藏自己真實的網址後，再假借免費貼圖載點的名義散播出去，誘騙收到訊息的人點下連結進而受害。

四、字典攻擊（Dictionary attack）

字典攻擊的方式主要是用在猜測帳號密碼上，駭客會藉由猜測常見或預設的帳號密碼組合來試圖登入目標服務。根據密碼安全公司 SplashData 的統計，2019 年最多人仍在使用的密碼前五名分別為「123456」、「123456789」、「qwerty」、「password」和「1234567」，這些密碼都很可能是駭客在嘗試登入目標帳號時優先嘗試的密碼之一。

類似但更進階一點的手法是透過將從不同來源取得的個人資料片段進行比對後，拼湊出完整的資料，再利用一般民眾喜歡用生日、電話號碼等特殊數字作為密碼的習慣，直接上網「測試」各種可能的帳號密碼組合，一般將這種方法稱為「資料拼圖」。一旦成功，即可以合法的身分登入使用者帳號，直接觀看使用者的個人資料與各種紀錄。

五、進階持續性滲透威脅（Advanced Persistent Threat, APT）

這種攻擊模式如同字面所述包含三個要素：進階、持續性、威脅。進階強調的是使用複雜精密的惡意軟體及技術以利用系統中的漏洞等進階攻擊手法；持續性則是指長期、持續性的潛伏、監控特定目標，並從其獲取數據。威脅則指較為高度的針對性。

APT 攻擊主要重點在於低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料；所以能發動這種 APT 攻擊手法的駭客，都是以長期滲透特定商業組織或政府機構為目標，擁有高超複雜的入侵技巧，並且有足夠資金，才能支持這樣的滲透及攻擊活動。

APT 具備下列五種的特色：

1. 高度針對性。
2. 具有潛伏並保持低調的技術能力。
3. 擁有資料情報分析之能力。
4. 擁有多樣工具的多重面向攻擊方式。
5. 資金充裕。

APT 和一般駭客攻擊的差異如下 ：

	APT	一般駭客攻擊
時間	較長的時間攻擊。	攻擊時間長短不一定。
動機	竊取所需要的特定機密，包括國家安全、商業機密等。	動機不同，從彰顯自己能力和炫耀自己到竊取個人資料換取實質利益都有。
攻擊者	有組織、有計畫的團體。	一般個人或駭客結盟。
攻擊對象	針對性、小範圍，如政府、公司行號、金融業等。	無針對性、大範圍，近年以具有大量個人資料的企業為主。
攻擊手法	長期、持續性、多樣性，經常是利用零時差系統漏洞的攻擊，確保達成攻擊目的。	多數為速戰速決，複合多種常見系統漏洞，以大量、快速、有效的單一手法入侵。

常見攻擊途徑

首先要建立起一個基本概念，那就是「絕大多數攻擊是不分目標的」，在網路傳輸和運算速度十分快速的現在，攻擊者們已經沒有必要為了節省資源來縮限自己的攻擊範圍，減少可能的受害者人數。也就是說，每個人都應該要時時警惕，不要認為自己是個不重要的人士所以不會遭受攻擊。

一、從中毒的設備感染

病毒透過 USB 隨身碟、光碟等攜帶型儲存設備從中毒的電腦將自身散佈至未中毒的裝置中並將其感染。例如會隱藏檔案並創造同名捷徑的隨身碟病毒 movemenoreg.vbs 就是許多學校公用電腦中常見的病毒之一。

網路也是許多病毒散播自己的管道，他們可能會透過嘗試存取區域網路的共用資料夾，或是以電子郵件的形式進行散播，並透過信件內容來誘騙使用者開啟附件（Attachment）檔案來增加感染的機會。

二、系統漏洞

不管是系統程式還是應用軟體都是由人類所撰寫，既然如此，就不可避免的會出現系統設計上的瑕疵或缺漏，讓有心人士們有機會透過這些漏洞入侵，發動攻擊。如 2019 年盛行的勒索蠕蟲病毒 WannaCry，就是駭客們利用美國國家安全局（NSA）的「永恆之藍（EternalBlue）」漏洞利用程式來進行攻擊，造成大量的資料被加密。

三、瀏覽網頁

除了之前提到的攻擊手法中，透過仿真的釣魚網頁來騙取使用者的帳號密碼等重要個人資料以外，一般人在上網的時候還可能會遭受到其他的攻擊手法。

目前許多網站會在使用者觀看文章或影片前彈出廣告以增加收益，這些廣告並非全都是合法安全的，如果它會將惡意程式一起載入或是將使用者引導至有問題的網站，我們就稱之為「惡意廣告」。在過去十年間，許多高知名度的網站如紐約時報、Google 都曾因為他們的廣告通路而在不知情下成為網路犯罪市場的幫兇。

另外一種在瀏覽網頁時會遭受到的攻擊方式是「路過式下載（Drive-by Downloads）」，或稱為「網頁掛馬」：駭客透過在目標網站中加入部分程式碼，讓使用者在瀏覽網頁時暗地裡下載或執行惡意程式。

最後則是將惡性程式偽裝成重要通知或有趣遊戲、美麗圖片等吸引使用者直接下載或執行，例如：

1. 當你要下載某些軟體或影片時，要你先下載執行「下載用的程式」。
2. 偽裝成防毒公司寄發「解毒程式」。
3. 偽裝成輔助遊戲進行的「外掛軟體」。

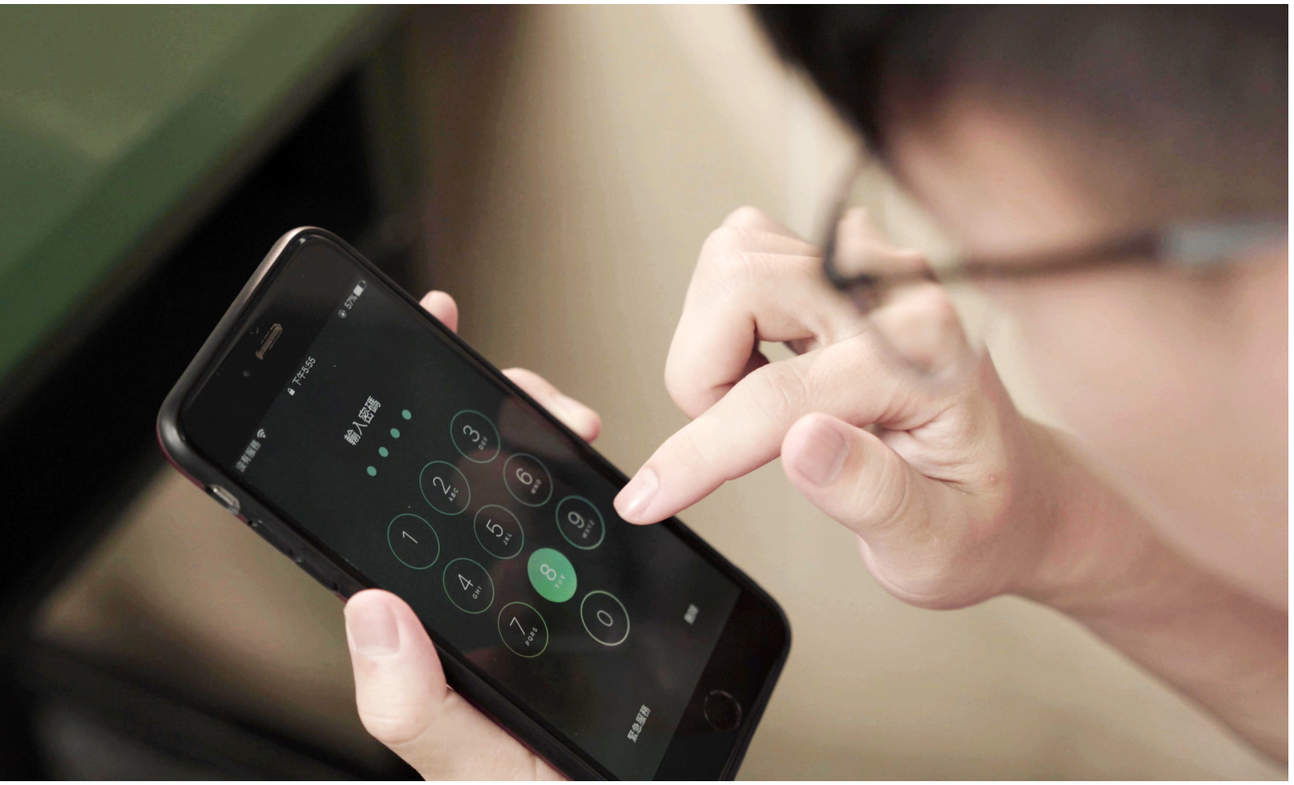
防護方法

在認識常見的攻擊類別和散佈途徑之後，就更能夠「對症下藥」針對弱點進行補強。以下我們將介紹一些資訊安全領域裡常見的防護方法。

一、定期更新

市面上絕大多數的軟體都會持續改版來修補漏洞或錯誤，以確保自身的商品維持一定程度的安全，進而維護自己的商譽，使用者也應該盡可能地維持自己的軟體版本處在較新的狀態以確保安全。

雖然有些人認為在第一時間更新可能會因為更新檔案和之前既存的版本產生衝突或產生新的漏洞而拒絕更新，不過這樣子反而可能錯過漏洞修補的機會。比方說 2017 年 5 月爆發的勒索蠕蟲病毒 WannaCry 所使用的作業系統漏洞，其實微軟公司早在同年的 3 月就已經發布更新程式修補該漏洞，如果使用者當時有進行更新就可以避免中毒，也就不會損失重要的資料。



二、安裝防毒軟體

防毒軟體（英語：Antivirus software）是能夠偵測、移除病毒、蠕蟲、和特洛伊木馬程式等惡意程式的軟體。防毒軟體會透過比對用以識別病毒程式特徵的「病毒碼」、或是透過觀察目標程式的行為來辨別是否中毒，並進一步進行清除、隔離等對應行動以確保資訊安全。

因為病毒不斷的推陳出新，所以防毒軟體也需要定期更新病毒碼，才能盡可能的正確辨別出病毒、保護裝置。然而就像現實生活中發現病毒到識別毒株、找出解藥中間仍需要一些時間，所以不能認為裝了防毒軟體就百毒不侵，依然要做好其他保護措施才行。

例如以下幾個跡象發生的時候可能代表有惡意軟體在侵害你的電腦：

1. 電腦變得比以前慢

病毒在運作的時候會占用 CPU、記憶體或網路流量等系統資源，拖慢電腦整體的速度。

2. 好友收到奇怪信件或訊息

因為惡意程式可能會透過通訊錄，以電子郵件或即時訊息的方式擴散出去，所以當好友向你反應的時候就要特別注意。

3. 瀏覽器出現莫名其妙的工具列或附加元件

如果在瀏覽網站時畫面上彈出奇怪的視窗，瀏覽器很可能已被惡意程式入侵並安裝了一些附加元件。

4. 電腦開機時載入不明軟體

如果你看到某個應用程式在開機時自動載入，接著就立刻消失，或者在開機時看到不認識的應用程式，但你最近卻並未安裝任何軟體，那麼你的電腦很可能已遭感染。

雖然目前的防毒軟體多能夠在第一時間將中毒的檔案進行隔離，但若是不幸中毒，會建議依照以下的順序進行處理：

1. 進行隔離，避免受害範圍擴大

將電腦關機，網路切斷，移除外接式的裝置，目的是為了讓病毒停止運作和避免傳染擴散。

2. 在安全乾淨的環境中進行解毒

若是已經有足以辨識出病毒的資訊，則可以上網搜尋解決方案並依照步驟處理；或是直接使用防毒軟體來協助掃瞄並清除病毒。

3. 系統與資料的恢復

將受損的軟體、程式重新安裝，使用備份的資料讓系統重新回復正常運作。

三、資料備份

數位型態的資料最大的特徵之一就是因為它是由數字所構成，所以可以完美地進行複製－原版檔案和複製品在構成上完全的一致，沒有差異。也因此可以透過備份的方式很好的避免資料或系統被破壞，維持其可用性。

在確定備份範圍後，開始進行備份的時候有幾個重要的原則，分別是：

1. 複數備份

俗話說「狡兔有三窟」，建立多個備份檔有助於降低被害和資料損壞的風險。用極端一點的例子來說，假設每個檔案損壞的機率都是 1%，有三份備份檔案就相當於把損壞的機率降低為本來的 3 次方，也就是 0.0001%。

2. 異地儲存

使用不同形式的儲存方式並存放在不同的地方，也就是「不要把雞蛋放在同一個籃子裡」的概念。透過存放在不同的裝置，例如把備份分別儲存在隨身碟和網路

雲端硬碟中並且將隨身碟放置在學校，這樣不管是遇到數位資料檔案的損壞或是儲存設備地點上的損壞（如房間發生火災），都能夠確保還有備份可以使用。

3. 定期更新

由於資料也會不斷的新增和修改，因此定期更新備份才不會發生雖然有備份但是備份檔卻過於陳舊無法使用的狀況。目前有許多雲端儲存服務、手機系統都有提供自動定期備份的功能以確保使用者的。

四、良好的使用習慣

如同之前提及的，現在有許多攻擊手段和散佈手法中是透過人性的弱點來誘騙使用者，所以養成良好的使用習慣有助於避開很多隱藏的風險。

1. 保持警覺

由於許多的攻擊都是透過人性的弱點來誘騙使用者上鉤，例如在彈出廣告、電子郵件中放上中獎訊息、便宜商品、色情內容、恐嚇威脅吸引點擊；或是利用人的粗心不查以仿真的網站或信件詐騙個資。所以時時保持懷疑和警覺，不要過於貪心好奇，並多方進行檢查（如網址、寄件者）和查證，就可以避免掉很多陷阱。

近年來因為上架容易，有許多免費的手機應用軟體（APP）甚至會用資安工具作為包裝，暗藏惡意程式，所以使用者在下載前可以透過觀察 APP 商品資訊中的公司及使用者評價來協助判斷是否安全。另外，有許多 APP 會做許多超出其功能應有的權限要求，比方說明明是單機手機遊戲卻要求存取通訊錄聯絡人，就很有可能有問題。

2. 避免曝露

當離開電腦或手機的時候，記得關機、登出帳號或以密碼保護，避免無關人士能夠隨意的瀏覽或操作。密碼本身也要注意不要使用太過簡單或是預設的密碼，以免讓人可以輕鬆猜出。

在網路上發言或活動的時候，也要注意不要暴露過多自身的訊息，比方說真實的姓名、聯絡方式或住所，以免惹來不必要的困擾。極端一點的案例是 2019 年日本有女偶像因為自拍照中瞳孔反射出住處附近的街景，而引來瘋狂粉絲循線找到並猥褻。

3. 培養應對能力

如果能夠隨時注意可能的危害新知，並且知道對應的處理方式，就可以避免真的在遭受攻擊時因為慌亂而無法正確處理，縮小被害範圍。比方說在大多數的情況下，當發現自己中了勒索病毒，應該要立刻切斷網路並關閉電源，避免讓病毒繼續加密尚未受害的檔案，再尋求解密的方法或使用備份進行復原。

「三」絕韋編 – 鑑往知來

參考資料

1. Samantha D. Haworth (2014). Laying Your Online Self to Rest: Evaluating the Uniform Fiduciary Access to Digital Assets Act. (University of Miami Law Review). Retrieved form https://repository.law.miami.edu/umlr/vol68/iss2/10/
2. 如何保護網路上的個人資料？（民 106 年 9 月 27 日）。全民資安素養網。取自 https://isafe.moe.edu.tw/article/1831?user_type=4&topic=8
3. 保護社群網站上個資你可以這樣做（民 108 年 10 月 1 日）。全民資安素養網。取自 https://isafe.moe.edu.tw/article/2101?user_type=4&topic=8
4. 小治（民 101 年 10 月 1 日）。新版個資法上路，4 個重點、8 大案例，認識網路個人資料保護問題【T 客邦】。取自 https://www.techbang.com/posts/10878
5. 熊貓燒香（民 109 年 2 月 3 日）。維基百科。取自 https://zh.wikipedia.org/wiki/ 熊猫烧香
6. 惡意軟體（民 108 年 12 月 2 日）。維基百科。取自 https://zh.wikipedia.org/wiki/ 恶意软件
7. Google Ads 說明（民 109）。Google Ads 說明文件。取自 https://support.google.com/google-ads/answer/2375413?hl=zh-Hant
8. Trend Labs 趨勢科技全球技術支援與研發中心（民 107 年 12 月 24 日）。【資安漫畫】什麼是網路釣魚？何謂 Phishing? (同場加映 : 魚叉式網路釣魚 Spear Phishing) 【部落格文字資料】。取自 https://blog.trendmicro.com.tw/?p=136
9. 網路釣魚（民 108 年 12 月 15 日）。維基百科。取自 https://zh.wikipedia.org/wiki/ 钓鱼式攻击
10. The Worst Passwords of 2019（民 108 年 12 月 23 日）。SECURITY。取自 https://www.securitymagazine.com/articles/91461-the-worst-passwords-of-2019
11. WannaCry（民 109 年 2 月 22 日）。維基百科。取自 https://zh.wikipedia.org/wiki/WannaCry
12. Trend Labs 趨勢科技全球技術支援與研發中心（民 107 年 12 月 24 日）。《資安漫畫》系統漏洞是什麼？為何要更

新修補程式？【部落格文字資料】。取 自 https://blog.trendmicro.com.tw/?cat=3220
13. Trend Labs 趨勢科技全球技術支援與研發中心（民 105 年 7 月 5 日）。「只要不點入可疑網站就不會中毒」?!【部落格文字資料】。取自 https://blog.trendmicro.com.tw/?p=18525
14. 中央社（民 105 年 10 月 22 日）。瀏覽合法官網也會中毒？問答集一次看懂。中時電子報。取自 https://www.chinatimes.com/
15. Unknown（民 98 年 9 月 15 日）。[技術分享] 網頁掛馬攻擊 (Drive-by Downloads) 介紹【部落格文字資料】。取自 http://cyrilwang.blogspot.com/2009/09/drive-by-downloads.html
16. 防毒軟體（民 108 年 7 月 7 日）。維基百科。取自 https://zh.wikipedia.org/wiki/ 杀毒软件
17. Trend Labs 趨勢科技全球技術支援與研發中心（民 106 年 12 月 22 日）。如何判斷電腦已遭感染？電腦中毒的 4 個跡象【部落格文字資料】。取 自 https://blog.trendmicro.com.tw/?p=53651
18. Trend Labs 趨勢科技全球技術支援與研發中心（民 106 年 3 月 30 日）。世界備份日 (World Backup Day)：三二一原則【部落格文字資料】。取 自 https://blog.trendmicro.com.tw/?p=4707
19. 劉惠琴（民 108 年 3 月 7 日）。你手機安裝的免費 App 會外洩個資嗎？隱私自保 2 招撇步學起來。自由時報。取自 https://news.ltn.com.tw/
20. Trend Labs 趨勢科技全球技術支援與研發中心（民 107 年 2 月 22 日）。下載應用程式時為何要注意存取權限設定？【部落格文字資料】。取自 https://blog.trendmicro.com.tw/?p=54309
21. 談雍雍（民 108 年 10 月 9 日）。狂粉用「瞳孔倒影」找到住處　女偶像慘遭襲擊猥褻。TVBS 新聞網。取自 https://news.tvbs.com.tw/
22. Trend Labs 趨勢科技全球技術支援與研發中心（民 107 年 2 月 22 日）。感染勒索病毒的四個主要症狀與緊急措施【部落格文字資料】。取 自 https://blog.trendmicro.com.tw/?p=38368
23. 資通安全處（民 102 年 11 月 26 日）。使用個人電腦應注意事項為何？行政院國家資通安全會報。取自 https://nicst.ey.gov.tw/Page/16FFA138E66A0905/6da2af6e-8f10-4eac-8b30-4a1c2b559302
24. 資通安全處（民 106 年 1 月 6 日）。行動裝置資通安全注意事項 (簡要版)。行政院國家資通安全會報。取自 https://nicst.ey.gov.tw/Page/16FFA138E66A0905/a91dad4c-11e6-43e7-a4bb-23af28029988
25. 資通安全處（民 102 年 10 月 24 日）。常見的社交工程攻擊方式有哪些？應如何防範？行政院國家資通安全會報。取自 https://nicst.ey.gov.tw/Page/16FFA138E66A0905/6aececb4-50ec-4c3e-b331-d8e0ddfc4586

「四」通八達－小試身手

自我檢測

Q１：請同學使用「How Secure Is My Password?」或「Password Strength Checker」等密碼強度檢測網站測試自己的密碼強度，並嘗試什麼方式可以有效地增加自己密碼強度。

Q２：請同學分享一下再哪些網站很容易看到彈出式視窗？這些彈出式視窗的內容又通常是什麼類型的？

Q３：如果使用無痕式視窗瀏覽網頁，就真的安全了嗎？無痕式視窗可以避免掉那些危險？又可能會有遭遇那些資安問題？