第4章 資料保護與資訊安全

- 個人資料的定義
- 個人資料的保護措施
- 資訊安全與防範措施

翰林出版

目　錄

資料保護與資訊安全

1. 個人資料的定義

2. 個人資料的保護措施

3. 資訊安全與防範措施

個人資料保護法

簡稱個資法

動畫 個資法

■為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用。

■個資的保護涉及個資的運用（包括蒐集、處理及利用）及法令的規範。

- 姓名
- 出生年月日
- 國民身分證統一編碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 聯絡方式
- 財務情況
- 社會活動

哪些個資在尊重當事人及合法情況下，可以蒐集、處理或利用呢？

哪些個資在尊重當事人及合法情況下，可以蒐集、處理或利用呢？

- 姓名
- 出生年月日
- 國民身分證統一編碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 聯絡方式
- 財務情況
- 社會活動

- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

哪些個資在尊重當事人及合法情況下，可以蒐集、處理或利用呢？

- 姓名
- 出生年月日
- 國民身分證統一編碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 聯絡方式
- 財務情況
- 社會活動

- 病歷
- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

- 直接識別該個人之資料
- 間接識別該個人之資料

個人資料保護法

- **學號、電子郵件、會員編號**等，屬於「其他得以直接或間接方式識別該個人之資料」，同樣受個資法保護。

- 因執行業務的需求，必須依法令規定，才能蒐集，所以**病歷、醫療、基因、性生活、健康檢查及犯罪前科**等資料，除有規定外，不得蒐集、處理或利用。

常見的使用個資示例

■線上購物、網拍社群網站：

信用卡資料/客戶資料/宅配地址

■醫院、診所、健康檢查中心：

健檢報告/病歷/診斷書

■戶政、財稅、監理等政府單位：

身分證號碼/報稅資料/駕照申請或換發

■電信、網路業者：

帳單地址/電子郵件信箱/帳戶資料

■銀行、百貨公司、大賣場：

帳戶資料/會員資料/周年慶抽獎卷

■學校、社區活動中心：

學籍資料註冊/報名資料/家長會聯絡

個人資料合理使用

- 各機關對個資的蒐集、處理及利用，應有特定目的，並經當事人同意。

- 當事人對他的個資有**決定權**及**控制權**，可對蒐集單位行使下列權利：**查詢或閱覽、製給複製本、補充或更正、停止蒐集、處理或利用、刪除**。

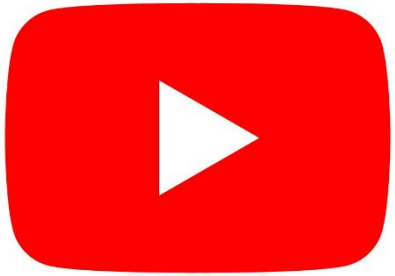
個人資料合理使用

個人資料合理使用

個人資料合理使用


學校想邀請您來當講師，需要您提供個資。
那講座結束後，我可以要求貴校刪除我的個資嗎？
講師資料
學歷：_____
聯絡方式：____
沒問題，這是法令規定的，請放心。

個人資料合理使用



- 當事人可自由選擇提供個資，但也要了解不提供時對自己權益的影響。例：到**銀行開戶**，如果**不提供申請表需要的個資，就無法完成開戶手續**。

- 當事人如果了解蒐集單位對個資運用的相關事項，並提供個資，蒐集單位需依**個資法規定**，確保個資正確及安全。

翰林出版

個資保護案例

近年來，許多校園為打造智慧校園，開始引入**人臉辨識**技術。臺灣人權促進會、人本教育基金會、臺灣學生聯合會等團體指出，人臉辨識技術作為一種監控技術，倘若裝設於師生皆會活動或停留的場域，除了是否符合**個資法的爭議**外，對於長時間生活在校園內的師生來說，後續更可能會因**資料管理不當**，導致生物特徵外洩。

個資保護案例

對於校園內使用人臉辨識技術對師生可能造成隱私侵害，教育部目前並沒有要求學校一定要使用人臉辨識，同時指示校園若使用人臉辨識，也應符合個資法關於資料蒐集、處理、利用的規範，也會會持續跟學校宣導使用相關技術的規範事宜。

個資保護的法令規定

- 公務機關保有個資檔案者，需專人負責管理，以防個資被非法竊取、竄改、毀損、滅失或洩漏。如：教育部為保護高中學生學習歷程檔案的安全，規定相關人員有登載不實，導致影響學生的權益，應負法律責任。
- 非公務機關(私人醫院、私立學校…)持有個資檔案者，須訂個資檔案安全維護計畫或業務終止後個資處理方法。未善盡保護違反規定者，除罰款，情節嚴重者要負刑事責任 。

翰林出版

個資保護的法令規定

翰林出版

個資保護的法令規定

翰林出版

個資保護的法令規定


同學，這是僱用工讀契約，請你簽名並提供相關個資。
老師，如果契約期間結束，我的個資會怎麼處理呢？
工讀生勞動契約書
甲方：_____
出生年月日：_____
身分證字號：_____
ooooooooooooooooo
ooooooooooooooooooooooo
放心，依個資法有訂定個資檔案處理辦法，學校會妥善保管你的個資，若未保護個資也會受到政府處罰。
學 務 處

個資保護的注意事項

網路詐騙案件層出不窮，手法不斷更新，為確保個資安全，個人應注意下列事項：

1. 不要任意將個資提供給他人。
2. 登入電腦系統完成作業後，務必登出帳號。
3. 與他人共用電腦時，切記關閉瀏覽器視窗並清除紀錄。
4. 避免使用任何人都能連接上網的無線網路。

個資保護的注意事項

5. 避免透過公用電腦使用網路服務。
6. 經常變更密碼，勿與其他系統的密碼共用。
7. 勿點選來路不明的網址及程式。
8. 安裝防毒軟體，且隨時更新。
9. 勿書寫密碼在他人可取得的地方。
10. 勿把密碼記錄於電腦或行動裝置內。

個資保護的注意事項

個資保護的注意事項

翰林出版

資訊安全與防範措施

■ 資訊安全(資安)指保護資料及資訊系統，使其不會受到非法進入、揭露、破壞等侵害。

■ 在網路環境，資訊交換或傳遞易被截取、入侵或攻擊，要了解資安問題，可以從資安意識、資安技術及資安管理等議題來討論。

影片 矯正網路使用習慣 防範資安漏洞

動畫 資訊安全

影片 行動裝置陷資安危機 防範有撇步

資安意識

- 資安意識指認識資安問題並了解其重要性，以及理解資訊的安全與相對的風險。
- 無論是數位資訊或是傳統資料，其資安主要涉及資料本身的
  機密性（Confidentiality）
  完整性（Integrity）
  可用性（Availability）
- 三者簡稱為 CIA，違反任一項，會讓資料或系統處於高風險狀態。

■ 機密性（Confidentiality）

在資料傳遞與儲存過程中確保其隱密性，避免未授權的使用者有意或無意的揭露資料 。

■ 完整性（Integrity）

避免資料遭到未經授權的使用者所竄改。

■ 可用性（Availability）

能夠讓資料隨時保持堪用的狀態。

資安意識

- 駭客不僅透過網路入侵，竊取敏感資訊，甚至綁架資料進行勒索，更嚴重者則透過網路進行攻擊，以致於讓網路無法正常運作。
- 資訊安全就是為了防範這種資訊被盜竊或攻擊所採取的防範措施。

資安技術

常見的資安技術有

1. 數位浮水印
2. 防火牆
3. 加密

數位浮水印

- 數位浮水印是指將**特定的資訊嵌入**於數位資料中。
- 若要複製有數位浮水印的資料，也會將嵌入的資訊複製下來。
- 數位浮水印分為**顯性**和**隱性**兩種。

數位浮水印

■ 數位浮水印分為顯性和隱性兩種。

顯性：肉眼可見的浮水印資料，通常含著作權所屬者的名稱或標誌。

隱性：用數位的方式加入資料中，一般無法看見，藉由隱密的設計，來避免或阻止資料未經授權而被非法複製，以保護著作權。

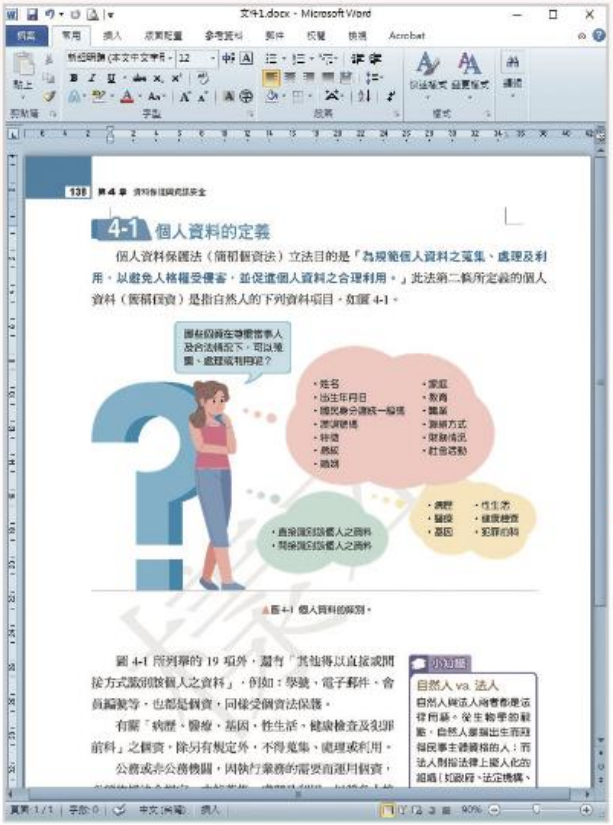
數位浮水印

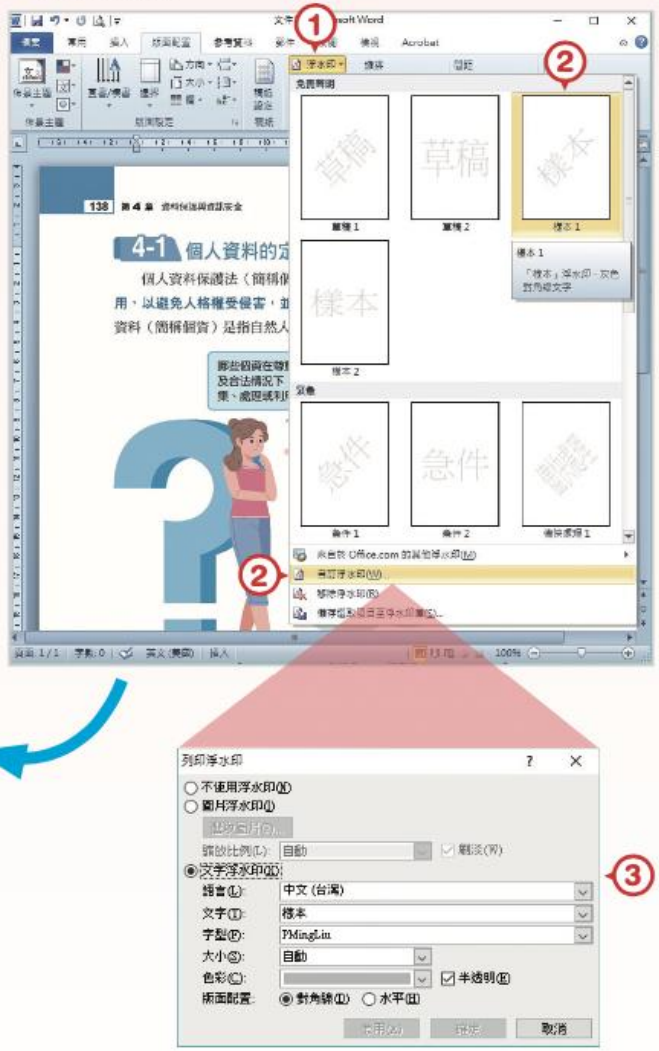
① 點選 Word 版面配置功能中的浮水印。

② 選擇配置的樣式或自訂浮水印。

③ 若選擇自訂浮水印，可進行各選項的調整。

▼圖 4-6 加上數位浮水印的檔案（以 Microsoft Word 2010 為例）。





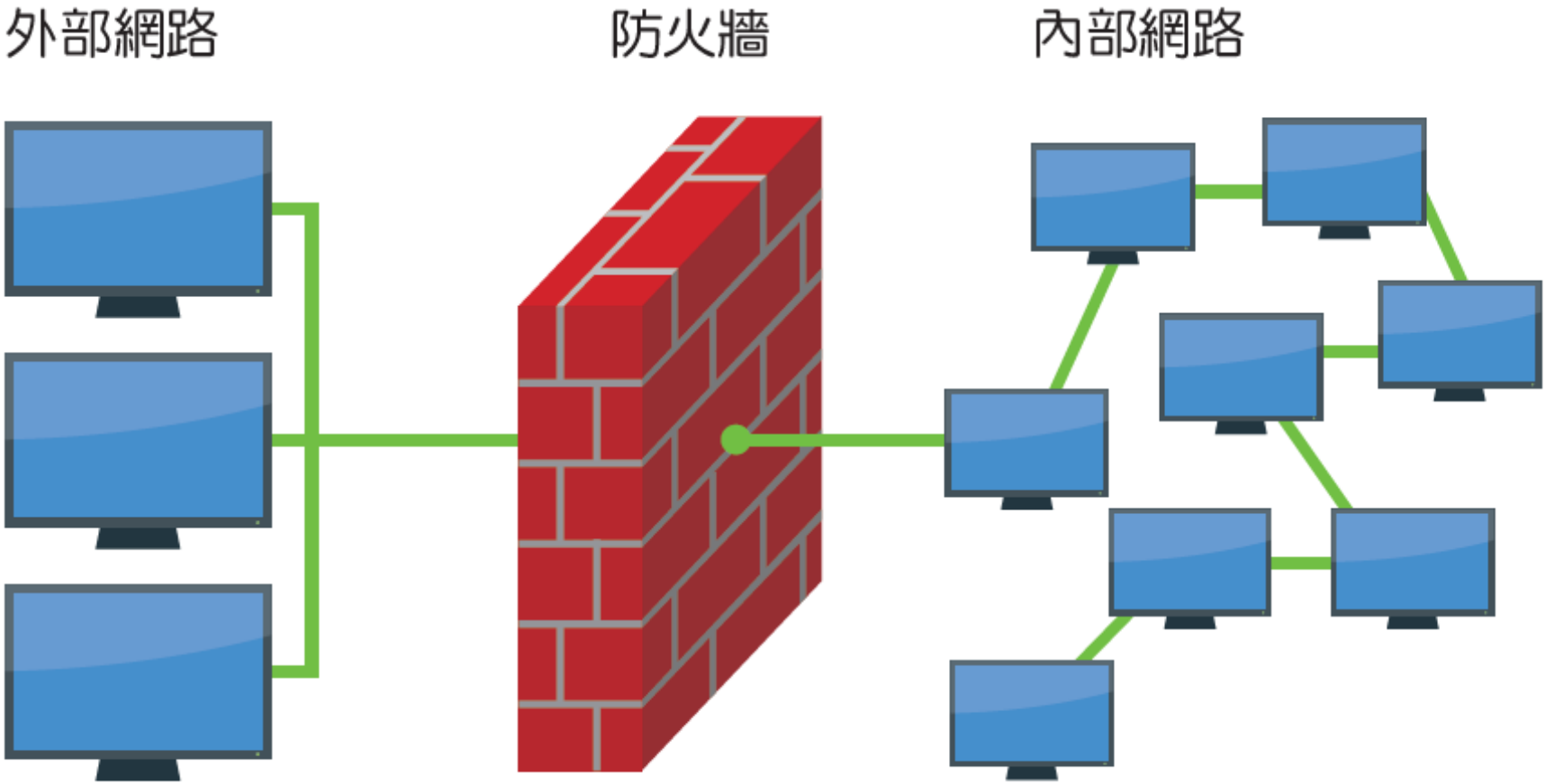
防火牆

- 防火牆是協助保障資訊安全的裝置。
- 可以是擁有專屬功能的硬體，或是用軟體的方式架設在一般硬體上。運作方法是依設定的規則，如：透過**封包**的篩檢，**允許**或**限制**傳輸的資料通過。

封包

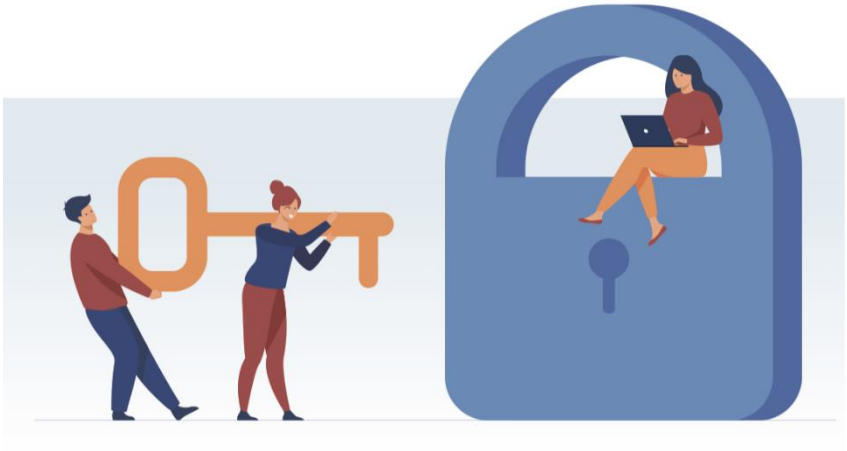
網路上傳送資料時，需先將資料依既定格式，切割為一個一個小塊，此一小塊稱為封包。

防火牆



加 密

- 加密是原始資訊經由加密過程，轉換為**無法直接讀取內容**的資訊。
- 只有知道解密方法者，經由解密過程，才能將密文還原為可讀的明文內容。



資安管理

- 機構為防範非法入侵或攻擊的安全措施，除了資安技術之外，更要從資安管理著手。

- 資安管理主要有3A 安全防護與4D 防護管理兩種資的機制。

3A 安全防護

- 組織內部的使用者如果不當使用系統內的個資，會導致資料外漏。
- 系統安全防護，常採取：**認證（authentication）**、**授權（authorization）**、**紀錄（accounting）**三層機制來管理資安的問題，也就是 **3A 安全防護**。

3A 安全防護

第一層：認證

認證是資訊系統辨別使用者的身分，通過辨識才能進入系統，也可**記錄資訊曾被何種身分的人使用過**。

3A 安全防護

第二層：授權

授權是用於**資源的存取控管**，判定使用者是否有權使用特定的資源，依使用者身分或工作權限，給予他所能擁有的權限。

例如：**教務處及學務處可以取存學生的資料應該要有差異**。教務處只能讀取/儲存學習成績資料；學務處僅能管理獎懲資料。

3A 安全防護

第三層：紀錄

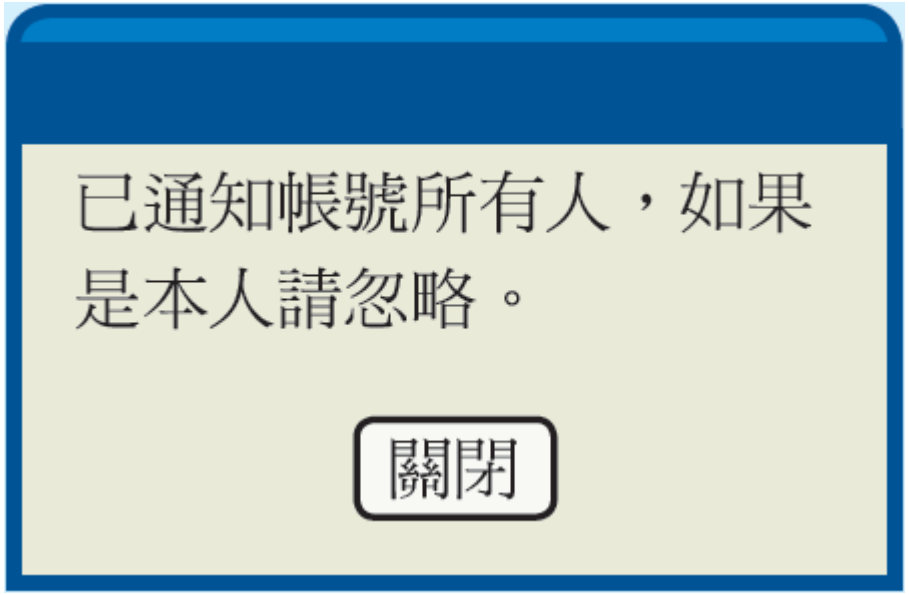
紀錄在於蒐集使用者與系統之間互動的資料，**使用者在系統中進出、存取、更動等行為，都會留下紀錄**，一旦系統出現異常，可供後續的查核。

防護管理

- 防護管理是為了防止從外部透過非法管道入侵組織網路的防護機制，以保護個資及資訊系統的安全。
- 4D防護管理包括
  - 嚇阻（deter）
  - 偵測（detect）
  - 阻延（delay）
  - 禁制（deny）

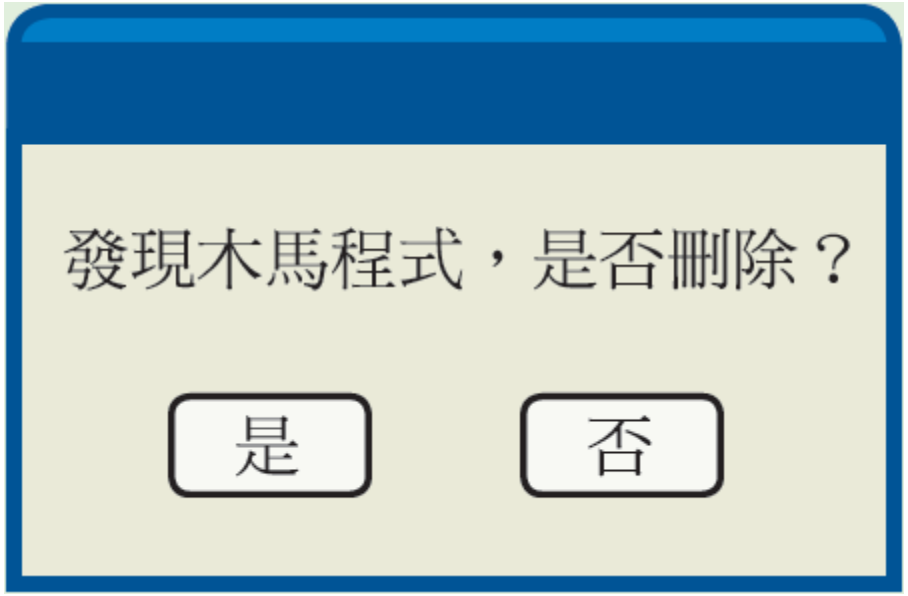
防護管理

嚇阻(deter)：
讓想入侵者知道風險高而放棄入侵。



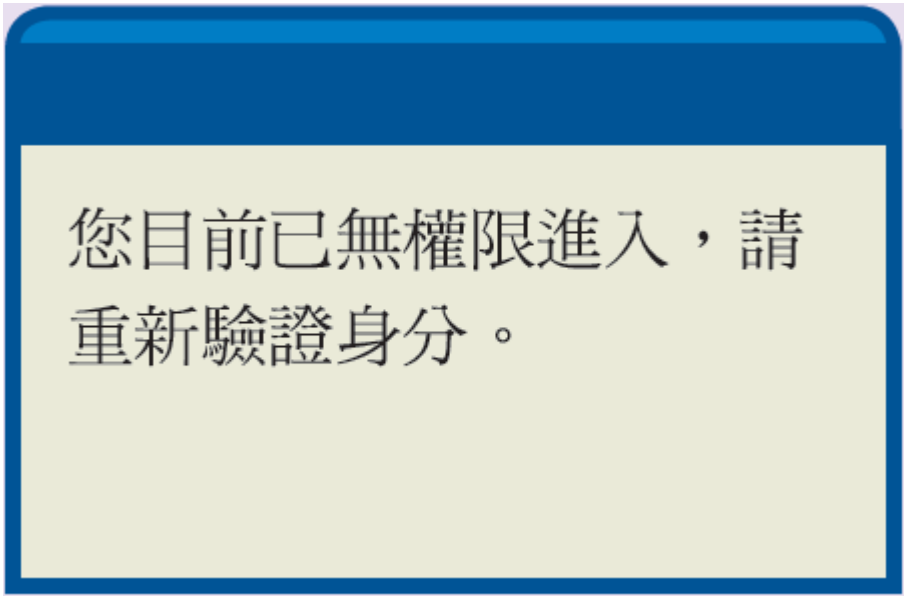
防護管理

偵測(detect)：
系統能及時發現入侵行為。



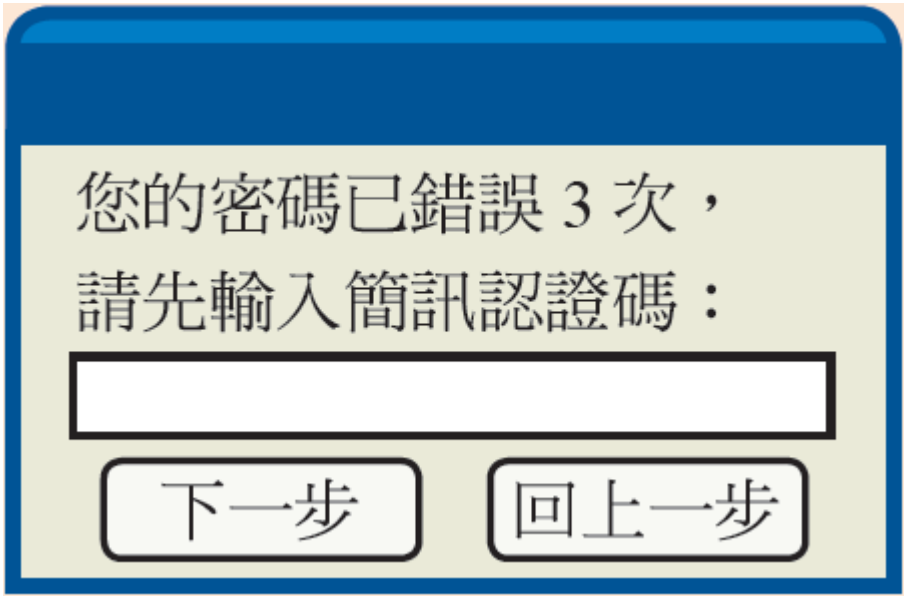
防護管理

阻延(delay)：
因防禦力強，使入侵行為費時而容易被發現。



防護管理

禁制(deny)：
直接阻止入侵行為。



3C 安全防護基本功

隨著科技發達與 3C 產品盛行，全民資安素養網提供 4 種安全防護方式及其操作說明：

1. 設定手機與電腦的螢幕上鎖密碼。
2. 為電腦安裝防毒軟體。
3. 絕對不點擊來路不明的超連結。
4. 更新系統與軟體。

（資料來源：全民資安素養網）

網路通訊的管理防護

除了資安技術與資安管理之外，系統安裝防毒軟體、辨別釣魚網站、避免社交工程攻擊，以及接收電子郵件等也是個人維護資安應注意的事項。

安裝防毒軟體

- 安裝防毒軟體是一般的電腦安全防護措施，不僅能防止病毒入侵，也可封鎖詐騙網站 。

- 並不是裝了防毒軟體，電腦系統就安全無慮，因新病毒隨時在產生，所以要持續更新病毒碼，才發揮防毒功效。此外，應設定主動掃描，且定期執行。

文件加密

- 機密性高的文件，透過網路傳輸時，可將文件**加密成為無法辨識的密文**，提高安全性。

- 操作實例：將「我的病歷資料」word 檔案加密。

我的病歷資料

文件加密

將「我的病歷資料」word 檔案加密

步驟1 開啓檔案

①開啟我的病歷資料檔案

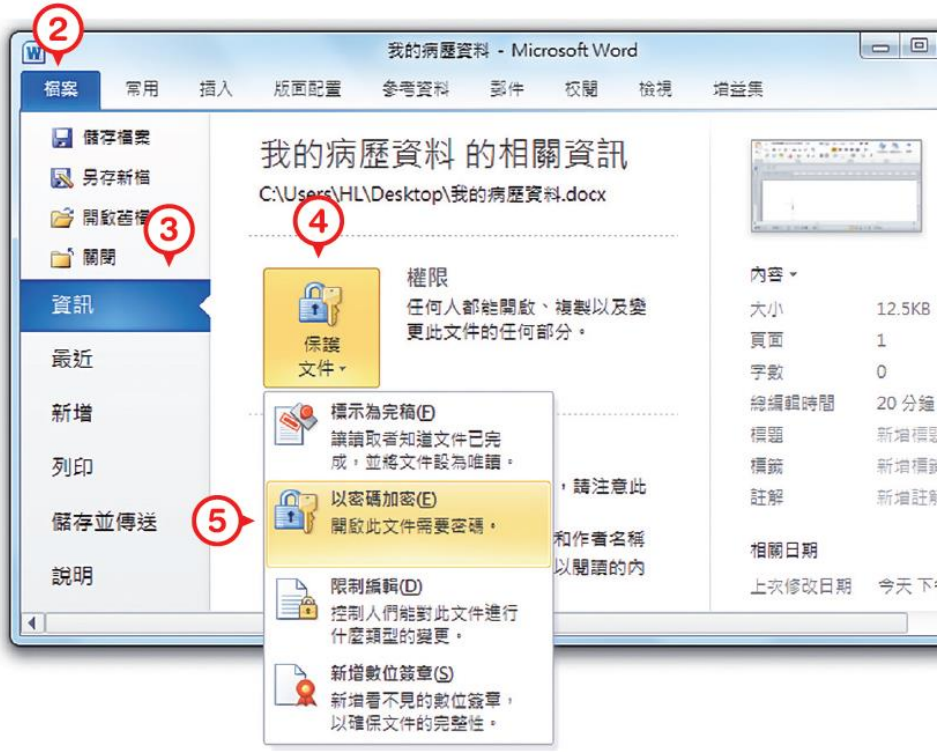
步驟2 將檔案加密

②點選檔案

③點選資訊

④點選保護文件

⑤點選以密碼加密



翰林出版

文件加密

將「我的病歷資料」word 檔案加密

步驟3 設定密碼

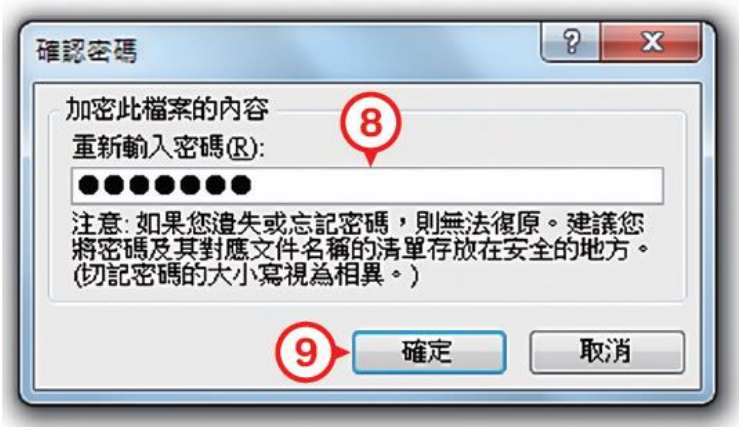
⑥ 輸入**密碼**

⑦ 按下**確定**

步驟4 確認密碼

⑧ 再次輸入**密碼**

⑨ 按下**確定**



文件加密

將「我的病歷資料」word 檔案加密

步驟5 加密完成

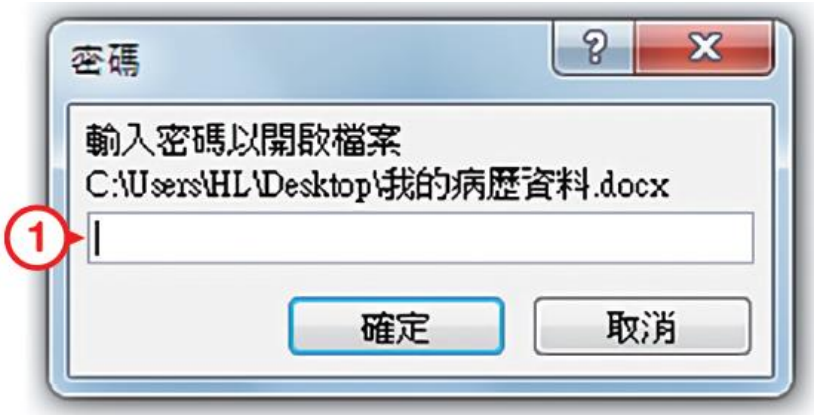
⑩ 出現**開啟此文件需要密碼**，表示此檔案已經加密。

文件加密

開啟加密後的「我的病歷資料」檔案

步驟1 開啟加密檔案需輸入密碼

① 如果要開啟加密檔案時，就會彈出密碼視窗，輸入**密碼**後，才能開啟檔案。

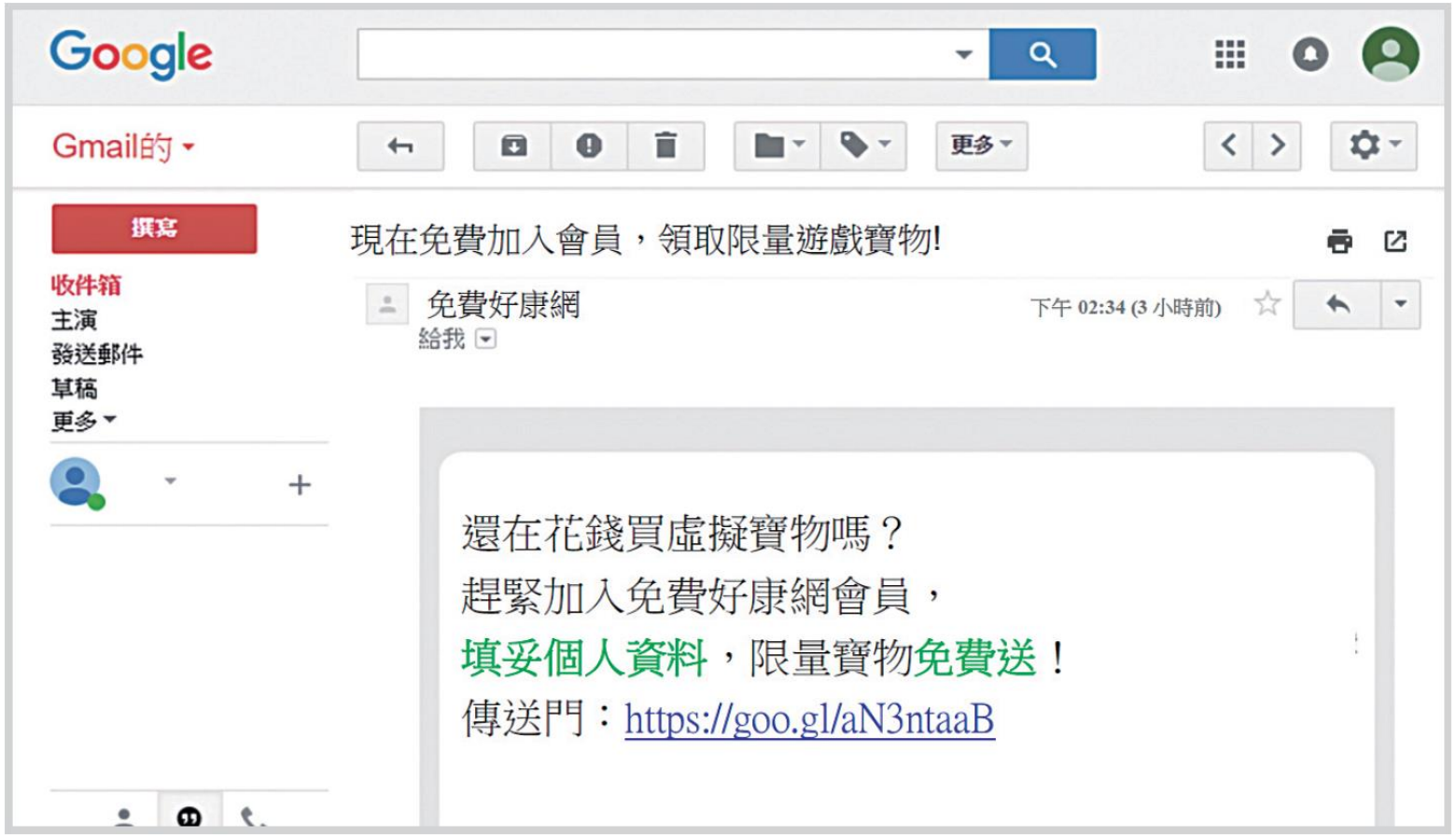


避免社交工程攻擊

- 社交工程是竊取資料的攻擊行為，早期社交工程使用電話或信件方式來詢問個資，而目前都使用電子郵件或網頁來進行攻擊。

- 社交工程是利用人性弱點或人際的信任關係，以獲取不當資訊。(不用程式技巧即可取得帳號、密碼、身分證號碼、信用卡密碼…等，足以辨識個人身分或機密資料)。

避免社交工程攻擊



▲圖 4-10 引誘提供個資的社交工程攻擊。

用電子郵件應注意事項

辨別網路釣魚：

- 有不少冒用資訊單位或學校名義，散發系統通知郵件，例如更新您的帳戶、Confirm email或「Attention：E-mail User」等主旨，想引誘及詐騙收件者提供帳號及密碼、點選郵件所附的連結或執行附加檔案等。

- 這類郵件通稱為網路釣魚（Phishing），就是利用假冒的身分，使人疏於求證而提供個人的帳號、密碼或卡號等機密資料。

常見電子郵件詐騙手法

網路使用普遍，電子郵件成為駭客攻擊、詐騙的管道之一，近年來 5 項常見的電子郵件詐騙手法簡述如下：

1. 不要隨意點開連結。
2. 把常用網站設為「我的最愛」或「書籤」。
3. 觀察網站的內容。
4. 確認網站是否有提供聯絡資訊。
5. 對於需要提供個人資料的網站提高警覺。

（資料來源：全民資安素養網）

用電子郵件應注意事項

辨別網路釣魚：

- 收到此類郵件，建議**直接刪除**，不要回應，也**切勿點選郵件上的連結或打開附件**。

- 一般機構的資訊中心皆有隨時更新郵件過濾機制及封鎖釣魚網站，但還是防不勝防，根本的防護之道是使用者要有**資安意識**，自己要熟悉如何辨識網路釣魚，以及如何設定收信軟體的過濾功能，**降低被駭/受害**的機會。

避開網路釣魚的陷阱

避開網路釣魚的建議：

1. 不要隨意點開連結。
2. 把常用網站設為「我的最愛」或是「書籤」。
3. 觀察網站的內容。
4. 確認網站是否有提供聯絡資訊。
5. 對於需要提供個人資料的網站提高警覺。

(資料來源:全民資安素養網)

用電子郵件應注意事項

判斷郵件的真偽：

- 非法人士常用電子郵件，企圖瞞騙或盜取重要個資。

- 收到電子郵件時，可以從寄件者、郵件主旨與附加檔案三方面來判斷郵件的真偽。

用電子郵件應注意事項

判斷郵件的真偽：

▲圖 4-12 需注意的電子郵件項目。

用電子郵件應注意事項

判斷郵件的真偽：

- **寄件者：**
  是否與你認識，並確認電子郵件信箱位址是正確的。如果信箱位址來自於**教育機構（.edu）**、**政府機構（.gov）**、**非營利機構（.org）**，可疑程度較低；否則要提高警覺。
- **郵件主旨：**
  與你無關，建議直接刪除，如果用詞怪異、過於聳動或看似緊急，或是察覺與發信人的習慣不同則要小心。

用電子郵件應注意事項

判斷郵件的真偽：

- **附加檔案：**
  若附加檔案名稱顯示**檔名怪異**、錯誤，切勿開啟開啟，建議直接刪除。
  副檔名為 .docx、.pptx 等附件，應特別小心，勿任意開啟，另外有雙副檔名者， 如 .jpg.exe，應立即刪除。
- **可疑郵件：**
  寄信非正常時間、陌生或極少來往的人的來信、要求提供敏感資料的信件。

常見的副檔名

.exe　執行檔
.txt　記事本文字檔
.bmp 圖片格式
.gif　圖片格式
.png 圖片格式
.jpg 圖片格式
.jpeg 圖片格式
.svg 圖片格式
.pdf PDF 檔案

用電子郵件應注意事項

判斷郵件的真偽：

- 非公務業務相關、不明來源與可疑的郵件，建議直接刪除、切勿開啟，也勿轉寄。

- 不輕易點選、下載或回傳電子郵件內的連結、附件檔案與資料。

問題與討論

你還想知道什麼?

線上派卷

第 4 章已經全部學習完畢，
點擊**速測派**按鈕進行題目練習！

速測派