

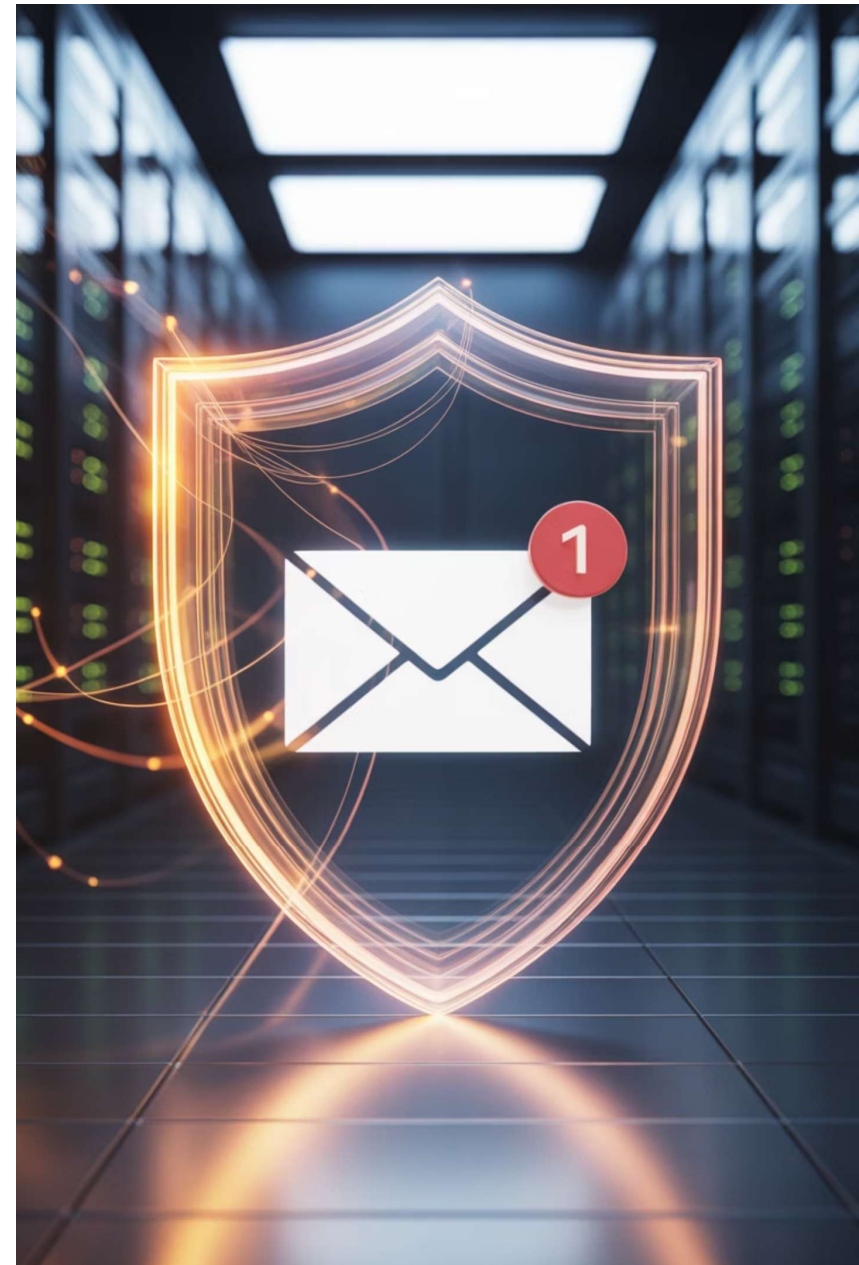


## 校園資安防護三合一： 社交工程防範、反詐騙與個資保護實務

透過案例解析與實務操作，協助教職員強化資安意識，建立辨識與防護能力，避免因社交工程、詐騙手法或個資管理疏失導致校園資通安全事件。

# 識破假郵件、守護真安全

電子郵件社交工程防範實務教育訓練



# 課程目標與重要性

本課程旨在全面提升本校教職員工對電子郵件社交工程攻擊的防範能力。隨著網路攻擊手法日益精進，電子郵件已成為駭客最常利用的入侵管道。透過系統性的教育訓練，我們將協助全體同仁建立完整的資安防護意識。



## 強化辨識能力

學會識別各類釣魚郵件與可疑內容的關鍵特徵



## 掌握防範技巧

建立正確的郵件處理流程與安全操作習慣



## 落實通報機制

熟悉校內資安事件通報與應變處理程序

# 為何電子郵件成為主要攻擊途徑

電子郵件社交工程攻擊已成為校園資安的首要威脅。根據資安機構統計，超過 90% 的資安事件源自於電子郵件攻擊。駭客利用人性弱點，透過偽造身分、製造緊迫情境等手法，誘使受害者洩漏機敏資訊或執行惡意程式。

大專院校因具有多元使用者、開放網路環境及大量個人資料等特性，更容易成為攻擊目標。一次成功的攻擊可能導致帳號外洩、研究資料竊取、系統癱瘓等嚴重後果，影響層面涵蓋個人隱私、校務運作甚至學術聲譽。





# 校園資安威脅現況

近年來大專院校面臨的電子郵件攻擊事件持續攀升，攻擊手法也更加專業化。了解當前威脅態勢，是建立有效防護的第一步。

90%

郵件攻擊佔比

資安事件中由電子郵件  
引發的比例

65%

校園目標率

教育機構成為攻擊目標  
的增長幅度

3分鐘

平均反應時間

使用者點擊釣魚連結的  
平均時間

48小時

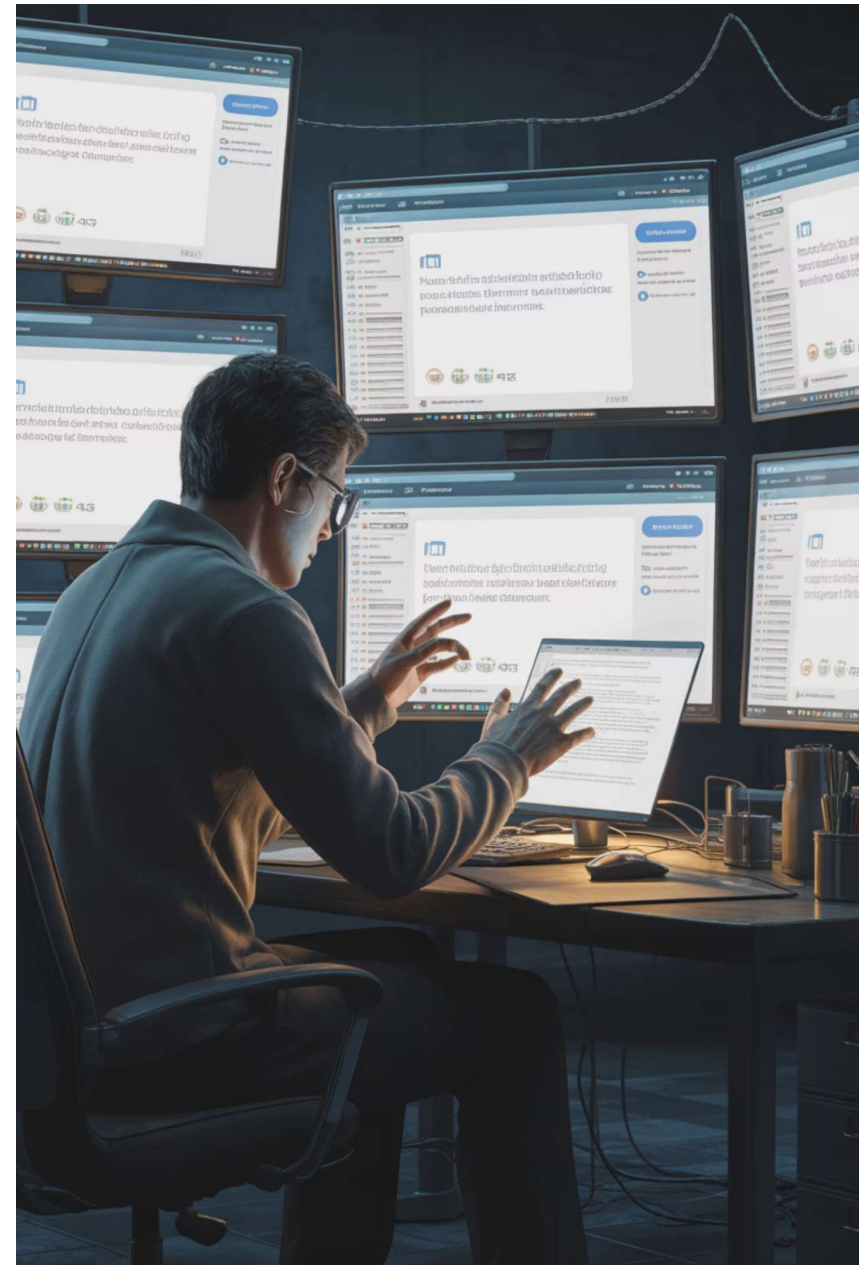
黃金處理期

發現異常後的關鍵通報  
時限

# 第一單元

## 電子郵件社交工程攻擊概論

建立基礎認知，了解攻擊本質與運作機制

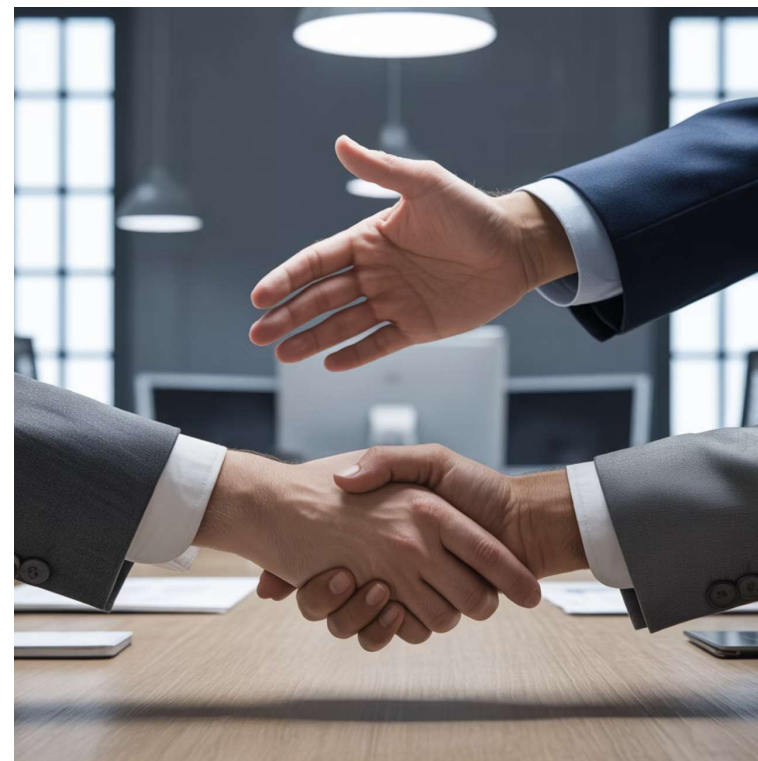


# 什麼是社交工程攻擊

社交工程攻擊是一種利用人性弱點而非技術漏洞的攻擊手法。攻擊者透過心理操縱、身分偽造、情境營造等方式，誘騙目標執行特定行為，進而竊取機敏資訊、植入惡意程式或取得系統存取權限。

電子郵件是社交工程攻擊最常使用的媒介，因為它具有易於偽造、成本低廉、覆蓋範圍廣等特性。攻擊者可以短時間內發送大量郵件，只要有少數人受騙上當，就能達成攻擊目的。

「最脆弱的資安環節不是系統，而是人。」



# 社交工程攻擊的四個階段

了解攻擊流程有助於在各階段及時識破並中斷攻擊鏈。每個階段都有其特定目的與手法特徵。



## 1. 誘導階段

建立信任感，偽裝成可信身分（主管、系統管理員、官方單位）



## 2. 引信階段

設計觸發機制，製造緊急情境或利益誘因，促使目標採取行動



## 3. 感染階段

執行惡意程式、導向釣魚網站，或誘騙輸入帳密等機敏資料



## 4. 竊取階段

取得目標資料、帳號權限或系統控制權，達成攻擊最終目的



# 電子郵件攻擊的常見管道

攻擊者會針對不同對象與目的，選擇適合的攻擊管道。校園環境中存在多種潛在風險入口。

## 個人信箱

透過公開資訊取得教職員個人郵件地址，發送偽裝成官方通知或個人邀請的釣魚郵件

## 校務信箱

利用校內通訊錄或公開聯絡資訊，假冒內部單位發送看似正常的公務郵件

## 群組郵件

透過系所、委員會等群組名單，一次觸及多位目標，擴大攻擊範圍與成功機率

## 回覆劫持

入侵他人帳號後，利用既有郵件串進行回覆，提高受信者的信任度

# 攻擊者如何選定目標



社交工程攻擊的成功關鍵在於充分的事前準備。攻擊者會透過多種管道蒐集目標資訊，包括學校網站、社群媒體、學術資料庫、公開研究計畫等。

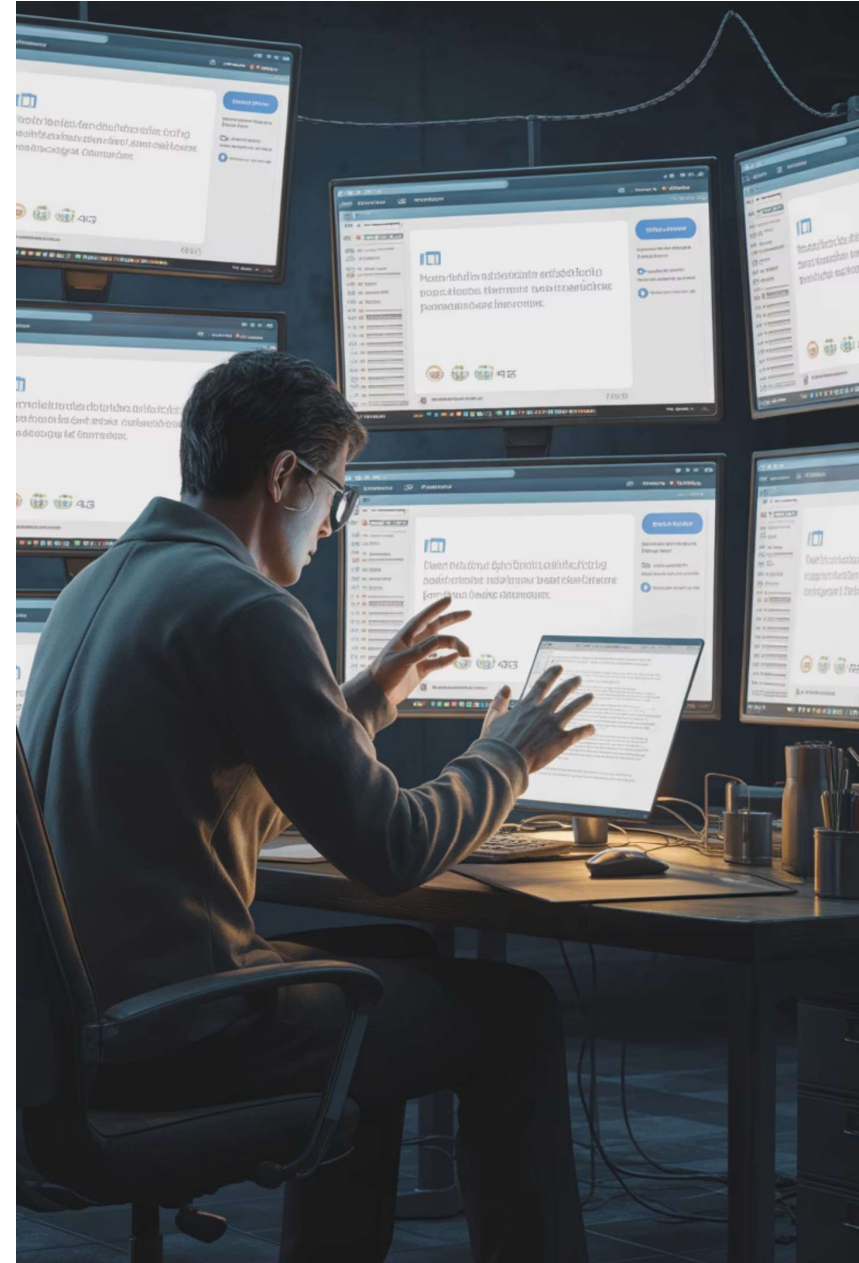
## 資訊蒐集重點

- 組織架構與職務關係
- 個人興趣與社交習慣
- 近期活動與重要事件
- 常用系統與作業流程
- 郵件格式與溝通風格

這些資訊讓攻擊者能夠精準客製化郵件內容，大幅提升攻擊的可信度與成功率。

# 第二單元

## 常見攻擊手法與郵件特徵



# 攻擊手法類型總覽

以下是針對大專院校最常見的電子郵件社交工程攻擊類型。每種手法都有其特定的偽裝方式與攻擊目的。

## 假冒主管指令

偽裝成校長、院長、主管等高階人員，發送緊急指示要求協助處理特定事項

## 假學校公告

仿冒教務處、學務處等行政單位，發送看似正式的通知或政策變更訊息

## 假系統通知

假借資訊室、圖書館等單位名義，要求更新帳密或執行系統維護操作

## 假獎助學金

偽造獎學金、研究補助或經費核銷通知，誘騙填寫個資或下載惡意檔案



# 案例一：假冒主管指令郵件

這是校園中最常見且成功率極高的攻擊手法。攻擊者利用職務權威與時間壓力，降低收件者的警覺性。

## □ 典型郵件範例

**寄件者：**校長室 <president.office@gmail.com>

**主旨：**緊急：需要您協助處理重要事項

**內容：**「您好，我目前正在開會不便使用手機。請立即協助購買 10 張面額 1000 元的超商禮券，用於急需的來賓接待。請先墊付，稍後會歸還款項。請將禮券序號以回信方式提供。此事急迫，請勿對外張揚。謝謝配合。」

# 假冒主管郵件的判讀重點

## 寄件者郵址異常

注意「gmai1.com」（數字1）而非「gmail.com」，或使用免費信箱而非校內官方信箱

## 要求不尋常行為

正常公務流程不會要求個人墊款購買禮券，更不會透過郵件傳送序號

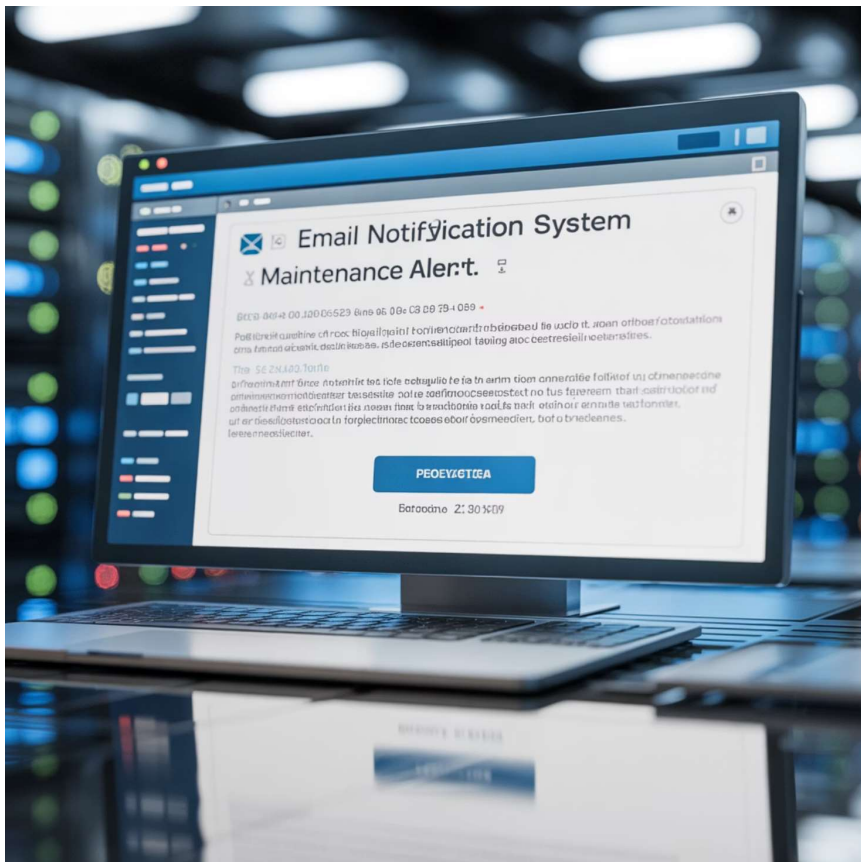
## 製造時間壓力

強調「緊急」、「立即」、「今日內完成」等緊迫用詞，迫使倉促決策

## 限制對外求證

「請勿對外張揚」是阻止受害者向他人確認的典型話術

## 案例二：假冒資訊室通知



### □ 典型郵件範例

寄件者：資訊中心 <it-support@university-system.com>

主旨：【重要】您的信箱即將超過容量限制

內容：「系統偵測到您的電子郵件帳號已使用 95% 容量。為避免無法收信，請於 24 小時內完成容量擴充作業。請點擊以下連結登入並確認帳戶資訊：[\[https://univ-email-upgrade.com\]](https://univ-email-upgrade.com)。逾期未處理將暫停信箱服務。資訊中心 敬啟」

# 假系統通知的辨識要點

系統維護通知是最容易讓人失去戒心的攻擊類型，因為看似技術性且來自官方單位。

1

## 檢查網域名稱

正確的校內信箱網域應為 @學校名稱  
.edu.tw，而非外部或相似網域

2

## 驗證連結網址

將滑鼠移至連結上（不要點擊），檢查實際  
導向網址是否為校內系統

3

## 質疑緊急時限

真正的系統維護通常會提前多日通知，不會  
要求 24 小時內完成

4

## 避免直接登入

不透過郵件連結登入，改以書籤或手動輸入  
網址進入官方系統



# 案例三：假冒獎助學金通知

此類郵件利用金錢利益誘因，特別容易讓師生放鬆警戒。附件檔案往往暗藏惡意程式。

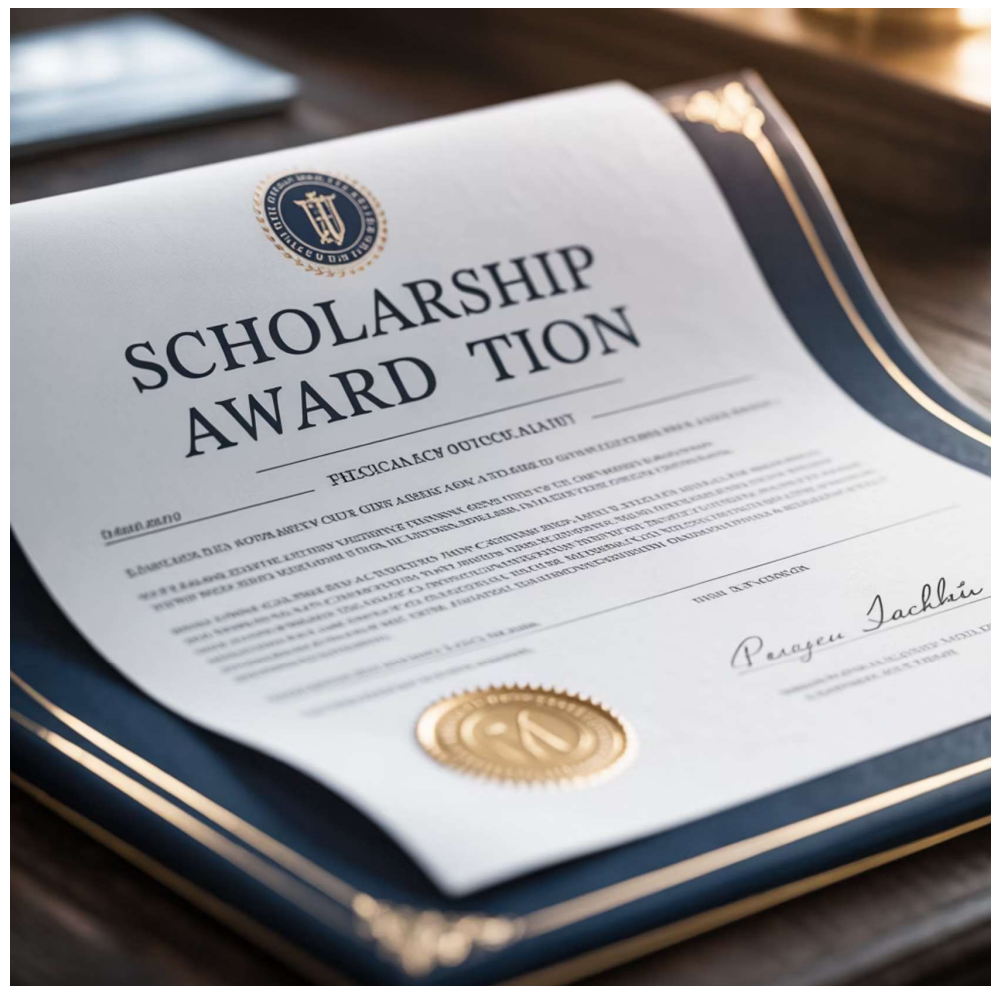
## □ 典型郵件範例

寄件者：學生事務處獎助組 <scholarship@edu-tw.info>

主旨：恭喜！您符合 112 學年度特殊貢獻獎學金資格

內容：「您好，經評選委員會審核，您獲得本年度特殊貢獻獎學金，金額新台幣 30,000 元。請下載附件申請表格填寫完整資料（包含身分證字號、銀行帳戶資訊），並於三日內回傳。逾期視同放棄資格。」

附件：獎學金申請表.xlsm ( 2.3 MB )



# 惡意附件的常見型態

附件是植入惡意程式的主要途徑。以下是最需要警戒的檔案類型與其風險特徵。



## **.exe / .scr / .bat**

可執行檔案，開啟後會直接執行程式碼。絕對不應透過郵件接收此類檔案



## **.zip / .rar / .7z**

壓縮檔案常用於隱藏惡意程式，繞過郵件系統的掃描機制



## **.xlsm / .docm / .pptm**

含有巨集的 Office 檔案，巨集可執行任意程式碼，風險極高



## **.pdf ( 含連結 )**

PDF 本身相對安全，但內嵌的超連結可能導向釣魚網站

## 案例四：假冒會計系統更新

針對行政人員設計的攻擊，利用公務流程與系統操作的熟悉感降低戒心。

### □ 典型郵件範例

寄件者：會計室系統管理員 <accounting-sys@campus-mail.net>

主旨：【系統升級】會計系統安全性更新通知

內容：「各位同仁好，為強化系統安全性，會計系統將於今日 18:00 進行更新。請所有使用者於更新前完成帳號驗證，以確保更新後能正常登入。請點擊以下連結完成驗證：

[<https://accounting-verify.campus-update.com>]。驗證時需輸入帳號、密碼及手機驗證碼。未完成驗證者將暫時無法使用系統。造成不便敬請見諒。會計室 資訊組」

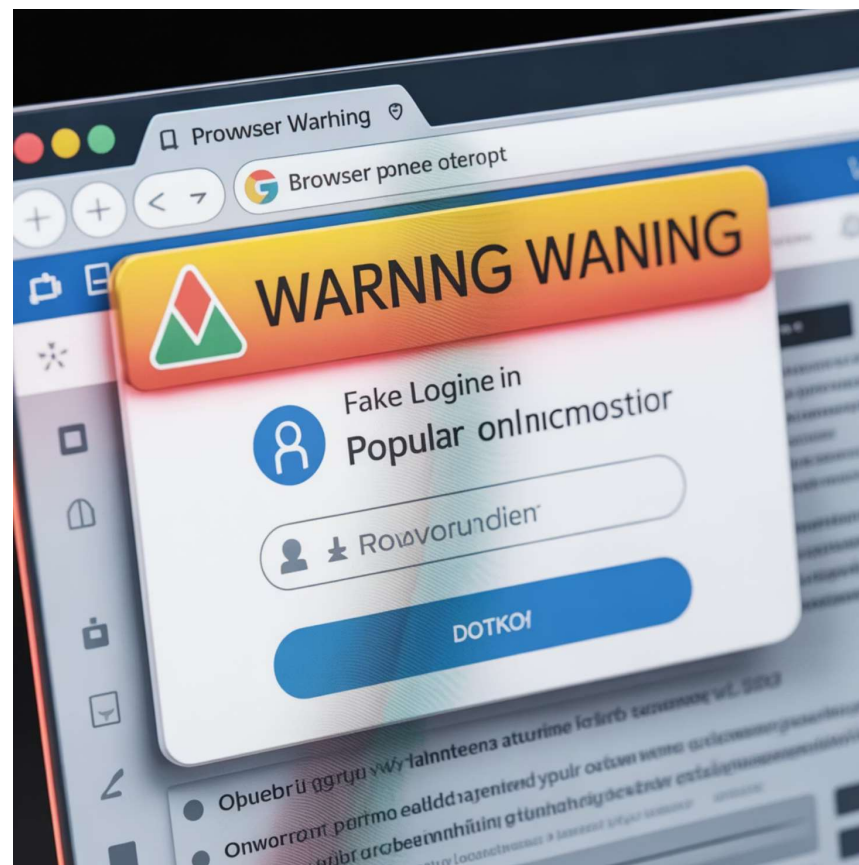
# 釣魚網站的辨識技巧

釣魚網站是用來竊取帳密的假網站，外觀常仿造得與真實網站極為相似。掌握以下辨識技巧可有效避免受騙。

## 網址檢查要點

- **網域名稱**：正確的校內系統應為「xxx.學校簡稱.edu.tw」
- **加密協定**：確認網址開頭為「https://」且有鎖頭圖示
- **拼字差異**：注意 O/0（英文O與數字0）、l/I（大寫I與小寫l）等混淆字元
- **子網域陷阱**：「university.fake-site.com」中真正的主網域是「fake-site.com」

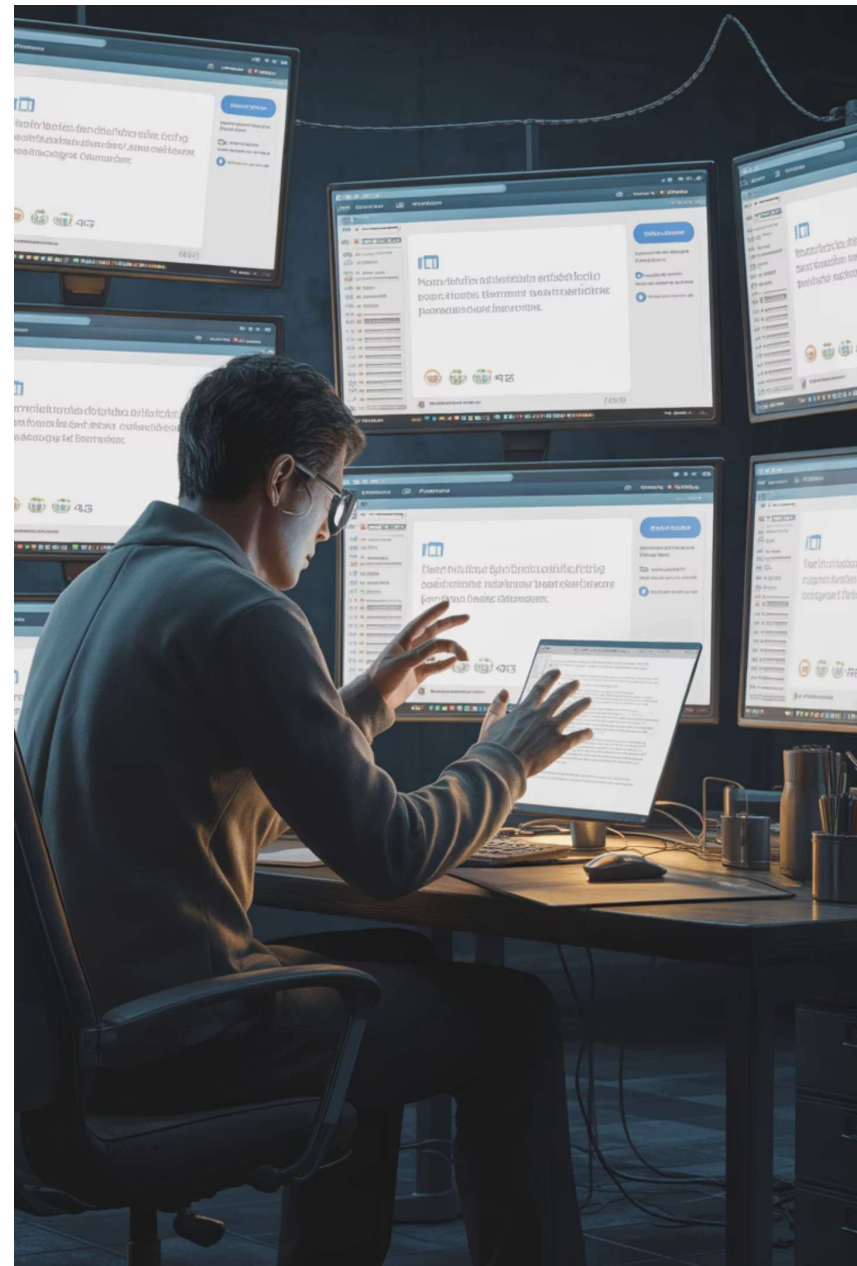
❏ **重要提醒**：永遠不要透過郵件連結登入重要系統，應使用書籤或直接輸入網址



# 第三單元

## 郵件判讀與防範技巧

建立系統化的郵件檢視流程，從技術面強化防護能力



# 郵件檢視的六步驟流程

養成以下檢視習慣，可以在開啟郵件的第一時間識別大部分的威脅。



## 步驟一：檢視寄件者

確認寄件者姓名與郵址是否相符，注意顯示名稱可以任意偽造

## 步驟二：分析主旨

警戒過度緊急、誇張或與自身無關的主旨內容

## 步驟三：檢查收件人

注意是否為大量群發，或收件人與內容不符的情況

## 步驟四：預覽連結

將滑鼠停留在連結上（不點擊），檢查實際導向網址

## 步驟五：檢視附件

確認附件類型是否合理，警戒可執行檔與含巨集檔案

## 步驟六：評估內容邏輯

思考郵件要求是否符合正常流程與常理



# 寄件人檢查的關鍵細節

寄件人資訊是最容易被偽造的部分，必須仔細檢視多個層面才能確認真偽。

## 顯示名稱

可任意設定，即使顯示「校長室」也不代表真的是校長發送。務必檢查實際郵址

## 郵件地址

檢查「@」後的網域是否為官方網域，注意相似但不同的網域名稱

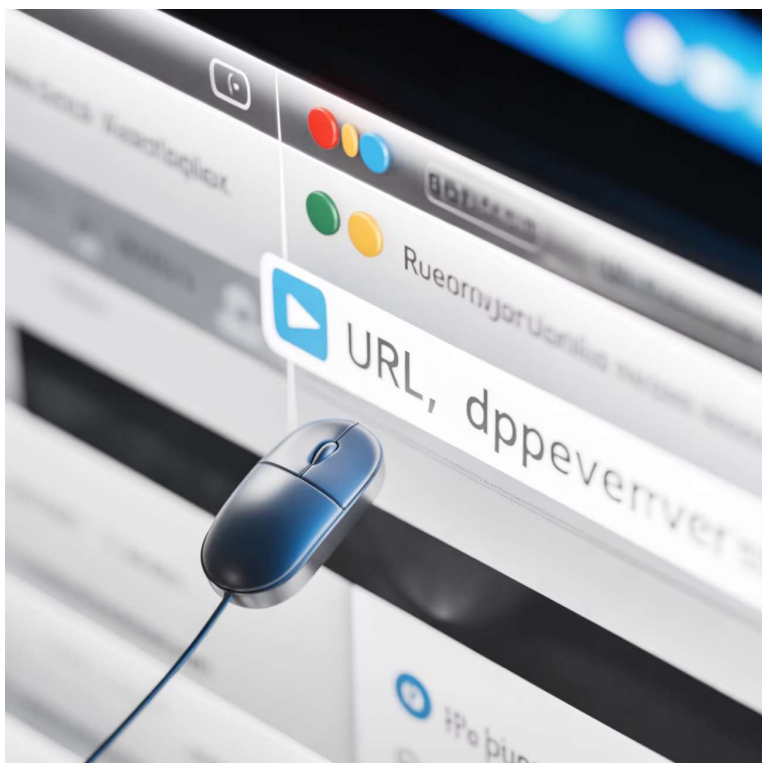
## 回信地址

有些攻擊會設定不同的回信地址，點選「回覆」時要特別注意收件者變化

## 簽章資訊

正式公文通常包含完整的單位、職稱、聯絡方式，格式混亂或資訊不全都是警訊

# 連結安全檢查方法



連結是導向釣魚網站的主要途徑。在點擊任何連結前，務必先進行檢查。

## 滑鼠預覽法

將滑鼠游標移至連結上方（不要點擊），瀏覽器或郵件程式會在左下角或彈出視窗中顯示實際網址。檢查該網址是否為預期的目的地。

## 短網址風險

bit.ly、tinyurl.com 等短網址服務常被用來隱藏真實目的地。收到短網址時，可使用短網址還原服務（如 checkshorturl.com）先查看真實網址再決定是否點擊。

- 📌 **最佳實務：**對於重要系統，不使用郵件中的連結，而是透過已儲存的書籤或手動輸入網址登入

# 防範原則：三不一要一再確認

將防範要點濃縮為簡單易記的口訣，幫助在面對可疑郵件時快速做出正確判斷。

## 不輕信

保持懷疑態度，特別是涉及金錢、機敏資訊或緊急要求的內容

## 不點擊

不隨意點擊未經確認的連結，不下載來歷不明的附件

## 不洩漏

任何管道都不應提供帳號密碼、身分證字號等機敏個人資料

## 要通報

發現可疑郵件或誤點後，立即向資訊單位通報

## 再確認

透過既有管道（電話、當面確認）驗證郵件真偽

# 校內郵件安全設定

校內郵件系統已配置多項安全機制，但使用者仍需了解並正確運用這些功能。

## 垃圾郵件過濾

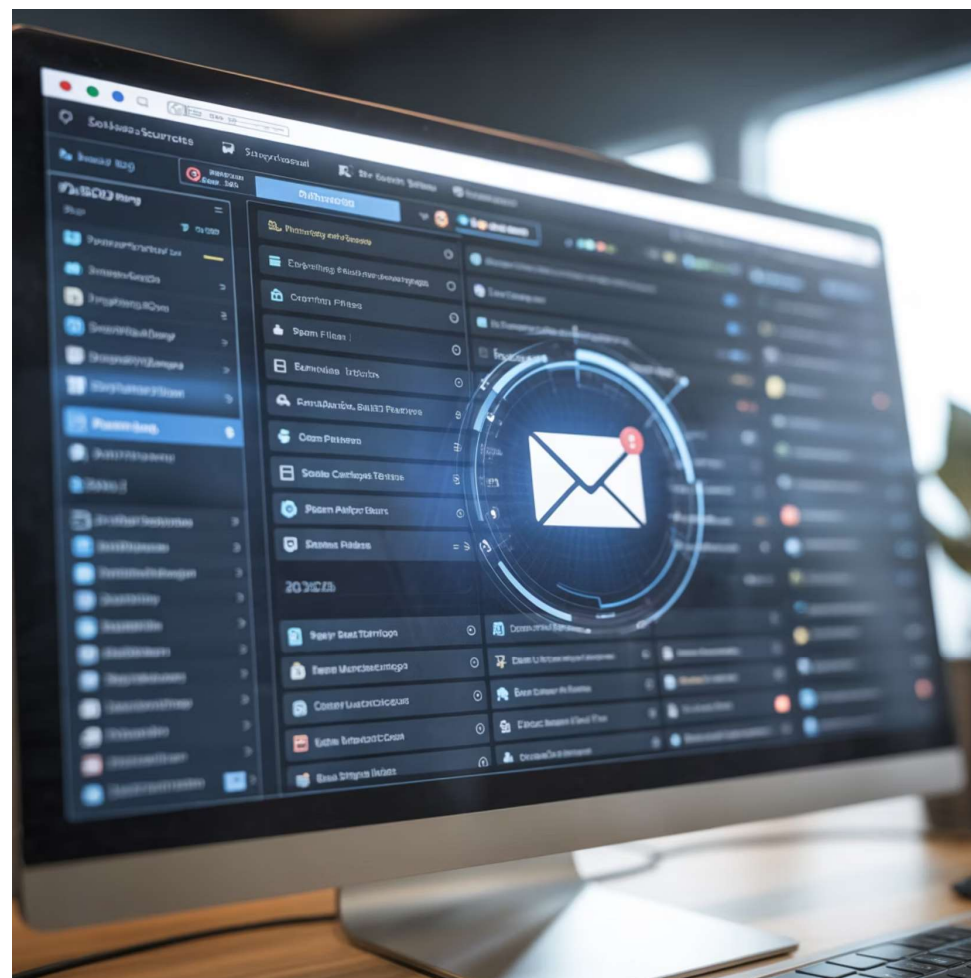
系統會自動將可疑郵件移至垃圾郵件資料夾。請定期檢查，確認沒有誤判的正常郵件，但不要輕易信任垃圾郵件中的任何內容。

## 外部郵件警示

來自校外的郵件會在主旨或內文開頭標註「外部郵件」警示。即使寄件者顯示為校內人員，只要有此標記就應特別謹慎。

## 附件掃描

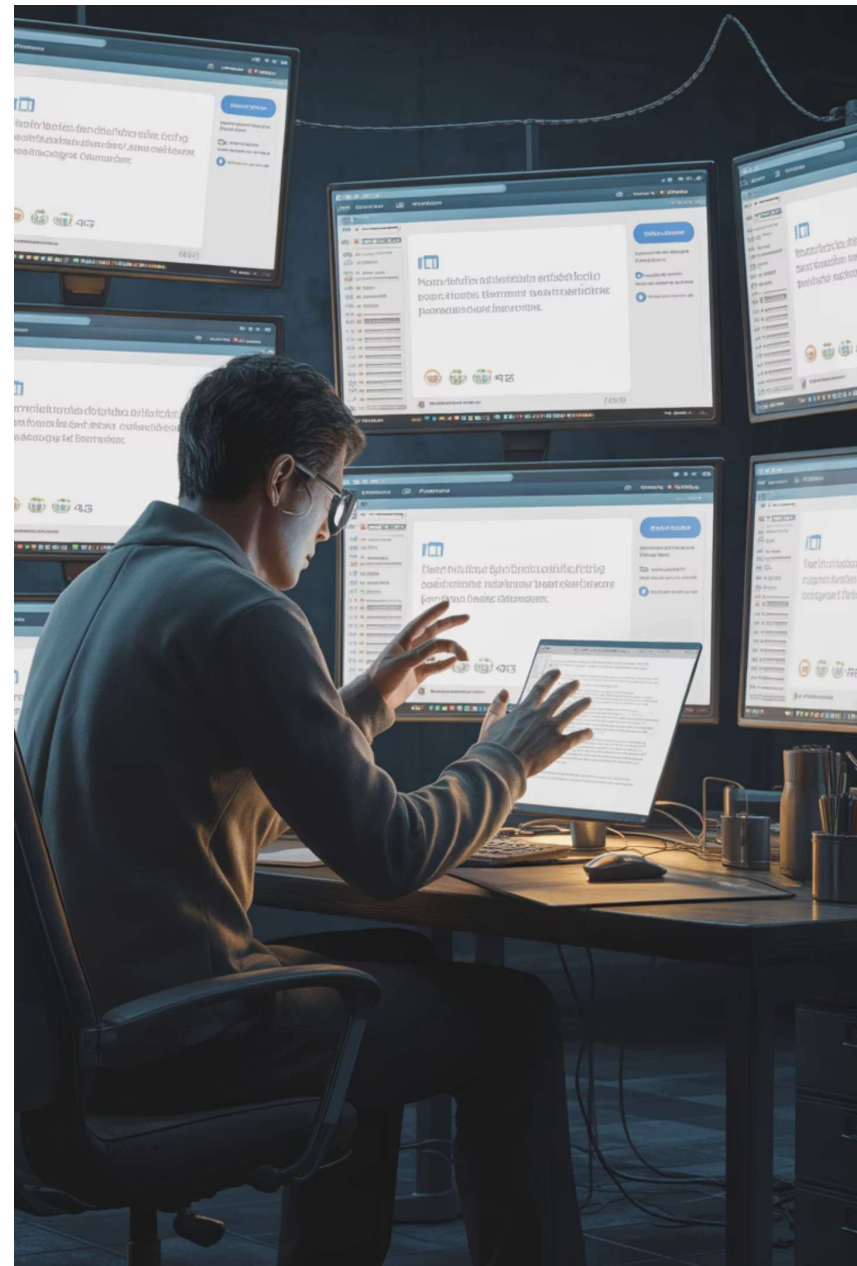
系統會自動掃描附件病毒，但無法偵測所有威脅。新型或變種惡意程式可能繞過掃描，因此不能完全依賴自動防護。



# 第四單元

## 實戰案例分析與演練

透過真實案例的深入分析,強化判斷能力與應變技巧



# 案例分析一：假冒校長郵件詳解

## ☐ 郵件內容重現

寄件者：校長 李大明 <president@gmail1.com>

主旨：【緊急】急需協助處理重要事項

內文：您好,我目前正在參加校外重要會議,手機訊號不佳無法接聽電話。有一筆急需支付的款項,麻煩您先協助墊付。請立即前往便利商店購買 10 張面額 1000 元的 Google Play 禮券,並將卡號序號拍照回傳。此事涉及重要貴賓接待,時間緊迫,請在今日下午 3 點前完成,切勿張揚。款項我會儘快歸還給您。謝謝配合。



# 案例一：可疑特徵分析

## 1 郵址拼字陷阱

「gmai1.com」使用數字「1」冒充字母「l」,真正的 Gmail 是「gmail.com」。這是常見的視覺欺騙手法

## 2 不合理的支付方式

正式公務不會要求個人墊款購買禮券,更不會透過郵件傳送序號。禮券是詐騙慣用的不可追蹤支付工具

## 3 製造時間壓力

「今日下午 3 點前」、「時間緊迫」等用詞意圖迫使匆忙決策,減少思考與求證的時間

## 4 限制求證管道

「切勿張揚」、「手機訊號不佳」預先阻止受害者向他人確認或透過電話聯繫校長

## 5 權威壓力

冒用校長身分利用職務權威,讓收件者不敢質疑或拒絕要求

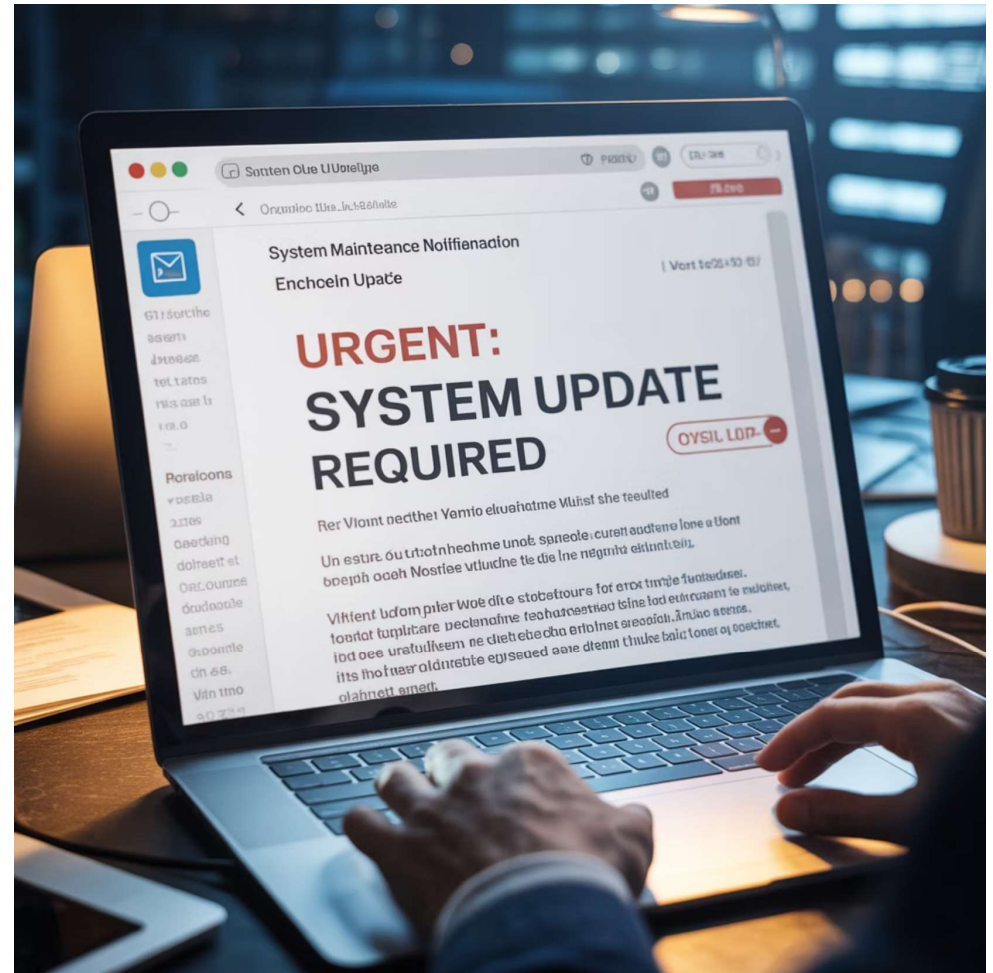
# 案例分析二：假系統維護通知

## ☐ 郵件內容重現

寄件者：資訊中心系統組 <it-service@university-sys.com>

主旨：【重要通知】電子郵件系統安全性升級

內文：親愛的使用者,為提升系統安全性,本中心將於今晚 23:00 進行郵件系統升級。為確保您的帳號能正常使用,請於升級前完成身分驗證。請點擊以下連結登入系統完成驗證:[<https://mail-verify.university-system.com/login>]。驗證時需輸入帳號、密碼及手機號碼。未於期限內完成者,系統將暫時凍結帳號以確保安全。造成不便敬請見諒。資訊中心 敬啟



## 案例二：破解關鍵點

1

### 網域名稱檢查

「university-sys.com」並非學校官方網域。  
正確的網域應為「university.edu.tw」格式

3

### 不合理要求

正常系統維護不需要使用者預先登入驗證,更不會要求提供手機號碼  
正確做法:不透過郵件連結登入,直接使用書籤或手動輸入官方網址檢查是否真有系統維護公告,或致電資訊中心確認。

2

### 連結分析

「mail-verify.university-system.com」的主網域是「university-system.com」,不是學校官方網域。子網域可以任意設定

4

### 威脅性語氣

「將暫時凍結帳號」製造恐慌,促使未經思考就採取行動

輸入官方網址檢查是否真有系統維護公告,或致電資訊中心確認。

# 案例分析三：惡意附件郵件

## ☐ 郵件內容重現

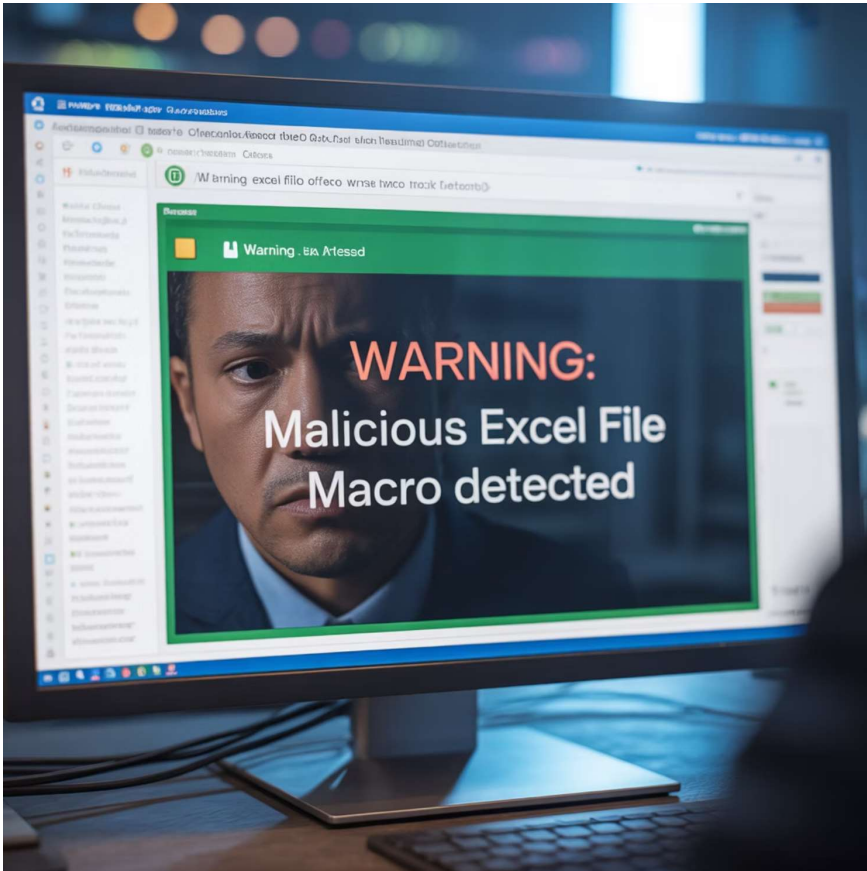
寄件者：會計室 <accounting@campus-mail.org>

主旨：112 學年度第二學期研究計畫經費核銷通知

內文:敬啟者,您的研究計畫「XXX」經費核銷作業已完成初審,請下載附件查看核銷明細並確認無誤。如有疑問請於三日內提出,逾期視同確認。附件採用新版格式,開啟時請啟用巨集功能以正常顯示內容。會計室

附件:經費核銷明細表\_112-2.xlsm (1.8 MB)

# 案例三：附件風險識別



## 危險信號清單

- **.xlsm 副檔名**  
「m」代表含有巨集(macro),可執行程式碼,是高風險檔案類型
- **要求啟用巨集**  
正常文件不需要巨集功能。「請啟用巨集」是惡意文件的典型話術
- **檔案大小異常**  
1.8 MB 對於試算表明細過大,可能包含隱藏的惡意程式碼
- **非官方網域**  
「campus-mail.org」不是學校正式網域,很可能是偽造的

📌 **防護建議:**收到含巨集檔案時,應透過其他管道確認來源。  
若確需開啟,應在隔離環境中操作,且絕不啟用巨集

# 真實案例啟示

回顧近年國內外大專院校發生的真實資安事件,了解攻擊的實際影響與教訓。

**某國立大學教授帳號被盜**  
因點擊釣魚郵件並輸入帳號,攻擊者取得郵件帳號控制權,對外發送詐騙郵件,影響校譽。損失:無法量化的聲譽損害

## **私立大學行政系統遭勒索軟體攻擊**

行政人員開啟惡意附件導致勒索軟體感染,校務系統被加密。損失:支付贖金約500萬元及一週系統停擺

## **研究資料外洩事件**

研究助理點擊假冒的雲端儲存連結,導致進行中的研究數據遭竊。損失:數年研究成果及潛在智慧財產權損失



# 課程重點回顧

讓我們快速回顧本課程的核心要點,這些原則應內化為日常工作習慣。

## 認識威脅

了解社交工程攻擊的四階段  
流程與常見手法特徵

## 建立警覺

掌握釣魚郵件的十大警訊,養成  
檢視郵件的六步驟習慣

## 正確防範

實踐「三不一要一再確認」  
原則,從根本阻斷攻擊途徑

## 有效應變

熟悉通報流程與應變措施,將損害控制在最小  
範圍

## 持續強化

保持學習態度,隨時更新對新型威脅的認知與  
防護能力



**校園反詐騙實務：**

**識「詐」防資訊，守「財」護人生**

**大專院校全體教職員工反詐騙教育訓練課程**

# 為什麼校園需要反詐騙教育？

## 詐騙案件持續攀升

根據警政署統計,詐騙案件逐年增加,校園成為詐騙集團鎖定的目標場域之一。

## 校園環境特殊風險

教職員工涉及財務、人事、採購、研究經費等多元業務,容易成為詐騙對象。

## 保護自己與他人

建立防詐意識不僅保護個人財產安全,更能協助學生與同事避免受騙。



# 課程五大核心目標

1

## 掌握詐騙型態

深入了解警政署統計與揭露的常見詐騙手法、話術模式與最新趨勢。

2

## 辨識高風險情境

學會從郵件、簡訊、電話、網路互動中快速識別可疑訊號與詐騙徵兆。

3

## 正確處理與通報

掌握遇到可疑情況時的正確應對步驟與校內通報流程。

4

## 落實防護習慣

在教學、行政、人事、研究等校園場域中建立日常防詐安全習慣。

5

## 建立行為模式

養成「遇到詐騙→查驗→不匯款→通報」的標準化反應模式。



# 詐騙問題有多嚴重？

**3.8萬件**

**年度詐騙案件**  
根據警政署統計,  
每年詐騙案件數  
持續增加,造成重  
大社會問題。

**68.7億**

**年度財損金額**  
詐騙造成的財產  
損失金額驚人,平  
均每件損失金額  
持續攀升。

**165**

**反詐騙專線**  
警政署設立的24  
小時反詐騙諮詢  
專線,是民眾求助  
的第一道防線。





# 校園為何成為詐騙目標？

## 教職員工特殊風險因子

- **財務權限**:接觸研究經費、採購預算、學雜費等金流
- **個資豐富**:掌握學生與同事的個人資料
- **信任文化**:校園環境相對單純,警戒心較低
- **業務繁忙**:工作壓力大,容易疏於查證
- **科技使用**:頻繁使用網路與電子郵件溝通



# 警政署反詐騙資源介紹



## 打詐儀表板

警政署建置的即時詐騙資訊平台,提供最新詐騙手法統計、案例分析與防範建議。定期更新詐騙趨勢與高風險情境。



## 手法分析文件

詳細解析常見詐騙手法、話術腳本與因應之道,提供完整的防詐知識庫。



## 防詐宣導影片

警政署製作的多元宣導影片,以真實案例重現詐騙過程,幫助民眾了解詐騙話術與應對方式。



## 165全民防騙網

整合查詢平台,民眾可查詢可疑電話、網站、帳戶,並即時通報詐騙案件。

# 如何使用165反詐騙專線？

01

## 撥打165專線

24小時免費服務,可用市話或手機撥打,不需加區碼。

03

## 獲得專業諮詢

專業人員協助判斷是否為詐騙,並提供處理建議。

02

## 說明可疑情況

詳細描述收到的訊息、來電內容或可疑網站資訊。

04

## 完成通報紀錄

如確認為詐騙,可直接完成通報,協助警方追查。

❏ **重要提醒:**遇到可疑情況時,寧可多打一通165確認,也不要冒險匯款或提供個資!



## 第二章

# 常見詐騙手法解析

認識校園場域的詐騙型態

# 警政署統計:十大常見詐騙類型

1

## 假投資詐騙

透過社群媒體、通訊軟體推銷高報酬投資方案

2

## 假網路拍賣

假買家或假賣家進行交易詐騙

3

## 假冒公務機構

偽裝成警察、檢察官、法院等單位

4

## 解除分期付款

假冒客服稱訂單設定錯誤需操作ATM

5

## 假交友詐騙

透過交友軟體建立關係後借款或投資

6

## 假冒親友詐騙

盜用通訊軟體帳號假冒親友借錢

# 校園特有詐騙情境(一):假買家/假賣家

## 常見手法

教職員工在網路平台出售或購買教學設備、二手物品時,遇到假買家要求私下匯款,或假賣家收款後不出貨的情況。

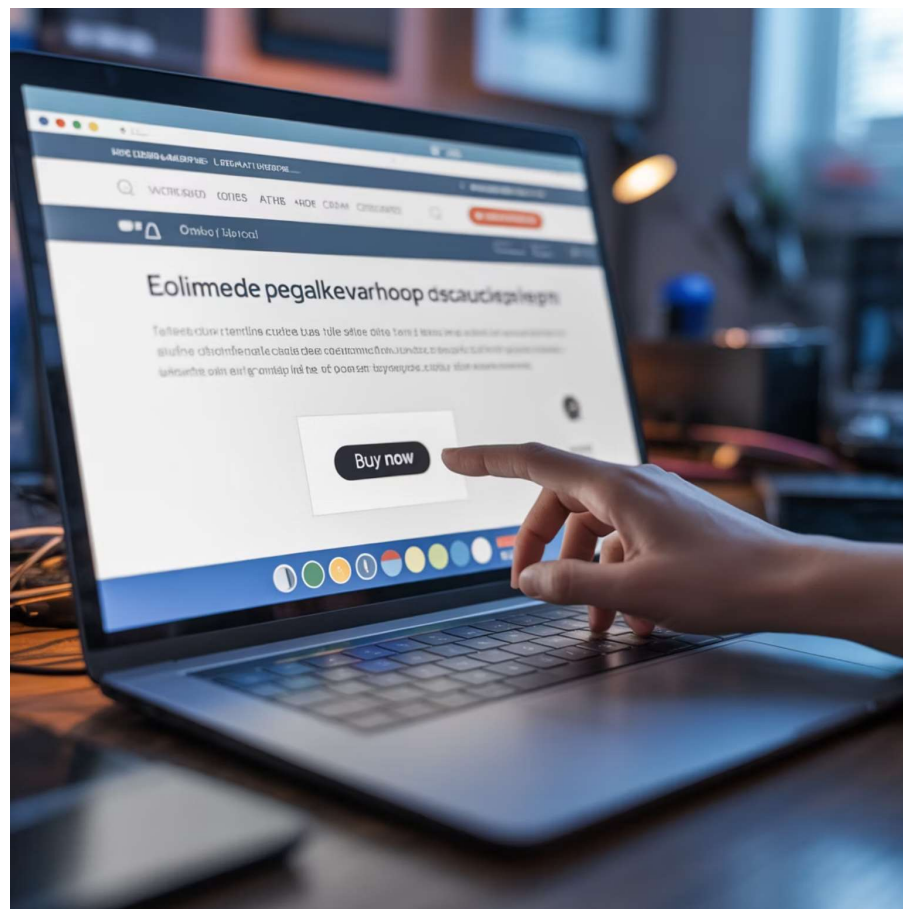
## 詐騙話術範例

「我想購買您的商品,但平台手續費太高,可以直接匯款給您嗎?我會多給您一些作為補償。」

「我已經匯款了,但銀行說您的帳戶有問題,需要您先操作ATM解除設定。」

### 防範要點

- 堅持使用平台交易機制
- 不接受私下匯款
- 不操作ATM解除任何設定
- 收到可疑訊息立即通報







## 校園特有詐騙情境(二):假投資詐騙

詐騙集團透過社群媒體、Line群組或簡訊,向教職員工推銷「穩賺不賠」的投資方案,聲稱有內線消息或獨家管道,承諾高額報酬。



### 接觸階段

透過Facebook、Instagram廣告或陌生訊息接觸



### 誘餌階段

展示假的獲利截圖,邀請加入投資群組觀摩



### 入金階段

要求匯款到指定帳戶或購買虛擬貨幣投資



### 收網階段

初期小額獲利後要求加碼,最終無法提領

# 校園特有詐騙情境(三):假公務通知

## 詐騙手法說明

詐騙集團假冒學校行政單位、教育部、警政署等公務機關,發送郵件或簡訊通知教職員工有未繳費用、違規罰款或需要更新資料。

## 常見偽裝身分

- 學校總務處或會計室
- 教育部或科技部
- 國稅局或健保署
- 警察局或檢察署
- 宿舍管理單位

## 典型話術

「您的健保費有異常扣款紀錄,請點選連結查看並立即處理,否則將暫停健保資格。」

「您的研究計畫補助款項需要重新驗證,請於三日內登入系統更新銀行帳戶資料。」



## 校園特有詐騙情境(四):假外包案與假補助



### 假外包案詐騙

詐騙集團偽裝成廠商,聲稱學校有採購或外包案件,要求教職員工協助處理並預付訂金或手續費。實際上並無此案件存在。



### 假補助通知

假冒科技部、教育部或基金會名義,通知教職員工獲得研究補助或獎助金,但需先支付審查費、保證金或手續費才能領取。

這類詐騙利用教職員工對研究經費與採購業務的熟悉度,製造看似合理的情境進行詐騙。務必透過正式管道查證所有涉及金錢的通知。



## 校園特有詐騙情境(五):人頭帳戶陷阱

詐騙集團以高薪兼職、協助轉帳等名義,誘騙教職員工或學生提供銀行帳戶、金融卡或證件,使其成為詐騙洗錢的人頭帳戶。

1

### 招攬階段

在網路或校園張貼高薪輕鬆的兼職訊息,如「協助收款」、「帳戶代管」等工作機會。

2

### 取信階段

以「公司業務需要」、「避稅節稅」等理由,要求提供帳戶資料或借用存摺、金融卡。

3

### 使用階段

將詐騙所得款項轉入該帳戶,再由人頭提領或轉出,完成洗錢程序。

4

### 法律後果

帳戶所有人可能被列為詐欺共犯或洗錢幫助犯,面臨刑事責任與帳戶凍結。

# 詐騙集團的共同特徵

## 營造急迫感

強調時間緊迫、限時優惠、立即處理,讓受害者沒有時間冷靜思考與查證。

## 要求保密

要求不要告訴他人、獨自處理,避免受害者尋求協助或向他人求證。

## 利用恐懼或貪婪

威脅法律後果、帳戶凍結,或誘以高報酬、中獎機會等利益。

## 要求匯款或提供帳戶

最終目的都是要求轉帳、提供帳戶資訊、購買遊戲點數或操作ATM。

## 仿冒專業身分

假冒警察、檢察官、銀行人員、客服等身分,製作假證件或假網站增加可信度。

## 使用非正式管道

透過Line、WhatsApp、私人電話等非正式管道聯繫,避開官方紀錄。



## 第三章

# 辨識詐騙技巧

從細節中發現可疑訊號





# 電話號碼辨識:警政署提示的可疑開頭

根據警政署與趨勢科技的分析,來電號碼的開頭可以透露重要訊息。以下是需要特別警戒的號碼類型:

## +886開頭

國際來電顯示為台灣區碼,但實際可能從境外撥打,常用於假冒公務機關。

## +86開頭

來自中國大陸的電話,詐騙集團常使用中國號碼進行詐騙。

## +0、+2開頭

異常的國際冠碼格式,明顯的詐騙電話標記。

## 不明+號開頭

任何不熟悉的國際冠碼來電都應提高警覺。

- ❑ **重要提醒:**正常的台灣電話號碼應顯示為09或02、03等區碼開頭,不會有+886格式的來電。如果看到+886開頭的來電,應立即提高警戒!

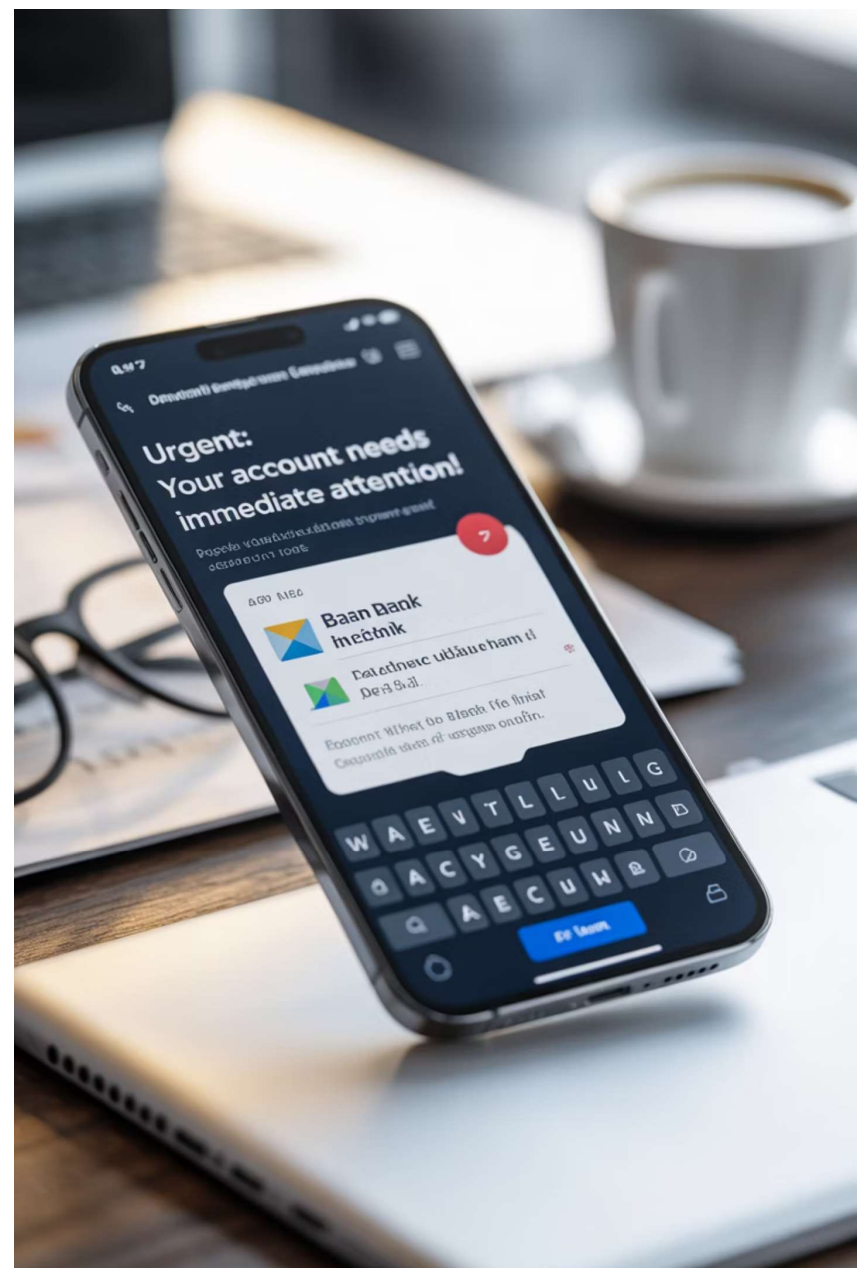
# 簡訊與郵件辨識技巧

## 可疑簡訊的特徵

- **短網址連結:**使用bit.ly等縮短網址隱藏真實網站
- **錯字或用詞不當:**官方訊息不會有明顯錯字
- **要求點選連結:**正式通知會要求主動登入官網查看
- **緊急語氣:**強調立即處理、帳戶將被停用等
- **陌生發送號碼:**非官方認證的發送號碼

## 可疑郵件的特徵

- **發件人網域異常:**非官方網域, 如gmail而非學校網域
- **附件或連結:**要求下載可疑附件或點選連結
- **要求提供個資:**詢問密碼、身分證號、帳戶資料
- **無個人化稱呼:**使用「用戶」而非您的姓名
- **威脅或利誘:**強調不處理的嚴重後果或誘人獎勵



# 網頁連結驗證方法

01

---

## 檢查網址完整性

查看完整網址,確認網域是否為官方網站,注意拼字與字母替換(如0替換O)。

03

---

## 避免點選簡訊連結

不直接點選簡訊或郵件中的連結,改為自行搜尋官網或使用書籤。

02

---

## 確認https與鎖頭圖示

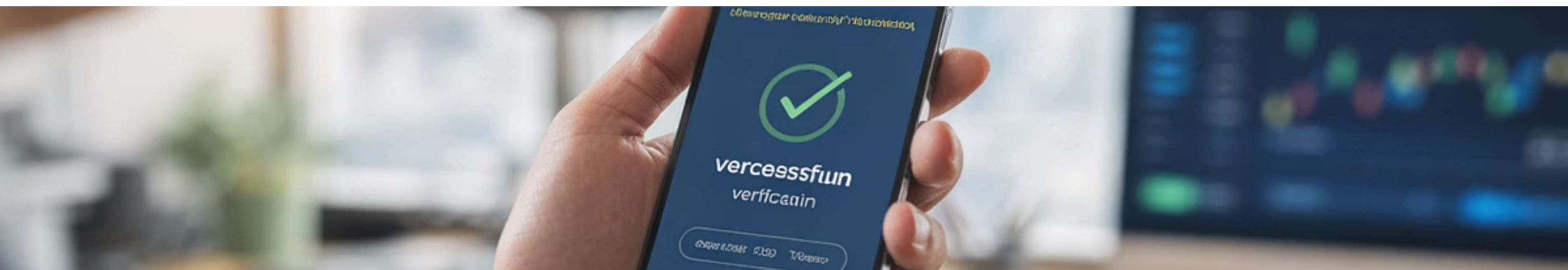
正式機構網站應有https加密連線與瀏覽器顯示的安全鎖頭。

04

---

## 使用165網站查詢

在165全民防騙網輸入可疑網址,查看是否已被通報為詐騙網站。



## 匯款前必做的查核步驟

### 1 確認收款對象身分

透過官方電話或親自聯繫,確認對方真實身分與款項用途,絕不透過對方提供的聯絡方式查證。

### 3 延後匯款時間

給自己充足的思考時間,任何要求立即匯款的情況都應該警戒。

### 2 查詢帳戶資訊

在165網站查詢收款帳戶是否為警示帳戶或已被通報的詐騙帳戶。

### 4 諮詢第三方意見

向家人、同事或165專線諮詢,多一個人的判斷就多一份保障。

# 銀行與公務機關聯繫查證方式

## 正確查證流程

1. 掛斷電話:先結束與對方的通話
2. 自行查找官方電話:透過官網、名片或帳單查詢
3. 主動撥打確認:使用查到的官方電話聯繫
4. 說明情況:描述收到的訊息或來電內容
5. 取得確認:由官方人員確認訊息真偽

### 絕對不要做的事

- 使用對方提供的電話回撥
- 在通話中直接轉接到「主管」或「警察」
- 相信對方提供的官網連結
- 在電話中提供個人資料或密碼
- 因為對方知道部分個資就完全信任



# ATM操作相關的詐騙話術破解

根據警政署統計,「解除分期付款設定」是最常見的詐騙話術之一。詐騙集團會假冒網購客服,聲稱訂單設定錯誤導致重複扣款,要求被害人到ATM操作「解除設定」。

## 真相一

**ATM沒有解除分期功能 -**  
ATM只能存款、提款、轉帳,絕對沒有任何「解除設定」的功能。

## 真相二

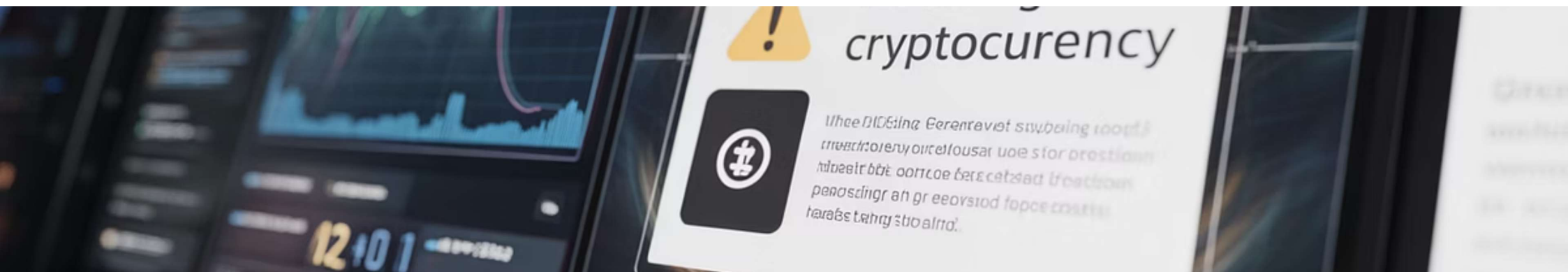
**所謂的「解除」就是轉帳 -** 詐騙集團要求的操作步驟,實際上就是將錢轉入詐騙帳戶。

## 真相三

**銀行不會電話要求ATM操作 -**  
任何要求到ATM操作的電話,100%都是詐騙。

**記住這句話:「要我去ATM操作任何事情的,都是詐騙!」**





# 遊戲點數與虛擬貨幣詐騙識別

詐騙集團近年常要求被害人購買遊戲點數或虛擬貨幣作為支付工具,因為這些管道難以追查且無法退款。

## 遊戲點數詐騙

要求購買Google Play、iTunes、Steam等遊戲點數卡,並提供卡片序號給對方。  
。聲稱這是「解除設定」、「繳納保證金」或「驗證身分」的方式。

## 虛擬貨幣詐騙

要求購買比特幣、以太幣等虛擬貨幣進行投資或交易。  
詐騙集團會提供假的交易平台,顯示獲利但無法提領。

## 辨識重點

任何正當的政府機關、銀行、公司行號,絕對不會要求以遊戲點數或虛擬貨幣支付款項。只要聽到這種要求,立即確認為詐騙。



## 第四章

# 防範原則與行為準則

建立個人防詐安全機制

# 防詐三大核心原則



## 一、冷靜查證

遇到任何涉及金錢、個資的要求,第一時間保持冷靜。不要被對方的急迫語氣影響,給自己時間透過官方管道查證。

- 掛斷電話,自行查找官方聯絡方式
- 使用165網站查詢可疑訊息
- 詢問同事或家人的意見
- 相信自己的直覺,覺得怪就停下來



## 二、絕不匯款

在完全確認對方身分與款項用途之前,絕對不要匯款、轉帳或提供任何金融資訊。

- 不提供銀行帳號、密碼、驗證碼
- 不購買遊戲點數或虛擬貨幣
- 不操作ATM的任何功能
- 不接受「代收代付」的要求



## 三、立即通報

發現可疑情況或不幸受騙,立即通報相關單位,既保護自己也保護他人。

- 撥打165反詐騙諮詢專線
- 向校內資安或總務單位通報
- 到警察局報案製作筆錄
- 通知銀行停止可疑交易

# 個人資訊保護守則

## 應該保護的個人資訊

- 身分證字號:不隨意提供或拍照上傳
- 銀行帳號與密碼:絕不透過電話或郵件告知
- 信用卡資訊:包括卡號、安全碼、有效期限
- 手機驗證碼:任何驗證碼都不應告訴他人
- 網路銀行密碼:定期更換且不與他人共用
- 個人照片與影片:避免被用於深偽詐騙

## 日常保護措施

- 社群媒體設定隱私權限
- 不在公開場合討論個人財務
- 定期檢查網路帳戶安全設定
- 使用強密碼並定期更換
- 啟用雙重驗證機制
- 謹慎加入陌生人的通訊群組



# 網路使用安全習慣



## 謹慎使用公共WiFi

避免在公共WiFi環境下進行網路銀行、購物等涉及金錢或個資的操作,駭客可能攔截資料。



## 警覺可疑郵件

不開啟來源不明的郵件附件,不點選可疑連結,收到異常郵件立即刪除並通報資訊單位。



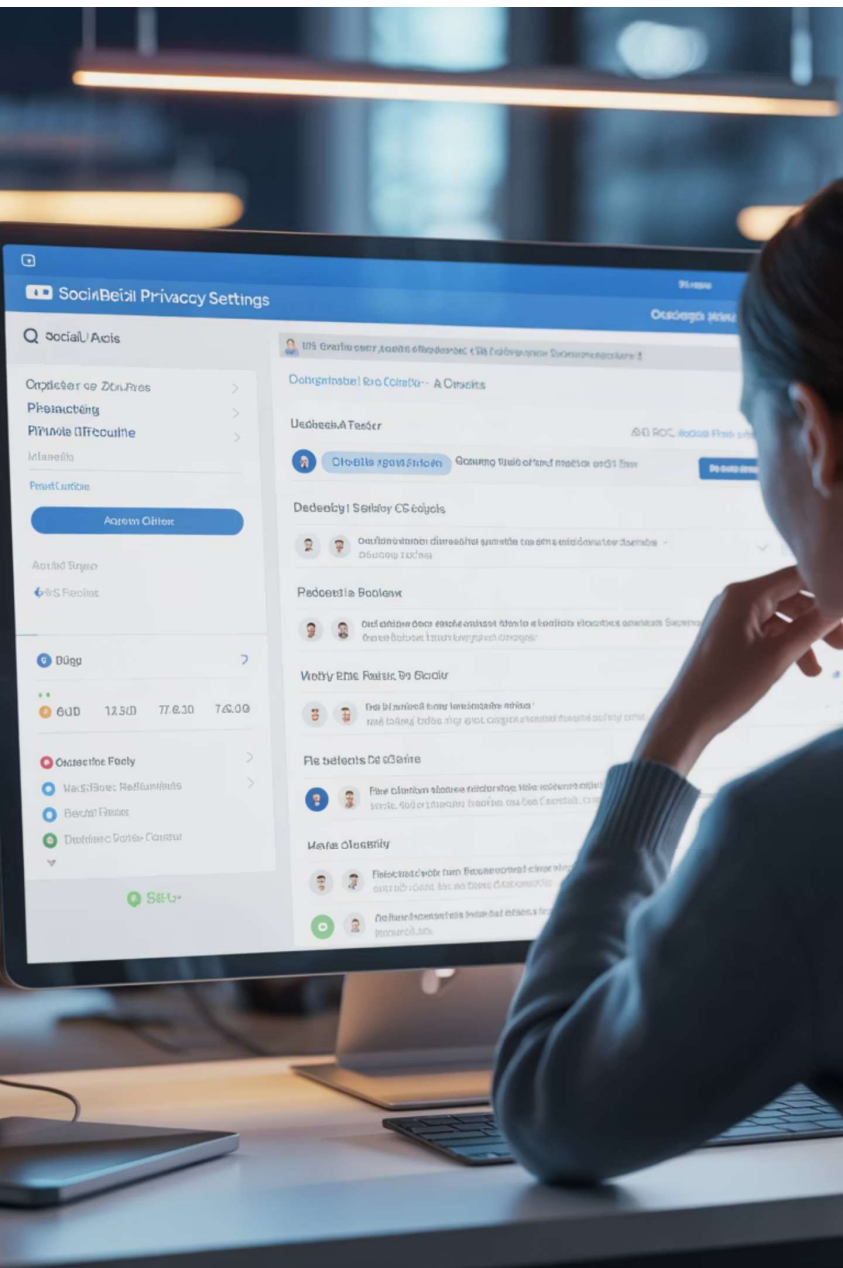
## 保持軟體更新

定期更新作業系統、防毒軟體與應用程式,修補已知的安全漏洞,降低被駭風險。



## 使用密碼管理

每個帳號使用不同的強密碼,避免一個帳號被盜導致連鎖反應,可使用密碼管理工具協助。



# 社群媒體安全注意事項

社群媒體已成為詐騙集團蒐集個資與接觸目標的重要管道。教職員工在使用Facebook、Instagram、Line等平台時,應特別注意以下事項:

## 檢查隱私設定

定期檢查社群平台的隱私設定,限制個人資訊的公開範圍,避免陌生人取得過多資訊。

## 謹慎接受好友邀請

不隨意接受陌生人的好友邀請,詐騙集團常建立假帳號進行詐騙或盜取資訊。

## 避免過度分享

不公開分享行程、住址、財務狀況等敏感資訊,這些都可能成為詐騙集團的工具。

## 警覺可疑訊息

即使是好友傳來的借錢或投資訊息,也應透過其他管道確認,可能是帳號被盜。



# 辦公場域防詐注意事項

## 財務作業安全

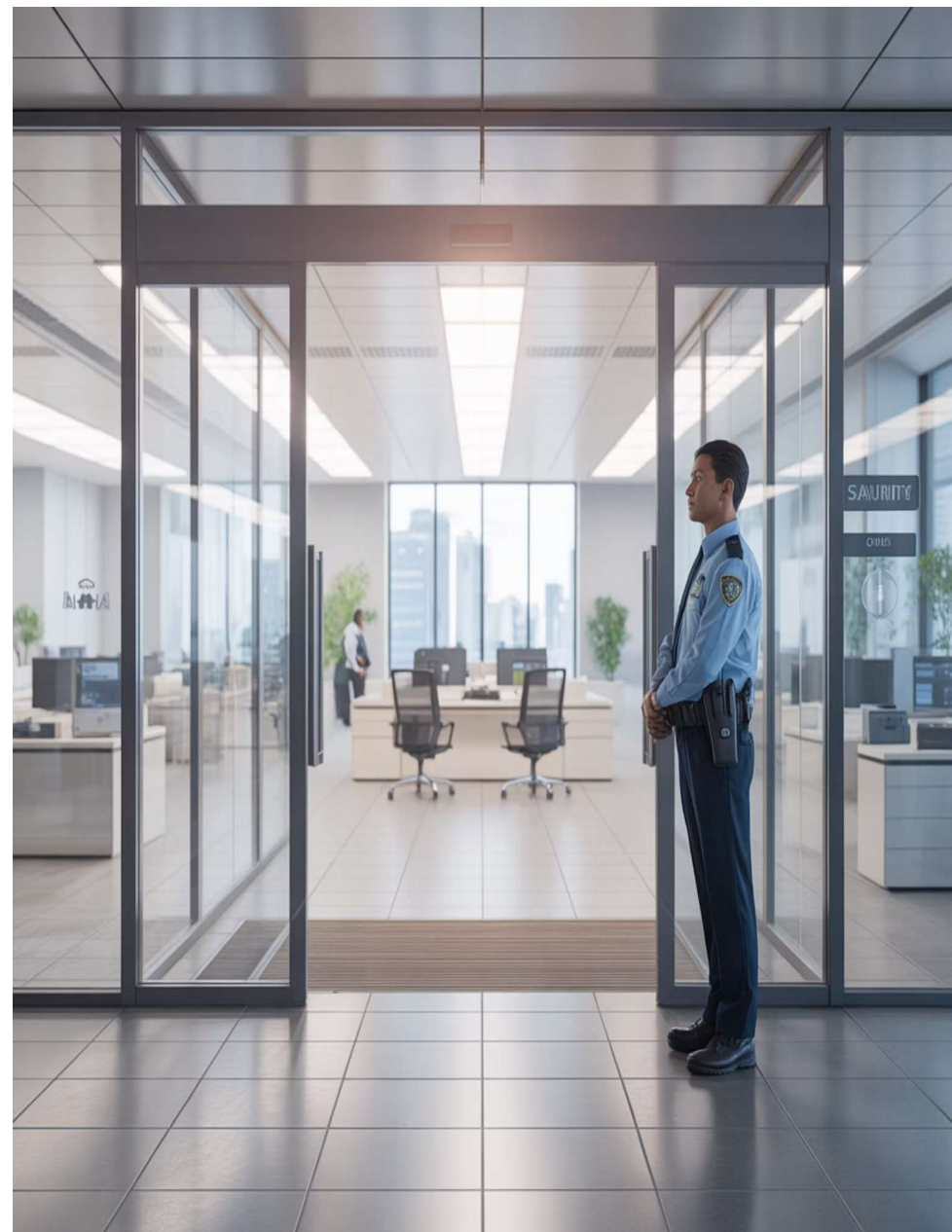
- 採購與報帳流程嚴格遵循校內規定
- 確認廠商資料並透過正式管道聯繫
- 大額款項需經主管覆核確認
- 可疑的匯款要求立即暫停並通報
- 保管好公務用印鑑與財務文件

## 研究經費管理

- 研究補助通知應透過官方平台確認
- 任何需要先付費的補助都是詐騙
- 經費動支嚴格按照計畫書執行
- 定期檢視帳戶交易紀錄

### ▣ 特別提醒

校園採購與財務作業涉及公款,更應謹慎小心。任何異常的款項要求都應該停下來查證,不要因為趕時間或怕麻煩而省略驗證步驟。





## 第五章

# 實務案例分析

從真實案例學習防詐技巧

# 案例一:假網購客服詐騙

## 案情描述

某大學行政人員在網路購買辦公用品後,接到自稱是購物平台客服的電話,表示訂單設定錯誤將重複扣款,需要至ATM操作解除設定。

## 詐騙手法分析

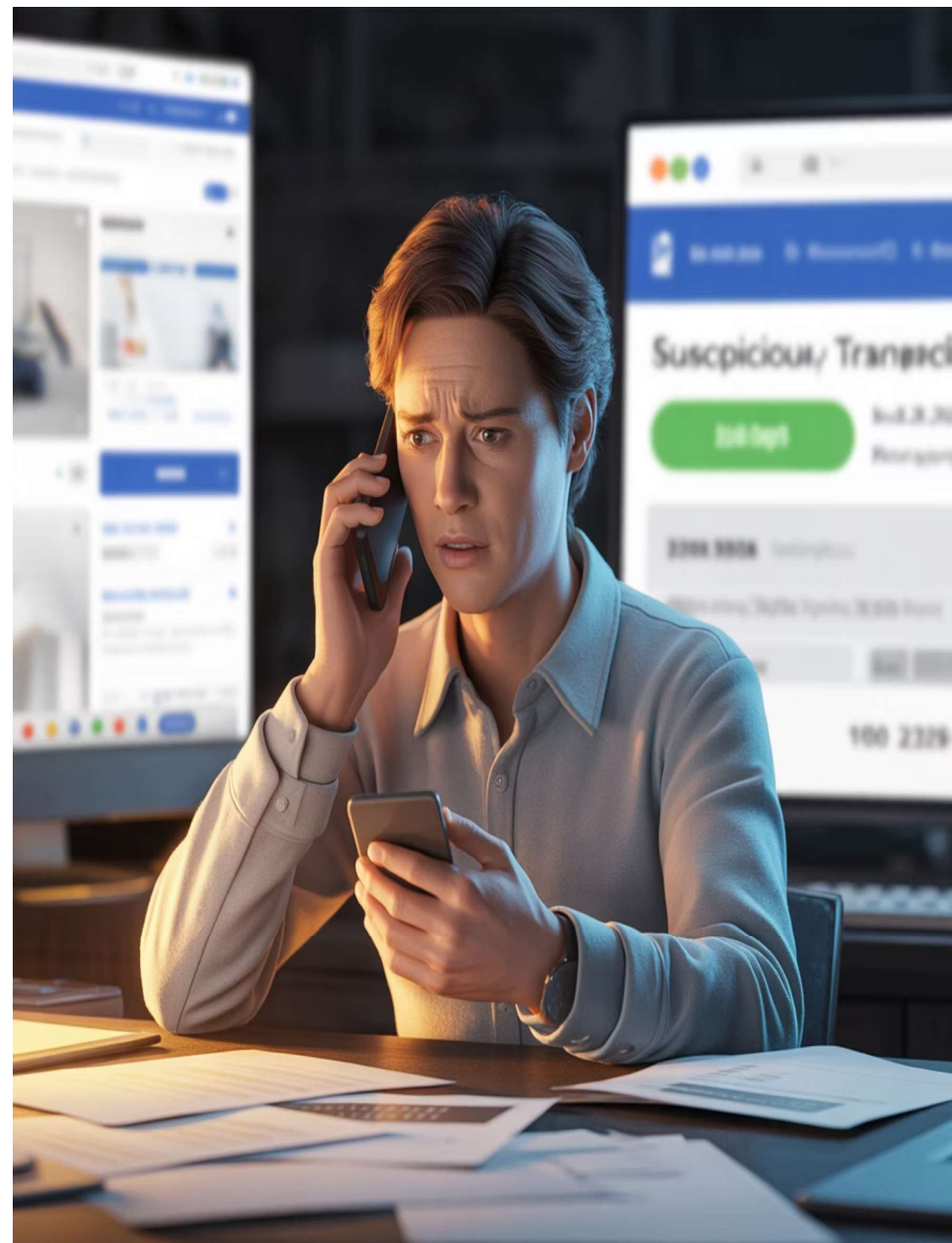
- 掌握真實購物資訊取信
- 製造緊急情況引發恐慌
- 使用專業術語增加可信度
- 要求到ATM操作(實為轉帳)
- 全程電話指導避免被發現

## 正確應對方式

1. 掛斷電話:不要在電話中繼續對話
2. 自行查找官方客服:從購物平台官網找客服電話
3. 主動聯繫確認:使用官方管道確認訂單狀況
4. 絕不到ATM操作:記住ATM沒有解除功能
5. 通報165專線:提供詐騙電話號碼協助預警

**關鍵學習:**任何要求到ATM操作的電話,100%是詐騙。

真正的客服會協助你在網站或app上處理問題,絕不會要求操作ATM。



## 案例二:假投資詐騙

某大學教師在Facebook看到投資廣告,加入Line群組後看到群組成員分享獲利截圖,在「投資顧問」的慫恿下投入研究經費20萬元,初期獲利後追加投資,最終無法提領,平台也消失。

**接觸階段**  
透過社群廣告或陌生訊息接觸,宣傳高報酬投資機會

**無法提領**  
以各種理由阻止提領,最終平台關閉消失



### 營造氛圍

邀請加入投資群組,展示假的獲利截圖與成功案例

### 小額測試

允許小額投資與提領建立信任,實為釣魚餌

### 慫恿加碼

宣稱限時優惠或重大機會,誘使追加投資

## 案例二:防範要點與反思

### 詐騙警訊

- 承諾穩賺不賠的高報酬
- 使用群組營造從眾壓力
- 獲利截圖可能是偽造的
- 投資平台未經金管會核准
- 要求匯款到個人帳戶

### 正確做法

- 投資前查證平台是否合法
- 不相信過高的報酬承諾
- 不因他人獲利而盲目跟進
- 諮詢專業理財顧問意見
- 使用正規金融機構投資

❏ **重要觀念:**投資一定有風險,任何承諾「穩賺不賠」、「保證獲利」的都是詐騙。合法的投資平台可以在金管會網站查詢,陌生人推薦的投資機會應該要非常謹慎。



# 案例三:假冒公務機關詐騙

## 案情描述

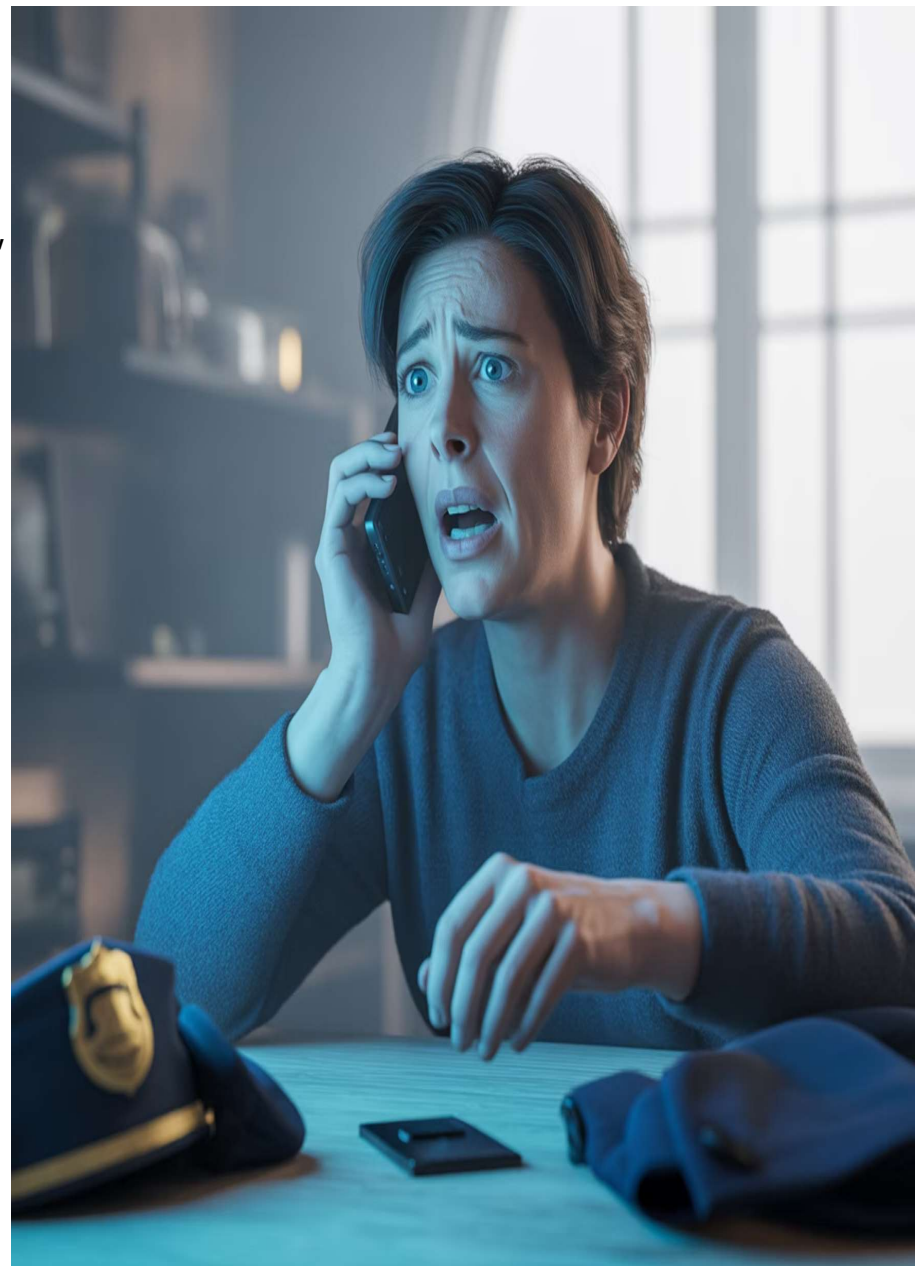
某研究助理接到自稱「刑事局」的電話,表示其身分證被冒用申請人頭帳戶,涉及洗錢案件需要配合調查,並要求加Line提供證件照片與帳戶資訊以證明清白。

## 詐騙手法

- 假冒執法機關製造恐懼
- 使用法律術語增加威嚇感
- 要求保密不能告訴他人
- 轉到通訊軟體持續控制
- 索取個資與帳戶資訊
- 可能要求監管帳戶(實為詐騙)

## 破解關鍵 警察、檢察官絕對不會:

- 透過電話辦案或調查
- 要求加Line或其他通訊軟體
- 要求提供帳戶密碼
- 要求匯款到指定帳戶
- 要求到超商操作任何事情
- 禁止當事人告訴他人





# 案例三:正確應對流程

## 保持冷靜

不要被對方的威嚇語氣嚇到,記住警察不會這樣辦案。

## 記錄資訊

記下對方自稱的姓名、單位、電話,但不要相信。

## 掛斷電話

禮貌地表示需要確認身分,掛斷電話不要繼續對話。

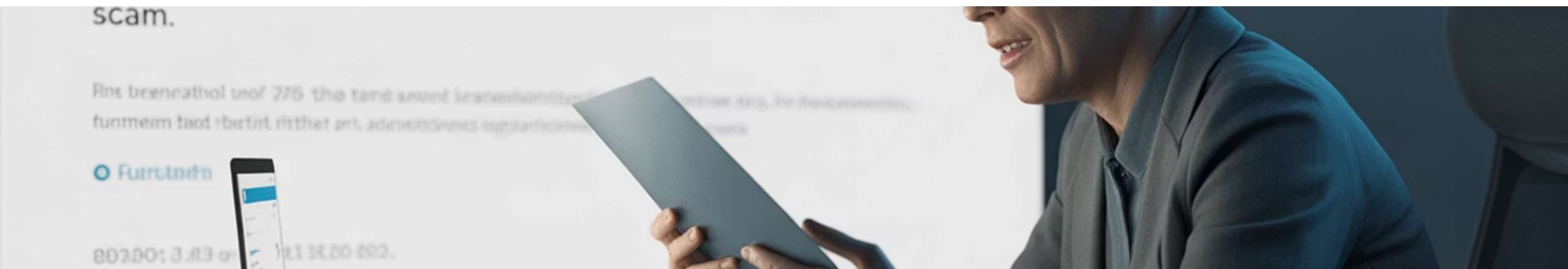
## 撥打165查證

打165說明情況,確認是否為詐騙,並通報對方電話。

## 通報單位主管

告知單位主管遇到的情況,避免公務資訊外洩疑慮。

**記住:**真正的警察會請你到警局製作筆錄,不會在電話中調查。如果對方堅持不能掛電話或到警局,就是詐騙!



## 案例四:假研究補助通知

某教授收到電子郵件,通知獲得科技部專題研究計畫補助,但需先支付「審查費」與「保證金」才能撥款,郵件看起來很正式,還附上假的公文與匯款帳戶。

### 詐騙特徵

- 發件人網域非官方網域 (@gmail.com等)
- 要求先付費才能領取補助
- 匯款帳戶為個人帳戶非公庫
- 強調時效性要求盡快處理
- 公文格式與文字有瑕疵

### 查證方式

- 登入科技部計畫申請系統查詢
- 撥打科技部官方電話確認
- 詢問學校研發處承辦人
- 確認是否有提出該計畫申請
- 檢查郵件發送網域與格式

### 正確認知

- 正式補助不需要先付費
- 補助通知會透過正式系統
- 款項會直接撥入學校帳戶
- 公文會有正式文號與印信
- 學校研發處會協助處理

# 案例五:假買家詐騙教職員

## 案情經過

某職員在二手交易平台出售閒置的辦公家具,買家表示想購買並願意多付運費,但要求賣家先到超商繳費「驗證帳戶」後才能匯款。職員依指示操作後,發現自己購買了數千元的遊戲點數,點數序號已被買家取得。

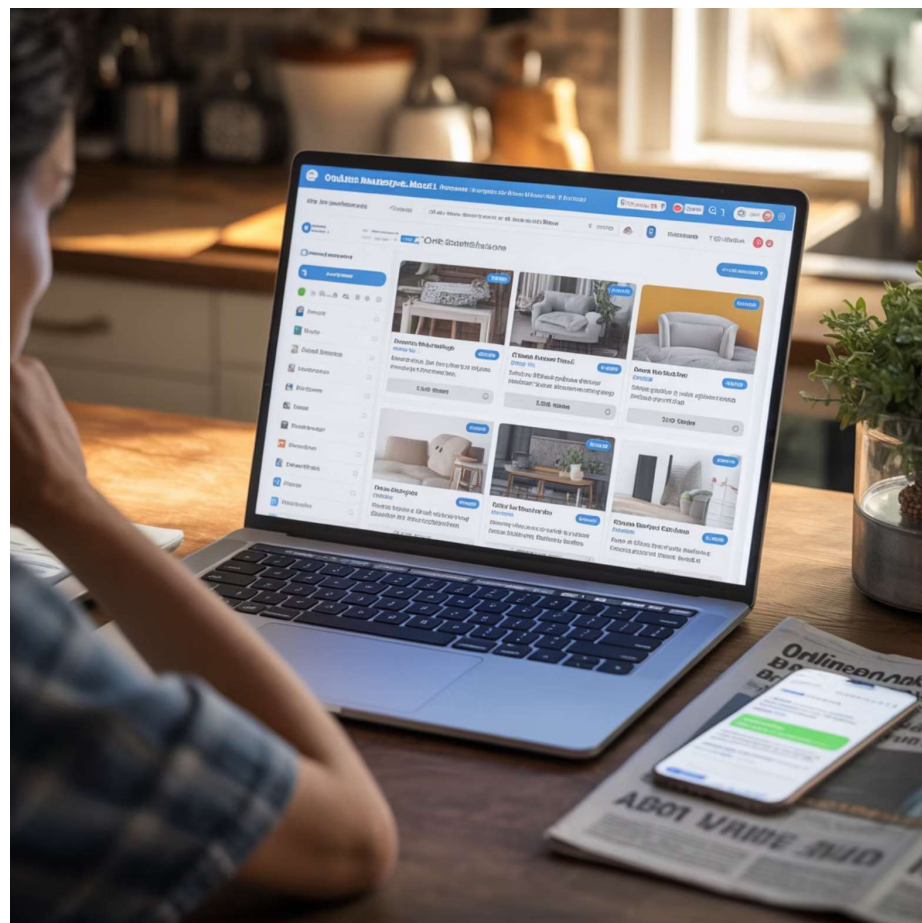
## 詐騙流程

1. 在拍賣平台找到交易目標
2. 假扮買家表達購買意願
3. 提出特殊付款方式要求
4. 誘導到超商操作繳費機
5. 實際是購買遊戲點數
6. 取得點數序號後消失

## 防範重點

- 堅持使用平台交易機制
- 不接受任何特殊付款方式
- 不到超商操作任何繳費
- 不提供遊戲點數序號
- 可疑對話立即封鎖通報

▣ 正常買家不會要求賣家去超商操作任何事情。一旦提到超商繳費或驗證,就是詐騙!





## 案例六:人頭帳戶陷阱

某兼任助理在求職網站看到「帳戶代管員」徵人廣告,工作內容是讓雇主使用銀行帳戶收款,每月可領取5,000元報酬。提供帳戶後,帳戶被用於詐騙洗錢,助理被警方約談並面臨法律責任。

### 警訊一

任何要求提供帳戶、存摺、金融卡的工作都是陷阱



### 警訊二

過於優渥的報酬且工作內容簡單不合理

### 警訊三

提供帳戶會觸犯洗錢防制法,面臨刑責

**法律後果:**提供帳戶可能被認定為幫助詐欺或洗錢罪,面臨刑事責任、帳戶被凍結、信用受損,甚至影響未來就業。絕對不要因為貪圖小利而提供帳戶!

# 防詐騙核心要點回顧

## 冷靜思考

不被急迫感影響,給自己時間查證與思考,詐騙集團最怕你冷靜。

## 即時通報

發現可疑立即通報,不論是否受騙都要協助警方預防。

## 分享經驗

將防詐知識分享給同事、學生,共同建立防護網絡。



## 多重查證

透過官方管道確認訊息真偽,使用165網站與專線協助判斷。

## 保護資訊

不隨意提供個資、帳戶、密碼,這些是詐騙的目標與工具。

## 謹慎匯款

匯款前再三確認,記住ATM沒有解除功能,不購買遊戲點數。



# 個人資料保護教育訓練

大專院校教職員工個資保護實務應用課程





# 課程目標與學習成果



## 法規認知

深入理解個人資料保護法的核心概念、法律義務與罰則規定,建立完整的法律框架認知



## 風險防範

識別校園環境中常見的個資風險情境,學習有效的預防措施與應對策略



## 實務操作

掌握個資蒐集、處理、利用、保存及刪除的標準作業程序與正確方法



## 制度遵循

熟悉校內個資管理制度、作業流程及事件通報機制,確保日常作業合規

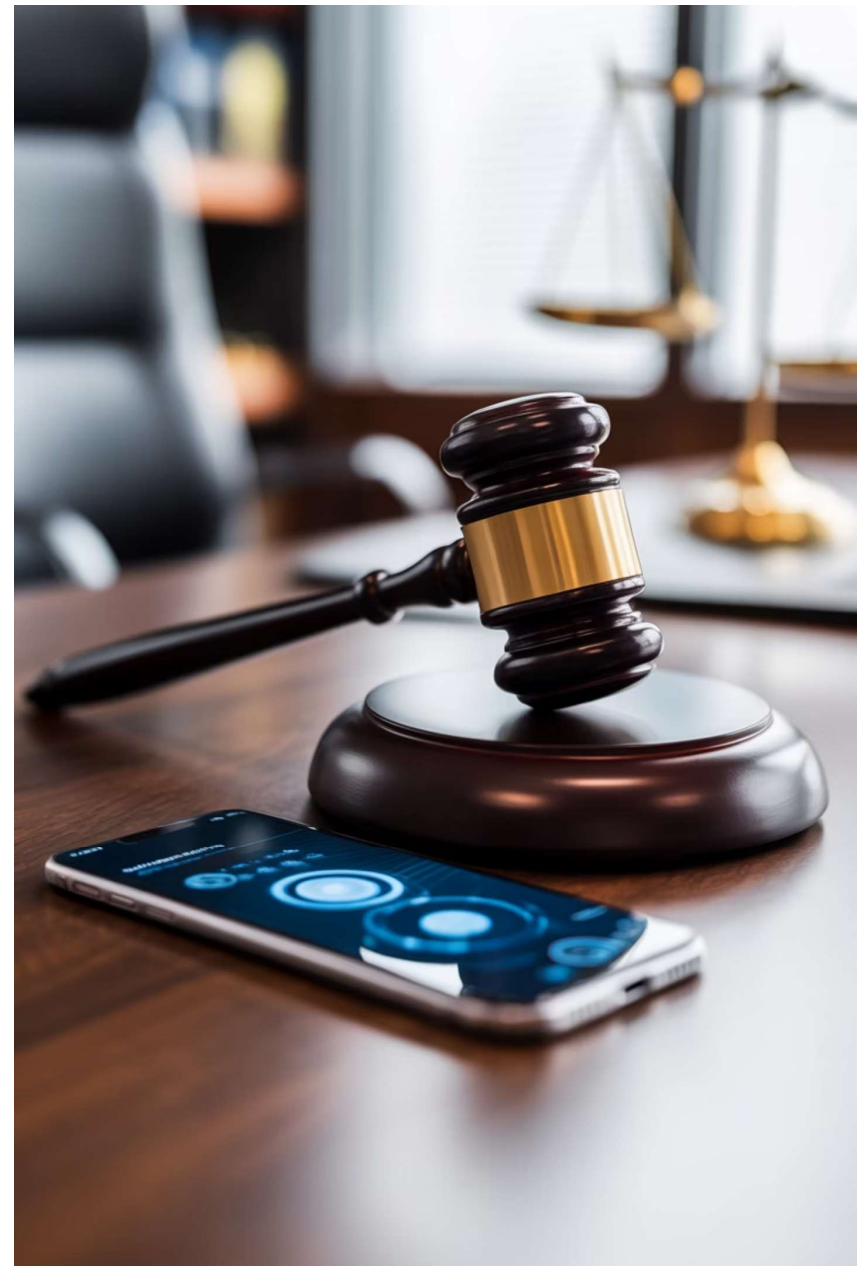
**為什麼個人資料  
保護如此重要？**



# 第一單元

## 個人資料保護法概要

認識法律框架與核心規範



# 個資保護的時代背景

## 數位化浪潮

校園全面數位化轉型,從招生、教學、行政到研究,大量個人資料以電子形式蒐集與儲存。雲端服務、行動應用與大數據分析的普及,使個資應用範圍大幅擴增。

## 資安威脅升級

駭客攻擊、勒索軟體、釣魚郵件等網路威脅日益嚴峻。校園往往成為攻擊目標,因其擁有大量師生個資且防護機制相對薄弱。

## 法規要求嚴格

個人資料保護法施行後,對公務機關與學校的個資管理提出明確規範。違法處理個資將面臨高額罰鍰與民事求償,甚至刑事責任。

## 權益意識提升

社會大眾對隱私權與個資自主權的重視程度不斷提高。學生與家長更加關注個資如何被使用,要求透明與安全保障。

# 什麼是「個人資料」？

根據個人資料保護法第2條, **個人資料**係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

## 關鍵要素

- **直接識別**:如姓名、身分證號
- **間接識別**:透過對照、組合可識別特定個人
- **範圍廣泛**:包含各種生活面向的資訊



# 個人資料保護法核心概念



## 法律定義

個人資料：指自然人之姓名、出生年月日、身分證字號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。



## 保護原則

合法性、正當性、必要性、比例性、當事人權益保障等五大核心原則，貫穿個資之蒐集、處理與利用全程。



## 法律責任

違反個資法可能面臨刑事責任（最高五年有期徒刑）、民事賠償（每人損害賠償最高二萬元）以及行政罰鍰。



# 教育部相關函釋重點

## 成績資料處理

學生成績屬個人資料，公開揭示需注意方式，建議採學號部分遮蔽或個別通知方式，避免整體公告。

## 監視錄影管理

校園監視錄影涉及個資蒐集，應明確告知、限定目的使用，並注意保存期限與調閱權限管理。

## 雲端服務使用

委託雲端服務廠商處理個資時，需簽訂書面契約，明定保護義務，並定期監督其執行狀況。

## 第三方資料分享

與外部單位分享學生資料需有法律依據或當事人同意，並採最小必要原則，僅提供必要欄位。



## 第二單元

### 校園常見個資風險與案例

# 校園個資風險地圖

## 學生資料

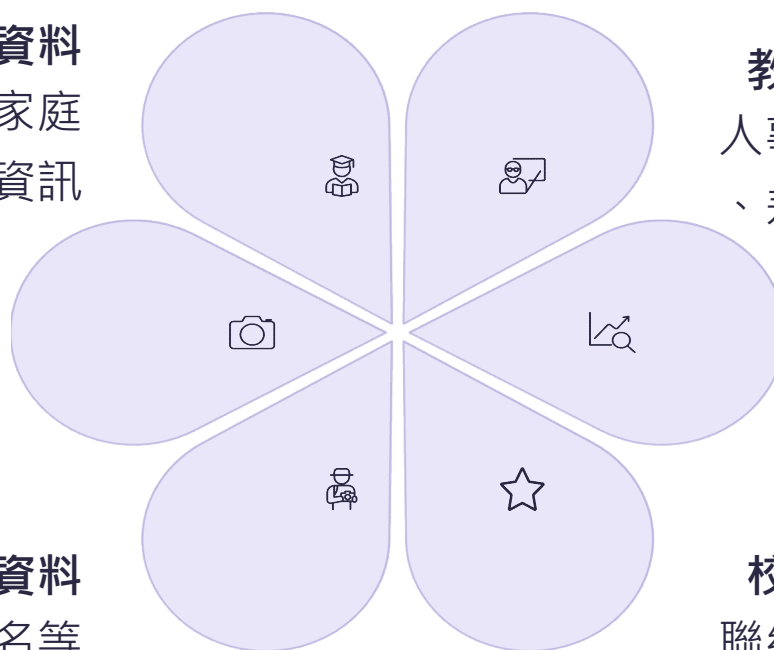
成績、缺曠課、獎懲、健康、家庭  
背景、財務狀況等敏感資訊

## 影像資料

監視錄影、活動照片、視訊會  
議紀錄等

## 訪客資料

門禁登記、會議簽到、活動報名等



## 教職員資料

人事檔案、薪資、考核、健康檢查  
、差勤紀錄等

## 研究資料

人體試驗、問卷調查、訪談紀  
錄等研究參與者資料

## 校友資料

聯絡資訊、捐款紀錄、就業狀況等



# 學生成績與缺曠資料的敏感度分析



## 成績資料

**敏感度等級：**高敏感

**洩漏風險：**影響學生名譽、升學機會、心理壓力，可能導致霸凌或歧視

**處理建議：**僅限授課教師、導師與學生本人查閱，嚴格控管存取權限



## 缺曠資料

**敏感度等級：**高敏感

**洩漏風險：**可推知學生行為模式、紀律狀況，涉及家庭教育品質評價

**處理建議：**僅限導師與家長（未成年學生）查閱，成年學生須經同意



## 輔導紀錄

**敏感度等級：**極高敏感

**洩漏風險：**涉及心理狀態、家庭狀況、人際關係等最私密資訊

**處理建議：**實施最嚴格權限控管，僅限輔導教師與經授權人員存取

教育機構應建立分級管理機制，依據資料敏感度等級制定不同的存取控制、加密傳輸及保存年限規範，確保學生個人資料獲得適當保護。

# 個資寄送對象與原則



## 未成年學生家長

家長為法定代理人，基於教育目的與監護權行使，學校可主動寄送成績與缺曠資料給家長。但仍需注意資料最小化原則，僅提供必要資訊。



## 成年學生（滿18歲）

學生已具完全行為能力，成績與缺曠資料屬其個人隱私。學校若需寄送給家長或第三方，必須事先取得學生本人的明確書面同意。



## 電子寄送注意事項

- 嚴禁使用群發功能，應個別寄送或透過加密系統通知
- 寄件信箱須經過身分驗證，確認收件者身分
- 信件內容應遵循最小化原則，避免包含不必要的個人資料欄位
- 附件檔案應加密處理，並以密碼保護

# 案例一：成績公告不當



## 事件描述

某系所將學期成績以完整學號及姓名方式張貼於公佈欄，並拍照上傳至社群媒體，引發學生家長投訴。

## 問題分析

- 未注意個資保護，完整揭露可識別資訊
- 擴大揭露範圍至網路，增加風險
- 未評估是否有其他替代方案

## 正確做法

- 採學號部分遮蔽（如末三碼）方式公告
- 或改採個別通知、線上查詢等方式
- 絕不將含個資之成績單上傳社群媒體



# 案例二:成年學生缺曠資料寄送爭議

## 事件背景

學務處依慣例每月寄送缺課通知表給全體學生家長,未區分學生是否已成年。

## 法律分析

成年學生已具完全行為能力,其個人資料應由本人決定是否揭露給家長,學校未經同意寄送違反個資法。

1

2

3

4

## 爭議發生

一位已滿20歲的大學生發現學校持續將其出缺勤紀錄寄送給家長,認為侵害其隱私權,向學校提出抗議。

## 改善方案

建立同意機制,於入學時取得成年學生的家長通知同意書,系統自動判斷學生年齡決定是否發送。

## 未成年學生處理原則

家長為法定代理人,基於教育指導目的,學校可主動寄送缺曠通知。但仍需注意資料保護,避免過度揭露學生個人生活細節。

## 成年學生處理原則

應在入學時或學生成年時,明確告知個資處理政策,並取得學生本人的書面同意,才可繼續寄送相關通知給家長。系統應自動辨識學生年齡狀態,啟動不同的通知機制。

## 案例三：雲端服務委外風險

某學院為便利教學，自行採用免費雲端平台儲存學生作業及成績，未經資訊單位審查，亦未簽訂個資保護契約。

### 法律風險

委外處理個資需簽訂書面契約，明定受託者保護義務，否則委託者仍需負法律責任。

### 技術風險

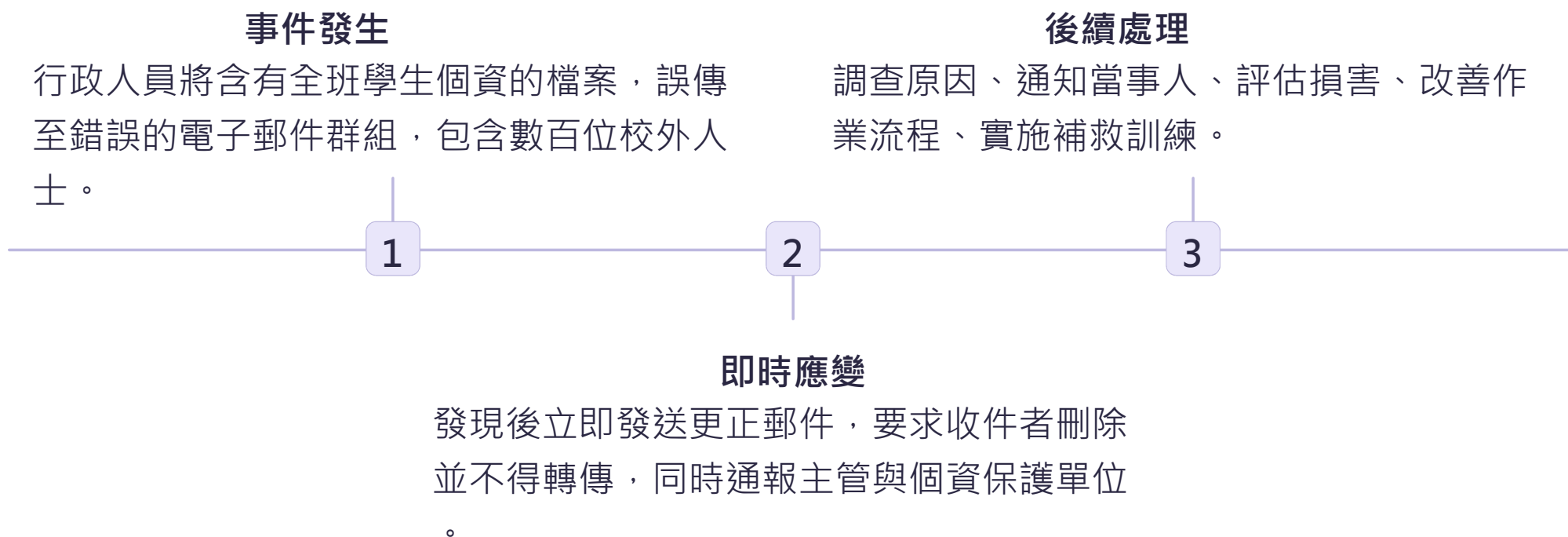
免費雲端服務可能缺乏足夠安全措施，資料可能流向境外，增加外洩風險。

### 管理風險

未經統一管理的雲端服務，學校無法掌握個資處理狀況，難以監督與稽核。



## 案例四：電子郵件誤傳



這類事件顯示人為疏失是個資外洩的主要原因之一，需透過教育訓練與作業程序雙管齊下預防。



# 近期校園資安事件趨勢

## 資料外洩事件頻傳

多所大學因系統漏洞、人為疏失或駭客攻擊導致學生個資外洩,影響數千至數萬人

## 雲端服務風險

教職員不當使用公開雲端資料夾分享敏感資料,或誤設存取權限造成資料曝光

## 委外廠商管理不善

外包廠商未遵守個資保護規定,擅自利用或洩露所蒐集的個資,學校負連帶責任

## 社交工程攻擊

透過釣魚郵件騙取帳號密碼,進而存取校務系統竊取大量個人資料

# 個資外洩的嚴重後果

**500萬**

**最高罰鍰**

違反個資法可處最高新  
台幣500萬元罰鍰

**2億**

**民事賠償**

每人每事件最高2萬元,  
集體訴訟金額可能達億  
元

**5年**

**刑事責任**

意圖營利違法利用個資  
,最重可處5年有期徒刑

**∞**

**聲譽損失**

學校形象受損、招生困  
難、社會信任度下降,  
影響深遠

# 校園常見個人資料類型



## 學生資料

姓名、學號、身分證號、出生年月日、聯絡電話、地址、家長資料、成績、缺曠紀錄、獎懲紀錄、社團參與、獎學金申請資料



## 研究資料

研究參與者個資、問卷調查資料、實驗數據、訪談紀錄、影音資料



## 系統資料

帳號密碼、登入紀錄、IP位址、電子郵件內容、雲端儲存檔案



## 教職員資料

人事基本資料、薪資、考績、研究計畫、授課資訊、帳號密碼、職員證號碼、銀行帳戶資訊



## 監視影像

校園監視器錄影、門禁刷卡紀錄、車輛進出紀錄、會議錄影



## 健康資料

健康檢查紀錄、體育課體適能測驗、身心障礙證明、傳染病通報資料





# 敏感性個人資料

個資法第6條規定,特定類別的個人資料因涉及隱私敏感性較高,原則上**禁止蒐集、處理或利用**,除非符合法定例外

## 醫療與健康

病歷、醫療、基因、性生活、健康檢查及犯罪前科

## 特殊身分

種族、政治觀點、宗教信仰、工會會籍

- ❑ **校園實例:**學生身心障礙證明、健康檢查紀錄、輔導諮商紀錄等均屬敏感資料,須特別謹慎處理並取得當事人明確同意。

# 個資法的核心原則

01

---

## 目的明確性原則

蒐集個資應有特定目的,不得逾越必要範圍

03

---

## 告知義務

蒐集個資時應明確告知當事人蒐集目的、類別、利用方式等事項

05

---

## 安全維護義務

應採取適當安全措施防止個資被竊取、竄改、毀損、滅失或洩漏

02

---

## 比例原則

蒐集之個資應與目的具關聯性,且為達成目的之最小必要範圍

04

---

## 當事人權利保障

當事人有權查詢、請求閱覽、製給複製本、補充或更正、停止蒐集處理利用及刪除

06

---

## 委外監督義務

委託他人處理個資時,應對受託者為適當監督

# 個資法第8條:告知義務

向當事人蒐集個人資料時,應明確告知下列事項:

1. 公務機關或非公務機關名稱
2. 蒐集之目的
3. 個人資料之類別
4. 個人資料利用之期間、地區、對象及方式
5. 當事人依第3條規定得行使之權利及方式
6. 當事人得自由選擇提供個人資料時,不提供將對其權益之影響

## 告知方式

可採書面、電子文件、簡訊、電話、網頁公告或其他足以使當事人知悉或可得知悉之方式為之。

❑ **重要提醒:**未依法告知或告知不完整,即屬違法蒐集,可能面臨行政處罰。



# 當事人的七大權利

1

## 查詢或請求閱覽

得向公務機關查詢或請求閱覽其個人資料

2

## 請求製給複製本

得請求製給個人資料之複製本,機關得酌收必要成本費用

3

## 請求補充或更正

認為個資有錯誤或不完整者,得請求補充或更正

4

## 請求停止蒐集處理利

個資蒐集之特定目的消失或期限屆滿,得請求停止蒐集、處理或利用

5

## 請求刪除

違法蒐集、處理或利用者,得請求刪除

6

## 拒絕直接行銷

得隨時向公務機關請求停止利用其個資行銷

7

## 救濟權

認為權利受侵害時,得向主管機關申訴或提起訴訟



# 機關的法定義務



## 建立個資檔案

應定期或依當事人請求,提供個人資料檔案清冊



## 維護資料安全

採行適當安全措施,防止個資外洩、竄改或毀損



## 事故通知義務

發生個資外洩事故時,應儘速通知當事人及主管機關



## 接受稽核

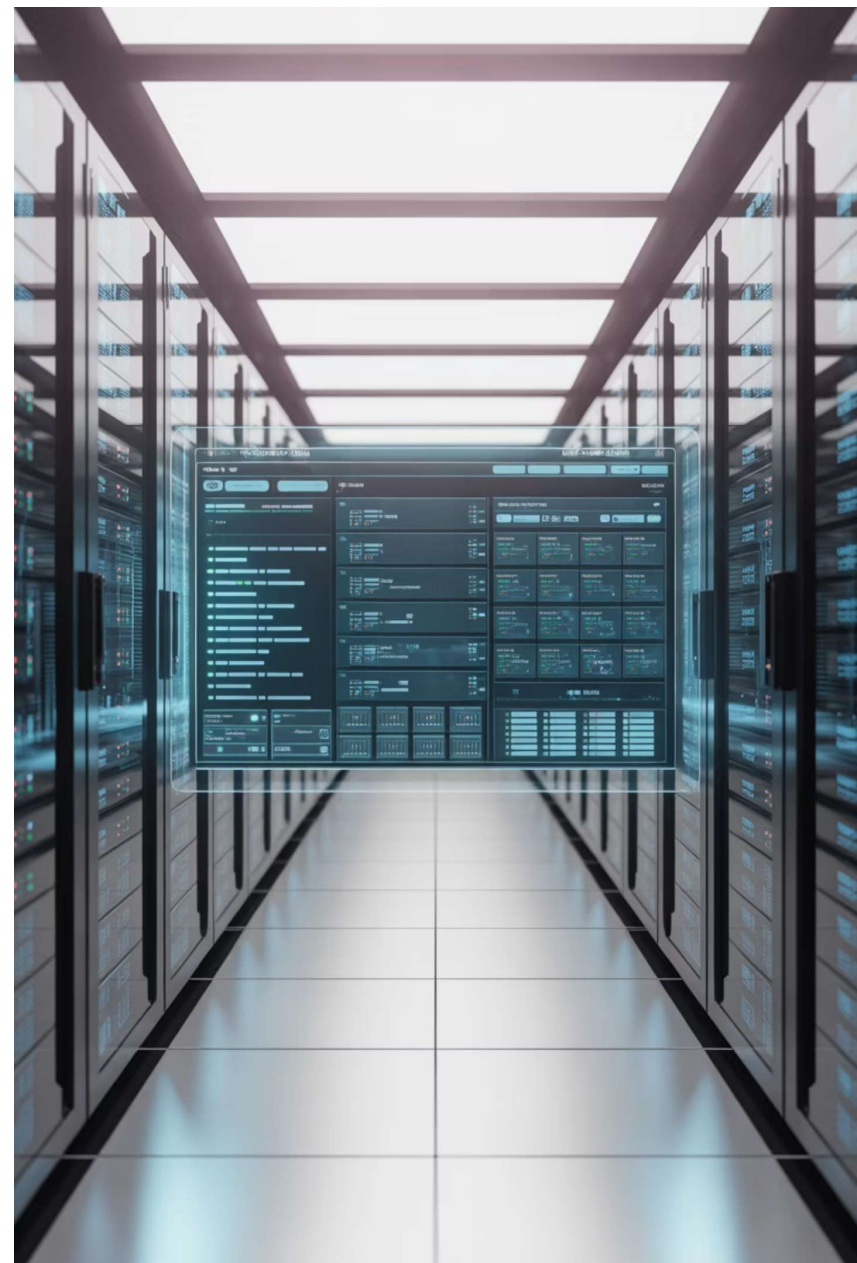
配合主管機關之檢查及資料提供要求



# 第二單元

## 校園個資蒐集與利用實務

從日常作業看個資保護要點





# 個資處理生命週期

**蒐集**  
確認目的、告知當事人、取得同意

**刪除/銷毀**  
目的消失或期限屆滿即銷毀



**處理**  
建檔、分類、整理、儲存

**利用**  
在特定目的範圍內使用

**保存**  
安全控管、定期檢視

每個階段都必須遵守個資法規定,確保個資安全與合法使用。

# 蒐集階段:核心要點

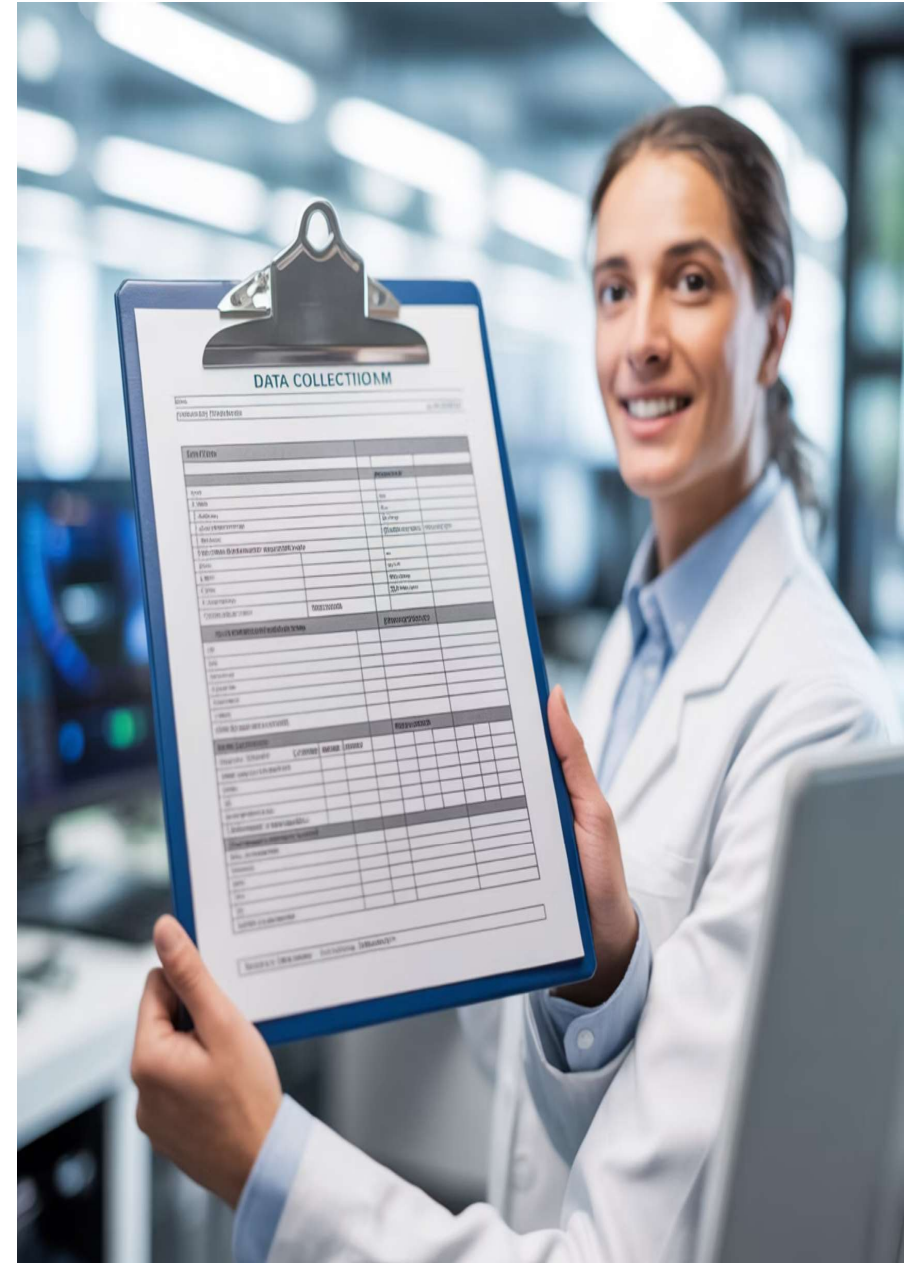
## 蒐集前自我檢視

- 目的明確? 蒐集目的是否具體清楚
- 是否必要? 該個資是否為達成目的所必需
- 有無法源? 蒐集依據是否合法
- 範圍適當? 是否僅蒐集最小必要範圍
- 是否告知? 已否依法告知當事人

## 取得同意的方式

可採書面、電子表單、勾選同意欄位、口頭錄音等方式,但**應保留紀錄**以備查證。

❏ **敏感資料特別注意:**蒐集敏感性個資原則上禁止,須有法律明確規定或當事人自行公開或已合法公開,且目的為增進公共利益。



# 教師常見的個資蒐集情境

## 課程點名與成績

蒐集學生姓名、學號、出席、成績等資料。應於課程開始時告知學生成績評定方式及個資利用範圍。

## 活動照片與影片

拍攝課程活動、校外參訪照片。應事先告知並取得同意,避免未經同意公開於網路或社群媒體。

## 研究計畫資料蒐集

進行問卷調查、訪談或實驗。須通過研究倫理審查,明確告知研究目的並取得書面同意,保障參與者匿名性。

## 線上教學平台

使用線上會議、數位學習平台蒐集學生帳號、學習歷程。應選擇符合個資保護規範的平台並妥善管理權限。

# 行政人員常見的個資蒐集情境

1

## 招生作業

蒐集考生基本資料、成績、審查資料。應於招生簡章明確告知個資蒐集目的、利用方式及保存期限。

2

## 獎助學金申請

蒐集家庭經濟狀況、成績等資料。應告知審查目的及資料提供對象,並注意敏感資料保護。

3

## 學生輔導紀錄

諮商輔導、身心障礙服務紀錄。屬高度敏感資料,應嚴格管控存取權限,僅限相關輔導人員查閱。

4

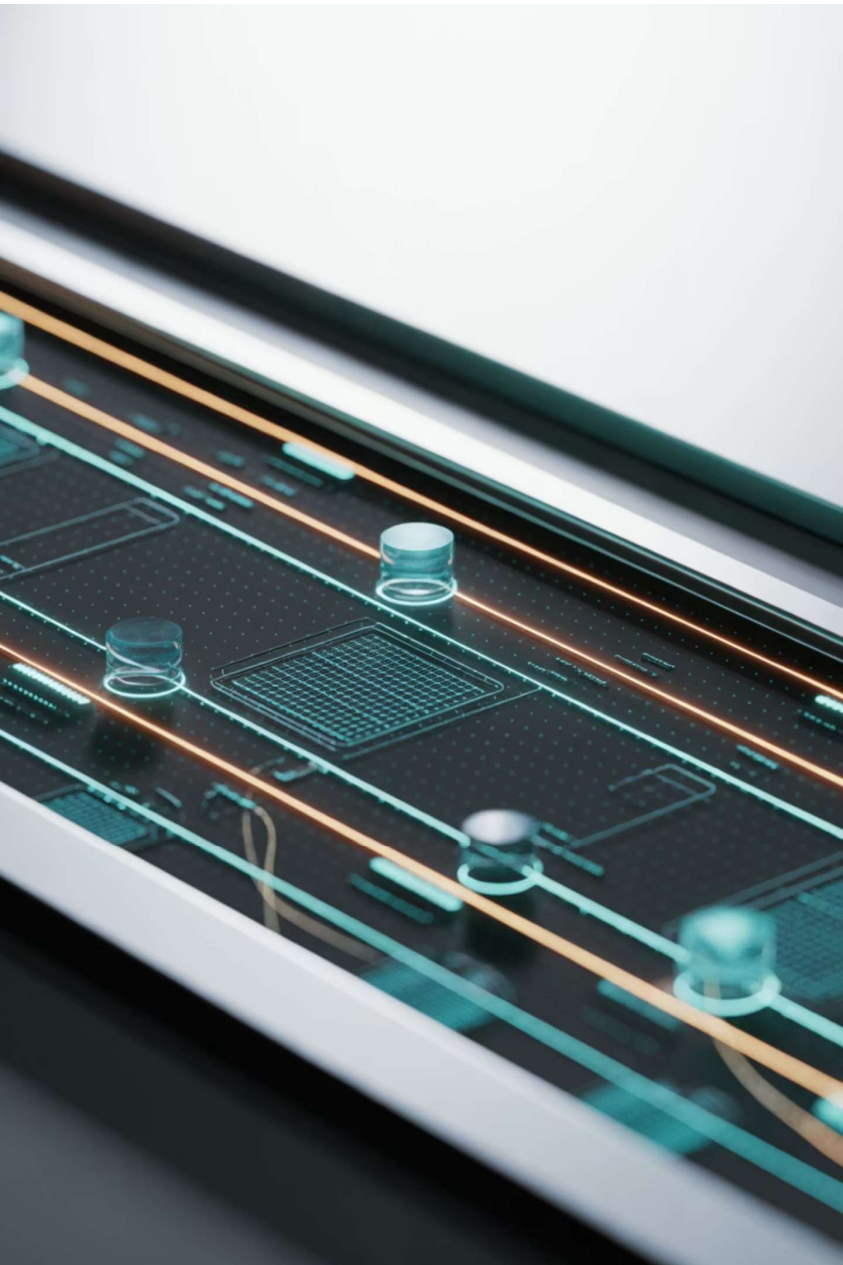
## 人事管理

教職員聘任、薪資、考績資料。應依人事法規蒐集,並限定人事單位人員方可接觸。

5

## 校友聯繫

畢業生聯絡資訊。應取得同意後始可用於校友活動通知或募款,不得任意轉供第三方使用。



# 利用階段:特定目的範圍內使用

個資的**利用**必須在蒐集時告知的特定目的範圍內進行,且不得逾越必要程度。

## ✓ 合法利用範例

- 學生成績用於學期成績計算與登錄
- 聯絡電話用於通知課程異動或緊急聯繫
- 研究資料用於論文撰寫與發表(已匿名化)
- 獎學金申請資料用於審核及撥款

## ✗ 違法利用範例

- 將學生名單提供給廠商行銷使用
- 未經同意將研究參與者資料用於其他計畫
- 將成績資料公開張貼於公布欄(可識別個人)
- 擅自將教職員通訊錄提供外部單位

# 常見違法利用案例警示

## 案例一:成績單誤寄

某教師將全班學生成績以電子郵件寄送,但誤將所有學生信箱放在「收件者」欄位而非「密件副本」,導致每位學生都能看到其他人的姓名、學號及成績。

**違法事由:**未妥善保護個資,導致資料洩漏給非當事人。

## 案例二:研究資料轉用

某研究助理將先前研究計畫蒐集之問卷資料,未經當事人同意即提供給另一位教師作為新研究使用。

**違法事由:**超出原蒐集目的利用個資,且未取得當事人同意。

## 案例三:名單外流

某系辦助理將學生名單及電話提供給廠商作為實習媒合,但廠商卻用於推銷課程。

**違法事由:**未經同意提供個資給第三方,且廠商利用超出原定目的。



## 第三單元

# 個資管理流程與文件

建立標準作業程序確保合規



# 告知同意書的撰寫要點

## 必備六大要素

1. **機關名稱**:○○大學○○系所/單位
2. **蒐集目的**:具體說明用途(如:課程成績管理、研究分析)
3. **個資類別**:列舉蒐集的資料項目
4. **利用期間、地區、對象及方式**
5. **當事人權利**:告知可查詢、更正、刪除等權利
6. **不提供的影響**:說明拒絕提供資料的後果

## 撰寫原則

- 使用**淺顯易懂**的語言,避免艱澀法律用語
- 版面清晰,重點項目以**粗體**或**底線**標示
- 提供**同意欄位**,讓當事人勾選或簽名
- 保留簽署紀錄,以備日後查證

☐ **提醒**:同意書應在蒐集個資之前或當下取得,事後補簽無效。



# 委外處理個資的管理要點

當學校委託廠商處理個資(如系統開發、資料建檔、問卷調查等),學校對受託者負有**適當監督義務**。若受託者違法處理個資,學校須負連帶責任。

## 委外前評估

- 確認受託者具備個資保護能力
- 檢視其資安措施與管理制度
- 要求提供個資保護聲明或證明文件

## 契約應載明事項

1. 個資處理的目的與範圍
2. 禁止轉委託或須經學校同意
3. 採取之安全維護措施
4. 委託關係結束後資料返還或銷毀方式
5. 違約責任與賠償條款
6. 學校得進行稽核之權利



# 個資存取權限管理

個資的存取應採取**最小權限原則**,僅授予必要人員適當權限,並建立完整的存取紀錄。



## 系統管理員

最高權限,負責系統維護與權限設定



## 業務主管

可存取所屬單位相關個資,進行審核與管理



## 一般承辦人員

僅能存取業務所需之特定個資



## 查詢權限人員

僅具備查詢權限,無法修改或下載

# 存取控制的具體措施



## 帳號密碼管理

設定強密碼政策,定期更換密碼,不得共用帳號,離職時立即停權



## 雙因素驗證

重要系統啟用多重身分驗證機制,提升安全性



## 存取紀錄

系統自動記錄存取者、時間、動作,定期檢視異常存取行為



## 資料加密

敏感個資應加密儲存與傳輸,防止未授權存取

# 個資盤點作業

個資盤點是管理制度的基礎,透過系統化清查,掌握學校內所有個資的流向與風險。

01

## 個資盤點作業

由各單位指派熟悉業務的人員組成

03

## 釐清資料流向

記錄個資從蒐集、處理、利用到銷毀的完整流程

05

## 填寫盤點表單

完整記錄於個資盤點清冊中

02

## 識別個資項目

列出單位內所有蒐集、處理或利用的個資類別

04

## 評估儲存方式

確認資料儲存位置、媒體類型與安全措施

06

## 定期更新

每年至少盤點一次,業務異動時即時更新



# 個資盤點清冊範例

個資項目	蒐集目的	保管單位	儲存方式	保存期限	安全措施
學生基本資料	學籍管理	教務處	校務系統	永久	帳號權限控管、加密傳輸
學生成績	成績管理	教務處	校務系統	畢業後5年	權限分級管理
獎學金申請資料	獎助學金審核	學務處	紙本+電子檔	核定後3年	上鎖櫃存放、電子檔加密
教職員人事資料	人事管理	人事室	人事系統	離職後10年	專人管理、限制存取
研究參與者資料	研究計畫執行	各研究單位	獨立電腦	計畫結束後3年	匿名化處理、實體隔離

# 個資風險評鑑

完成盤點後,應針對各項個資進行風險評鑑,識別高風險項目並採取優先管控措施。

## 風險評估面向

- **資料敏感度**:是否為敏感性個資
- **數量規模**:涉及人數多寡
- **外洩可能性**:存取控制與技術防護是否充足
- **影響程度**:外洩後對當事人與學校的衝擊

## 風險等級分類

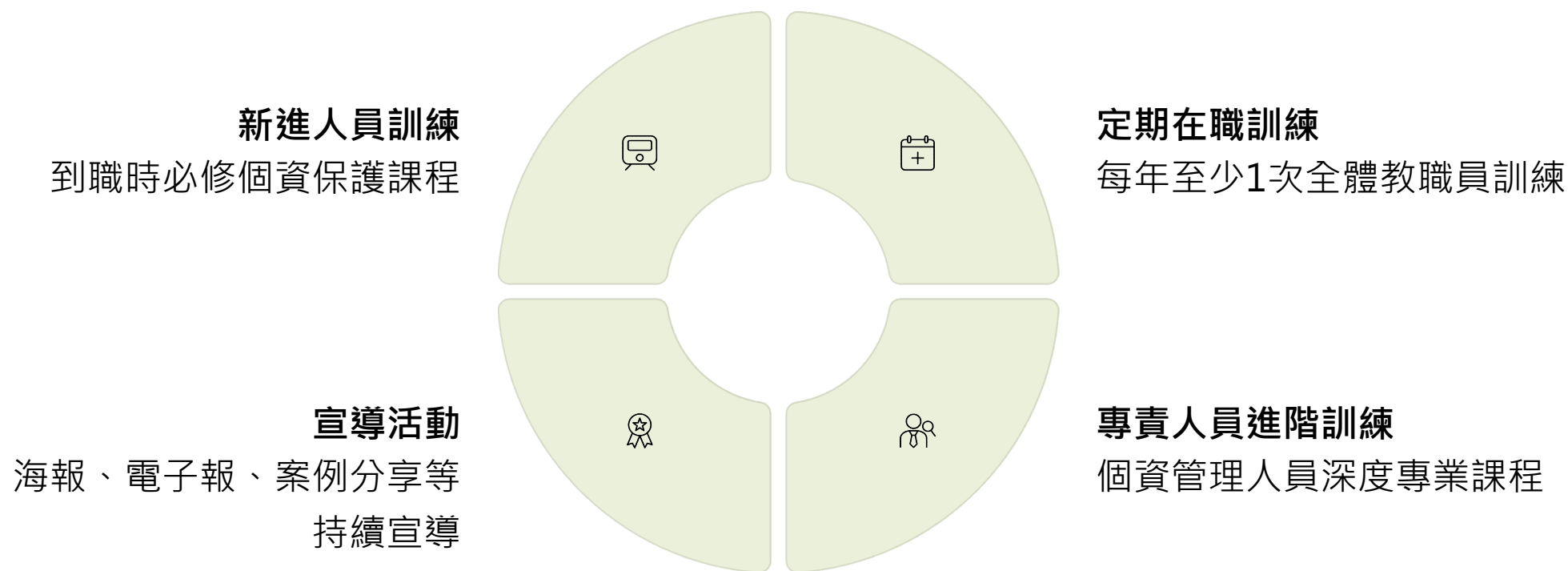
**高風險**:敏感資料且防護不足,優先強化

**中風險**:一般資料但數量大,需持續監控

**低風險**:非敏感且控管良好,維持現況



# 教育訓練制度



教育訓練應建立完整紀錄,包含課程名稱、時間、參加人員、測驗成績等,作為管理制度執行證明。

# 個資刪除與銷毀程序

## 何時應刪除個資？

- 特定目的消失或期限屆滿
- 當事人要求刪除(符合法定事由)
- 保存期限屆滿
- 個資已無保存必要

## 刪除方式

**電子檔案:**使用專業資料銷毀軟體進行多次覆寫,確保無法復原

**紙本文件:**使用碎紙機銷毀或委託專業銷毀公司處理,並取得銷毀證明

❏ **重要提醒:**僅刪除檔案或丟入資源回收筒不足以達到銷毀效果,資料仍可能被復原。應使用專業方法確保資料無法還原。



## 第五單元

# 個資外洩事件案例分析

從他人經驗學習預防之道







# 案例一:系統漏洞導致資料外洩

## 事件經過

某大學招生系統存在安全漏洞,未經授權者可透過網址列修改參數,存取其他考生的報名資料。該漏洞被發現前,已有數千筆考生個資(包含姓名、身分證號、聯絡方式)可能被不當取得。

## 原因分析

- 系統開發時未進行充分資安檢測
- 缺乏權限驗證機制
- 未定期進行系統弱點掃描

## 影響結果

- 遭主管機關裁罰150萬元
- 引發媒體關注,學校形象受損
- 考生提起集體訴訟求償

## 改善措施

- 立即修補系統漏洞
- 強化系統開發與上線前資安審查
- 建立定期弱點掃描機制
- 加強資安人員專業訓練



## 案例二:人為疏失誤寄郵件

### 事件描述

某系所助理在寄送獎學金獲獎通知時,將所有獲獎學生的電子郵件地址放在「收件者」欄位,而非「密件副本」,導致每位收件者都能看到其他人的姓名與電子郵件。

### 問題核心

承辦人員對電子郵件使用規範不熟悉,缺乏個資保護意識。單位內部也未建立郵件寄送的標準作業程序與覆核機制。

### 預防方法

群組郵件一律使用「密件副本」功能;建立郵件寄送檢核表;使用專業郵件系統的安全發送功能;加強教育訓練並定期提醒。

# 案例三:雲端資料夾權限設定錯誤



## 事件概況

某教師將學生作業與成績資料上傳至雲端硬碟,為方便助教存取,將資料夾分享連結設定為「知道連結的任何人都可檢視」,導致該連結被轉發後,校外人士也能查看所有學生的個資與成績。

## 根本原因

- 不了解雲端分享的權限設定選項
- 為求方便而犧牲安全性
- 未定期檢查分享設定

**正確做法:**指定特定人員存取,使用「僅限邀請對象」設定;避免使用公開連結;定期檢視分享狀態;敏感資料應加密後再上傳。

# 案例四:USB隨身碟遺失

## 事件發生

研究助理將問卷調查原始資料(含受訪者姓名、電話等)存於USB隨身碟中,在搭乘大眾運輸工具時不慎遺失

## 通知當事人

以電話及郵件通知所有受訪者,說明情況並致歉,提醒注意可能的後續風險

1

2

3

4

## 即時應變

發現遺失後立即向指導教授及學校通報,並評估資料外洩風險與影響範圍

## 檢討改進

要求所有研究人員不得使用個人隨身碟儲存研究資料;提供加密隨身碟;改用學校安全雲端儲存

# 案例五:委外廠商違規使用個資

## 事件始末

某大學委託廠商進行校友問卷調查,提供校友名單及聯絡方式。廠商完成調查後,未依約刪除資料,反而將名單轉售給補習班用於招生行銷,引發校友大量申訴。

## 責任歸屬

雖是廠商違約,但學校因未善盡監督義務,仍須負連帶責任,遭裁罰並賠償校友損失。

## 關鍵缺失

- 委外契約未詳細規範個資保護義務
- 未要求廠商簽署保密協議
- 委託期間未進行查核
- 結案時未確認資料銷毀

## 經驗教訓

選擇具信譽與資安認證的廠商;契約應明訂詳細個資保護條款;定期稽核執行情形;委託結束必須確認資料已完全銷毀。

# 課程總結:個資保護的核心要點



## 目的明確

蒐集個資前先確認目的,僅蒐集必要資料



## 充分告知

依法告知當事人蒐集目的、類別與利用方式



## 安全維護

採取技術與管理措施確保個資安全



## 限期保存

依規定期限保存,屆滿後立即銷毀



## 範圍內使用

在特定目的範圍內利用,不得挪作他用



## 持續警覺

保持個資保護意識,發現問題立即通報

# 個資保護是每個人的責任

個人資料保護不僅是法律要求,更是對當事人隱私權的尊重與保障。在數位時代,每一位教職員工都是個資保護的守門人。

從日常教學、行政作業到研究活動,我們無時無刻都在接觸個人資料。唯有建立正確的認知、養成良好的習慣、遵循標準的程序,才能真正落實個資保護。

記住:保護個資,就是保護他人的權益,也是保護自己與學校的聲譽。

## 從今天開始

- 檢視手邊的個資是否妥善保管
- 確認個資蒐集與利用是否合法
- 定期更新資訊安全知識
- 發現問題時勇於提出並尋求協助
- 將個資保護意識融入日常工作







謝謝參與

# 課後測驗(1/6)

- 本次測驗採線上方式實施，  
共計選擇5題，合格分數為80  
分。



# 課後測驗(2/6)

## 個人資料告知暨同意書

### 一、適用範圍

本同意書說明聯準科技服務有限公司（以下簡稱本公司）將如何處理本表單所蒐集到的個人資料。

### 二、資料的蒐集與使用方式

- 本表單會蒐集您的個人資料並處理與利用。
- 蒐集之目的：本表單蒐集之個人資料僅為教育訓練相關服務目的使用【「特定目的」代碼為：〇〇二 人事管理及一〇九 教育或訓練行政】，不做為行銷及其他之用。
- 蒐集之個人資料類別包括：單位及姓名【「個人資料之類別」代碼為：C〇〇一 辨識個人者】。
- 利用之期間、地區、對象及方式：
  - 期間：除法令另有規定之個人資料保存期限外，教育訓練相關資料於系統上保留3年，屆期即刪除。
  - 地區：台灣地區（包含澎湖、金門及馬祖等地區）或其他為完成上開蒐集目的所必須或本公司執行業務所必須之地區。
  - 對象：本公司客戶使用線上教育訓練評量系統及填寫問卷人員。
  - 方式：書面及電子方式。
- 您可隨時依個人資料保護法之相關規定，向本公司查詢本公司所蒐集您的個人資料、要求補充或更正、請求停止蒐集、處理或利用、請求查閱、製給複製本、刪除。本公司聯絡方式為：  
電話：(02) 2251-1393；電子郵件：alex.wu@twnexus.com
- 如您要求本公司停止蒐集、處理或利用您的個人資料，或是要求刪除您的個人資料，除有其他相關法規限制，本公司將比照辦理。
- 除非取得您的同意或其他法令之特別規定，本公司絕不會將您的個人資料揭露予第三人或使用於蒐集目的以外之其他用途。

### 三、資料之保護

- 僅有經過授權的人員才能接觸您的個人資料，相關處理人員皆簽有保密合約，如有違反保密義務者，將會受到相關的法律處分。
- 本公司將依據本公司的個資保護控管程序留存與銷毀您的個人資料。

### 四、其他

本同意書可能會因應個人資料保護法或其他相關法規、以及實際需求進行修正。

✓ 我瞭解與同意以上文字

離開

請點選同意

# 課後測驗(3/6)

選擇今日的課程名稱

請選擇課程與輸入姓名

○○室\_王○○

課程

智慧型手機資訊安全大揭密 (是非5題, 選擇5題)

姓名

請輸入【部門-姓名】，業者請輸入【公司(單位)名稱-姓名】

請輸入您的姓名！

☒ 我已閱讀並且同意個資告知條款

開始作答

記得勾選

# 課後測驗(4/6)

## 選擇題

1、下列何者非官方APP市集？

- A. App Store。
- B. Google play
- C. 阿榮福利味。
- D. Windows市集。

2、下列何者為行動APP安裝原則？

- A. 確認載點為官方市集。
- B. 下載前需詳細閱讀介紹與評論。
- C. 下載前需詳細閱讀授權原則。
- D. 以上皆是。

3、有關Line@的認證帳號下列何者為是？

- A. 灰色盾牌。
- B. 藍色盾牌。
- C. 綠色盾牌。
- D. 以上皆非。

4、下列何者設定不但是非避免干擾選擇，而且可能導致風險？

- A. Line關閉接收行銷資訊。
- B. Line關閉自動加入好友。
- C. Signal 關閉螢幕鎖定。
- D. 以上皆是。

5、有關行動裝置安全敘述，下列何者為是？

- A. 應有本機防護、使用者安全意識。
- B. 應建立安全的上網環境行為。
- C. 應選擇安全的APP下載環境。
- D. 以上皆是。

nexus1621.dscloud.mobi 說

提交後不能再修改，確定要提交嗎？

確定

取消

作答完成後  
點選確認提交

完成作答提交

# 課後測驗(5/6)

## 您已經完成課後評量

評量提交後無法修改，若您有任何問題，請向授課講師提出。

課程：智慧型手機資訊安全大揭密

姓名：111

得分：0

您的評量結果低於標準（70分），您可點擊【再評量】進行複測

再評量

其他課程評量

填寫課後滿意度調查表

**請填寫  
滿意度調查表**



# 課後測驗(6/6)

- 本次測驗採線上方式實施，共計選擇**5題**，測驗網址如右側QR code。
- <https://nexus1621.dscloud.mobi/exam/exam1.php?course=360508>
- 請在姓名欄位，填寫部門及姓名。  
範例：數資室-你的大名



# 課後隨堂測驗