茶餘飯後話資訊安全

-提高資安意識從現在起-

圖書資訊處/吳思緯 製作

一、為什麼要重視資訊安全?

為什麼要重視資訊安全 - Outline

- 層出不窮的資安問題影響你的食.衣.住.行
- 國內十大資安事件說給你聽
- 資訊安全的威脅來源
- 駭客們到底要什麼?
- 資安事件起因及因應
- ★ 資訊安全與資訊安全管理系統
- ★ 本校的資訊安全政策

層出不窮的資安問題 影響你的食.衣.住.行

- 資安事件透過不同駭客手法，影響個人生活、政治、金融等各種層面

  小至

  – LINE帳號遭假冒，親朋好友皆被騙!
  – 網購洩個資?
  – 丟廣告信/貨運包裝，姓名、地址、電話全都露!

  .....

  大至

  – 一銀內網遭駭，爆發跨國ATM盜領案
  – 希拉蕊電郵門事件，讓國家機密暴露在高風險，最終甚至影響了世界強國的選舉結果

  ……

國內十大資安事件說給你聽

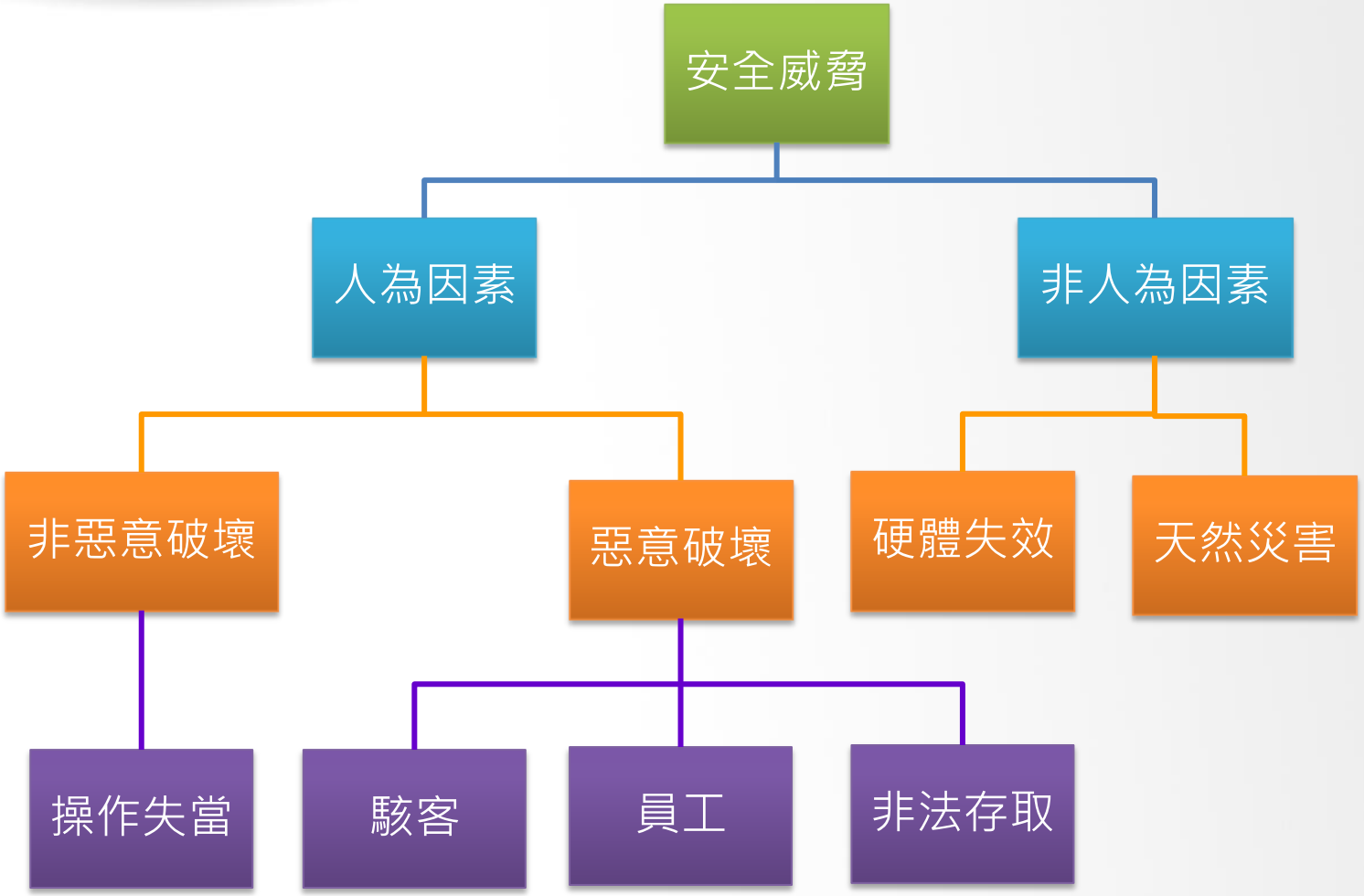
- 近年台灣資安事件層出不窮，造成國民個資外洩、電子商務及金融業營運損失、企業面臨駭客攻擊，更對國土安全形成威脅。
- 為加強台灣中小企業防範資安攻擊事件，經濟部工業局委託工業技術研究院執行「資通訊安全產業推動計畫」，針對台灣資安事件與需求進行調查，並歸納出十大國內資安事件，分析常見資安事件與案例，呼籲企業與個人提升危安意識，並提供資安解決方案，協助企業強化資安防護解決方案，將風險與成本降到最低。

1. 資料外洩
2. 進階持續性威脅(Advanced Persistent Threat，APT)攻擊事件
3. 分散式阻斷服務(Distributed Denial-of-Service Attacks，DDoS)攻擊
4. 資料庫遭駭
5. 社交工程郵件詐騙
6. 手機或即時通訊息詐騙
7. 惡意程式威脅
8. 網站(頁)遭駭
9. 身分帳密遭盜用
10. USB威脅事件

-- RUN!PC 施鑫澤 2014/6/6

http://www.runpc.com.tw/news.aspx?id=101271

資訊安全的威脅來源



駭客們到底要什麼?

電腦帳密

- 透過電腦軟體漏洞、社交工程、鍵盤側錄程式或木馬植入，竊取帳密掌控電腦資源進行非法用途
  - 偵九揭露一銀ATM駭客入侵內網關鍵，竊取密碼2套手法曝光 (iThome, 2016)

個資

- 透過電腦軟體漏洞、社交工程或木馬植入遠端竊取個資進行非法用途
  - 社交網站 駭客攻擊寵兒 個資外洩溫床 (趨勢科技, 2011)
  - 健保局全民個資 遭中國駭取作息 (自由時報, 2013)

駭客們到底要什麼?

金錢

- 透過勒索病毒，讓受害者失去對系統或資料的控制，如果不付贖金給犯罪組織，將無法把遭加密的資料救回
  - 「勒索病毒」猖獗 古坑鄉公所也中鏢 (自由時報, 2016)
  - 網傳「勒索病毒」大量災情，IE、中國網站勿碰！ (自由時報, 2016)

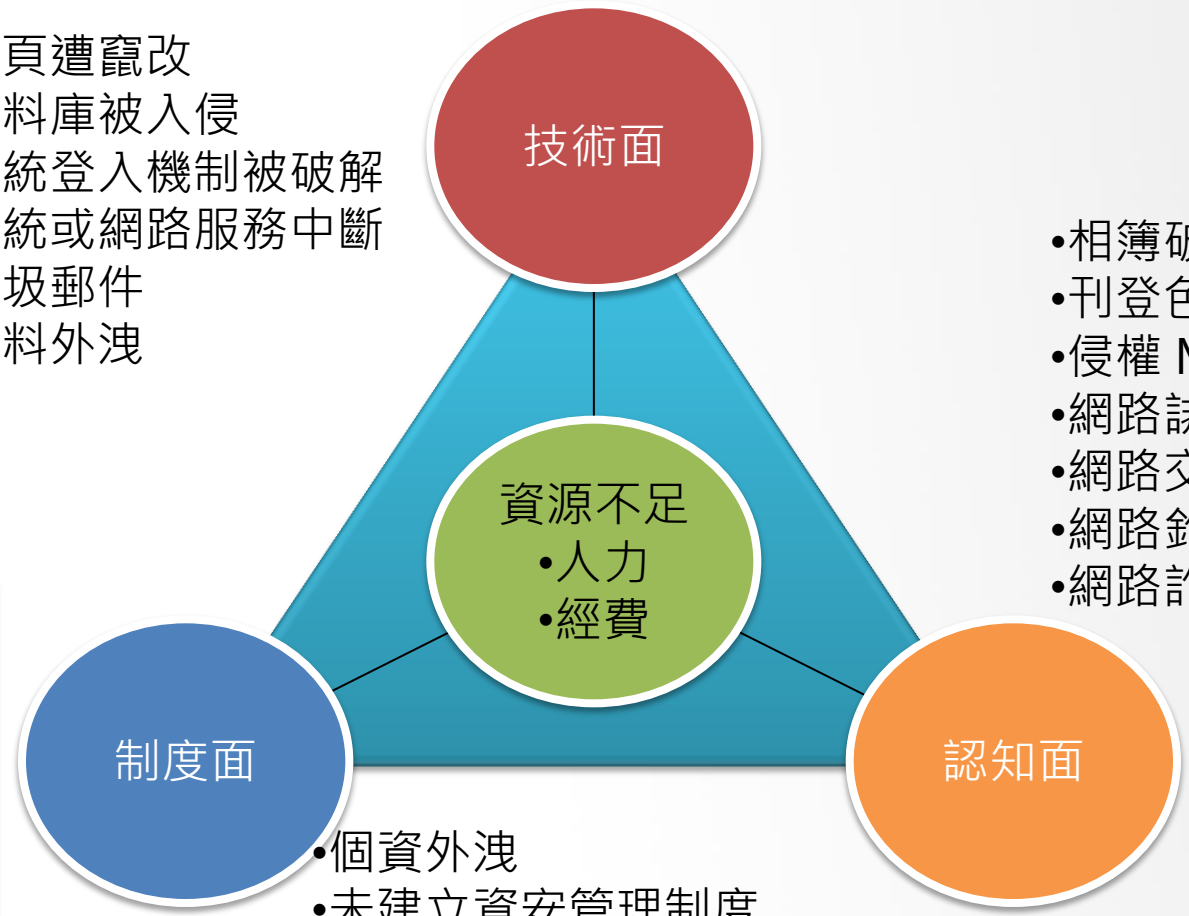
癱瘓主機或網路以達到特定目的

- 透過病毒發動DoS、DDoS與DRDoS或APT攻擊
- 可使目標網站或網路無法正常的運作
  - 駭客攻擊輔大官網為性侵受害者發聲 (風向新聞, 2016)
  - 中國網軍攻台轉向癱瘓作息 (自由時報, 2013)

資安事件起因及因應

強化系統安全

- 網頁遭竄改
- 資料庫被入侵
- 系統登入機制被破解
- 系統或網路服務中斷
- 垃圾郵件
- 資料外洩



- 相簿破解
- 刊登色情照片/影片
- 侵權 MP3/文章下載
- 網路誹謗
- 網路交易糾紛
- 網路釣魚
- 網路詐騙

增進資安認知加強教育訓練

- 個資外洩
- 未建立資安管理制度
- 資安管理制度未落實

落實之管理制度建立易於操作與

資訊安全與資訊安全管理系統

- 資訊安全 (Information Security)意旨在於保護資訊之機密性、完整性與可用性。

  ★機密性(Confidentiality)：確保只有被授權的人可以存取

  ★完整性(Integrity) ：確保資訊及處理方法的正確及完整

  ★可用性(Availability) ：確保被授權的人有需要時可以存取

- 資訊安全管理系統(Information security management system，簡稱ISMS)：
  - 乃組織整體管理制度的一部份，必需依據風險管理的方法加以制訂，進而用以建立、執行、操作、監控、審查、維護與改進組織的資訊安全。
  - 其目的在於保護資訊資產的機密性、可用性與完整性。

本校的資訊安全政策

- 為了促使本校各項資訊安全管理制度能貫徹執行、有效運作及持續進行，以維護本校重要資訊系統的機密性、完整性與可用性，特訂定以下資訊安全政策。作為日常工作的指導原則，以保障教職員生的權益。

★提升資安共識，強化資安訓練

- 督導同仁落實資訊安全工作，建立「資訊安全，人人有責」的觀念，每年持續進行適當的資訊安全訓練，以提高資訊安全意識。
- 如有違反資訊安全相關規定，究其權責依人員獎懲相關規定辦理。

★健全資安防護，確保營運持續

- 由本校全體員工貫徹執行資訊安全管理制度，以保護資訊資產免於外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險。
- 選擇適切的資安防護措施，將風險降至可接受程度。並持續進行監控、審查及稽核資訊安全有關的作業，以確保業務營運持續，達到永續經營的目的。

二、你我身邊的資安實例

你我身邊的資安實例 - Outline

- Q1. ATM提款機遭駭，自行吐鈔
- Q2. 勒索軟體 CryptoWall 3 已造成 3.25 億美元損失
- Q3. 公務即時 LINE，洩密也能賴？
- Q4. 手機中毒事件
- Q5. 各家瀏覽器停止支援 Adobe Flash Player
- 簡易資訊安全小撇步!

案例一：ATM提款機遭駭，自行吐鈔

【資料來源1：TechNews科技新報，103/02/03】
【資料來源2：iThome，102/10/18】
【資料來源3：iThome，103/05/09】
【資料來源4：網路社群文章】

1.案例說明

現第一銀行發生41臺ATM提款機遭駭，駭客在完全無操作ATM的情形下，直接讓ATM吐鈔後大量提領，盜領總額8327餘萬元。

2.原因分析

1) 全世界仍有超過九成的ATM提款機使用Windows XP作業系統
2) 透過 USB 裝置與 Windows XP 的自動播放功能，成功將惡意軟體植入 ATM，強制將 ATM 重開機後執行特定程式。
3) 本案例的發生原因，疑似持續使用已停止維護的舊版作業系統之結果
   ① 微軟已於103年4月8日終止 Windows XP 作業系統之維護，並不再修補系統漏洞
   ② 因此，在電腦連結網路的情況下，作業系統只要存在漏洞，就容易被駭客利用

3.資安風險

1) 使用外接式儲存裝置的風險

① 什麼是外接式儲存裝置？例如行動硬碟或隨身碟等

② 駭客會透過USB隨身碟、隨身硬碟來散布各種惡意程式，並把XP的漏洞極大化，藉此攻擊該電腦或系統

2) 瀏覽網頁的風險

① 在XP停止更新之後，新的XP入侵漏洞和攻擊套件，都可能會在駭客之間流通，進而被駭客所利用

② 因為微軟不再提供XP持續性的官方漏洞修補與更新，使用者在瀏覽網頁時，將持續性曝露在風險之中

3) 開啟Email 和使用即時訊息會有風險

① 有許多的攻擊會透過Email來發送含有非法網址的釣魚郵件，或利用即時訊息來發送詐騙的網址

② 使用者不小心連結並下載到這些網址所夾帶的附件，都可以被植入惡意程式，進而讓駭客控制電腦

4) 未安裝防火牆、防毒軟體，及使用弱強度密碼(例如密碼設定為1234簡單密碼)風險因為微軟不再提供XP的修補與更新，駭客可以利用最新的XP漏洞發動攻擊

4.建議方式

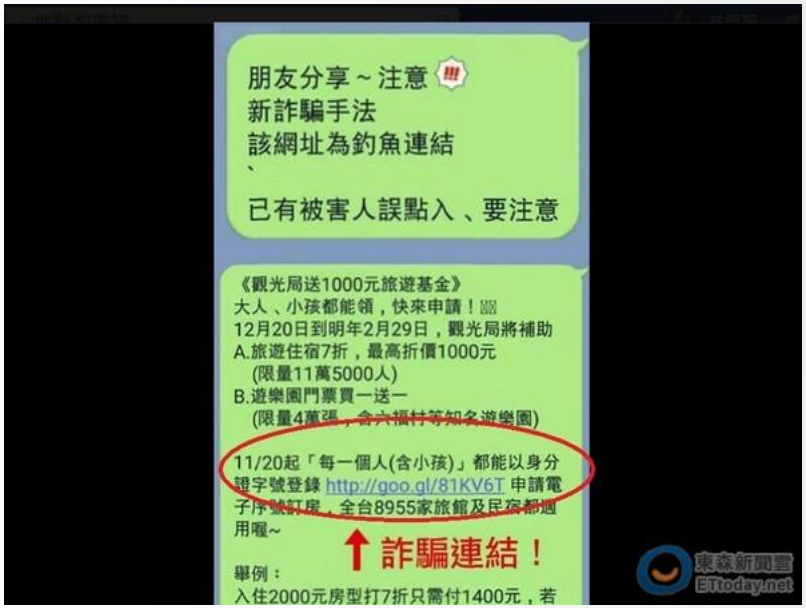
1) 升級仍提供維護支援的作業系統，例如：Windows 7(含)以上版本
2) 短期內無法升級，該怎麼辦？
   - ① 安裝防毒軟體，並定期更新病毒定義檔，可預防大約八成的已知病毒與惡意程式
   - ② 盡量不連接網路，避免遭受到攻擊、不隨意使用隨身碟等外接裝置

案例二：勒索軟體 CryptoWall 3 已造成 3.25 億美元損失

【資料來源：技術服務中心整理，104/11/17】

- 勒索軟體 CryptoWall 3 有兩大感染途徑，分別是網路釣魚郵件與攻擊套件
  - 在 7 萬個感染案例中約有三分之二是因網路釣魚郵件而受到感染。
  - 30%則是駭客透過攻擊套件攻擊受害者。
- CryptoWall 3 加密裝置上的檔案，駭客通常要求受害者支付比特幣，價格從數百美元到數千美元不等，受害者未於指定的時間內匯款，駭客即會將贖金提高到一倍。估計操作 CryptoWall 3 的駭客集團已獲利 3.25 億美元，主要的受害者位於北美市場。

- 加密勒索軟體目前尚未有有效解法
  - 資料被勒索軟體加密，以目前的解密技術及設備能量是無法在能接受的時間範圍解密成功。
  - 除了確實備份資料外，應從資安意識教育訓練著手。
  - 目前感染加密勒索軟體的途徑，大多是使用者被社交工程郵件攻擊，或是自行在網路上點擊不當惡意連結。



- 【管理 Tips】【資料來源：資通安全法律案例宣導彙編第 12 輯 104/12】
  - 為防範勒索軟體對於組織之危害，在日常資安教育訓練中，就應該對組織內的同仁加強宣導
    - 無論電子郵件、即時通訊或是社交軟體之來源管道為何，對於陌生的訊息都必須避免任意開啟
    - 未經查證下也應該儘量避免直接點選所附的連接
  - 在日常作業層面，組織應定期檢視現有的備份作業是否完整與依照既定計畫進行備份，避免因資料缺乏導致組織之正常作業停擺。
  - 因應新型態的攻擊模式，組織應定期接收相關的技術更新。
  - 發現資安管理措施有需要強化的地方，建議組織及早進行部署，或是增加監控的頻率，以確保組織資訊效能可正常運作。

案例三：公務即時 LINE，洩密也能賴？

【資料來源：聯合報 104/4/18】

- 拜科技進步所賜，即時通訊軟體(例如 skype 及 Line 等)越來越夯：
  - 在一般企業組織或社群中受到歡迎，成為政府機關提升公務聯繫效率的新幫手。
  - 提升公務聯繫效率的同時，即時通訊軟體的潛在風險也引發討論
    - 某公務人員曾將首長批示意見透過 Line 對外傳送，造成消息不當曝光。
    - 某公務群組遭駭客入侵，促使機關自我檢討公務聯繫作業，嚴禁「機密公文」以即時通訊方式傳遞。
  - 更深度的問題是，即時通訊所傳送的訊息無須依法進行存檔及列管，也無從追查，未來恐成了洩密和弊案的溫床。

- 【管理 Tips】【資料來源：資通安全法律案例宣導彙編第 12 輯 104/12】
  - 組織在導入或使用行動式設備時，應訂定相關政策規範，其中應包括：可在行動設備中使用的工作項目、資料儲存方式、行動設備需具備的保護設施、資料傳送要點，及資料銷毀的程序等。
  - 組織應採取相關配套措施以管控風險，並透過教育訓練、宣導或公告注意事項等方式，讓員工明瞭設備使用範圍、限制及相關安全規則。
  - 必要時，對於違反使用規範之員工應有相當內部懲處措施，以兼顧行動辦公需求並同時落實對於機敏資訊的保護。

案例四：手機中毒事件

【資料來源：iThome，104/10/12】

- 手機中毒事件
  - 用社交工程手法誘騙點擊簡訊中的連結網址，使手機被植入惡意程式，以致民眾收到高額電信帳單受害
  - Android 漏洞導致Google 帳號遭駭，利用Android 4.0 和5.0 作業系統漏洞，獲取在手機裡的Google相關應用程式資料(參考網址)

- IOS手機就不會中毒? – NO!!
  - IOS系統也不是沒有漏洞，只是由於封閉式的系統特性使得漏洞能夠及時的被發現和處理(原文網址)
  - 【iPhone】中國多款 App 被植入木馬程式
  - JailBreak(簡稱JB)後更容易中毒
- 簡易防範手機中毒
  - 隨時更新手機作業系統
  - 勿點擊來路不明訊息
  - 勿下載來路不明的app(特別是APK檔)
  - 使用兩階段驗證確保帳號安全
  - 可依需求安裝手機用防毒軟體

案例五：各家瀏覽器停止支援 Adobe Flash Player

【資料來源：TechNews科技新報，105/04/11】

- 各家瀏覽器停止支援Adobe Flash Player
  - Adobe Flash Player被大量運用在網路影片、遊戲及動畫等多媒體播放軟體
  - 但Flash存在最大缺點即是安全性漏洞，容易夾帶惡意程式，誘使使用者點擊後感染入侵
  - Google chrome於2016年12月釋出新版瀏覽器即停止支援Adobe Flash Player

- 簡易防範措施
  - 應用程式更新，確保漏洞已修補
  - 留意各種吸引點擊的連結，可能夾帶惡意檔案
  - 檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取
  - 定期資料備份

簡易資訊安全小撇步!

★簡易資訊安全小撇步!

- 作業系統更新、加裝防毒軟體並定期掃毒
- 避免將帳號密碼紀錄在他人可輕易獲取的地方。
- 可使用二次驗證增加帳號登入安全。
- 避免下載來路不明的程式。
- 避免開啟來路不明的信件。
- 避免瀏覽具有中毒高風險的網頁。
- 定期更換密碼，並使用他人不易猜出的密碼。
- 避免被聳動的標題吸引而點擊連結。

三、關於E-MAIL的資安小常識

關於E-mail的資安小常識 - Outline

- 社交工程：什麼是釣魚信呢?
- 防止網路釣魚找上你四步驟
- ★ 寄發全校信，請用密件副本 (BCC) 傳送郵件

網路釣魚信件類似的案例

- 好奇心是最大的漏洞

- 這樣的網路釣魚信件69%的人每週都碰到，25%高階員工被釣得逞，類似的案例還有:
  - 武媚娘有胸版影片
  - 遠離黑心食品
  - 這篇文章看了讓你多活 10 年
  - 行政機關辦公日曆表
  - 拍賣網站的 iPhone 新年特價超便宜?!
  - 二代健保補充保險費扣繳辦法說明

防止網路釣魚找上你四步驟

1. 點選連結前,先移動滑鼠檢查真實來源
   例如，以下連結似乎都指向Google？
   1) http://www.google.com — 真實的google 超連結
   2) http://www.google.com — 顯示文字是Google、但連結是Yahoo
   3) click here to go to Google（按這裡去Google） — 點我前往Google，但是實際上是到Yahoo
2. 收到要求提供個人資料的電子郵件要小心，即使信中有該公司的商標
3. 小心那些威脅要錢的電子郵件或其他訊息。
4. 檢查郵件內是否有拼寫錯誤和語法錯誤。
   – 當你收到寫得錯字連篇或是不通順的郵件時就有可能是假的。

寄發全校信，請用密件副本 (BCC) 傳送郵件

- 寄發大量收件人信件
  - 相信大家曾有過這樣的經驗，在一些朋友轉來轉去的信件中，在「收件者」這欄位一定會看到一些與你不相關的人。
  - 對於這樣沒有經過自己同意而被公佈電子郵件的行為在某些情境下是會造成收信人困擾的，然而很多人卻忽略了這小小的「禮節」
  - ★就個資法推行的角度來看，電子郵件帳號足以識別特定自然人之資料，也是所有同仁業務中不可或缺的一環，而上述的情況其實是可以利用**密件副本(BCC)**的功能來避免或保護的。
- 由於校內群組郵件寄送頻繁，務必使用密件副本。

什麼是密件副本(秘密副本)

- 密件副本 (BCC) 是看不見的複寫副本 (blind carbon copy) 之縮寫。
- 如果您將收件者的姓名加入到某份郵件的這個方塊中，則會將一份郵件傳送給該收件者，且郵件的其他收件者看不到此收件者的姓名。
- **密件副本使用原因**：
  - 保障隱私
  - 減少垃圾郵件