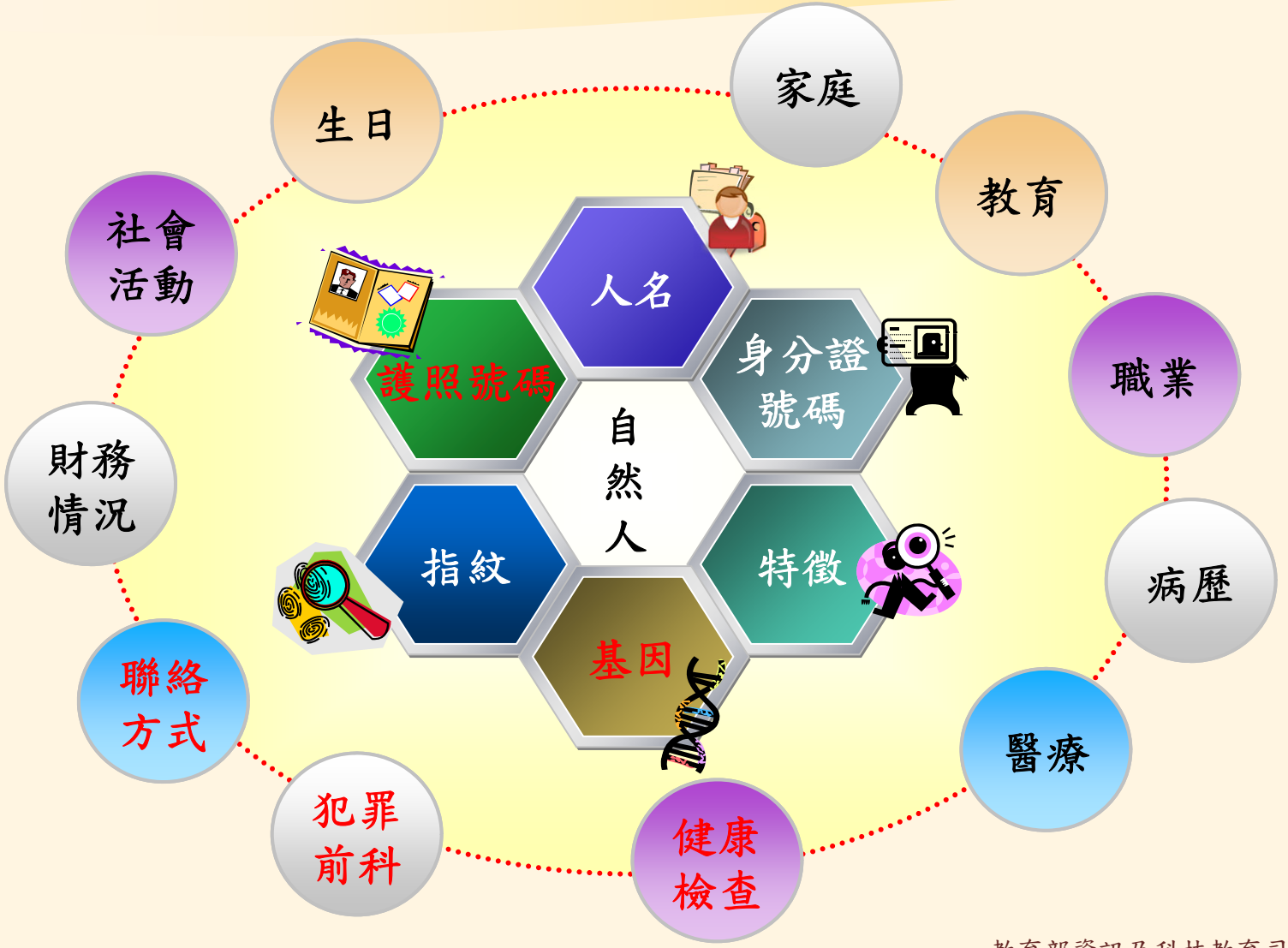
「資訊安全防護」宣導

資訊及科技教育司

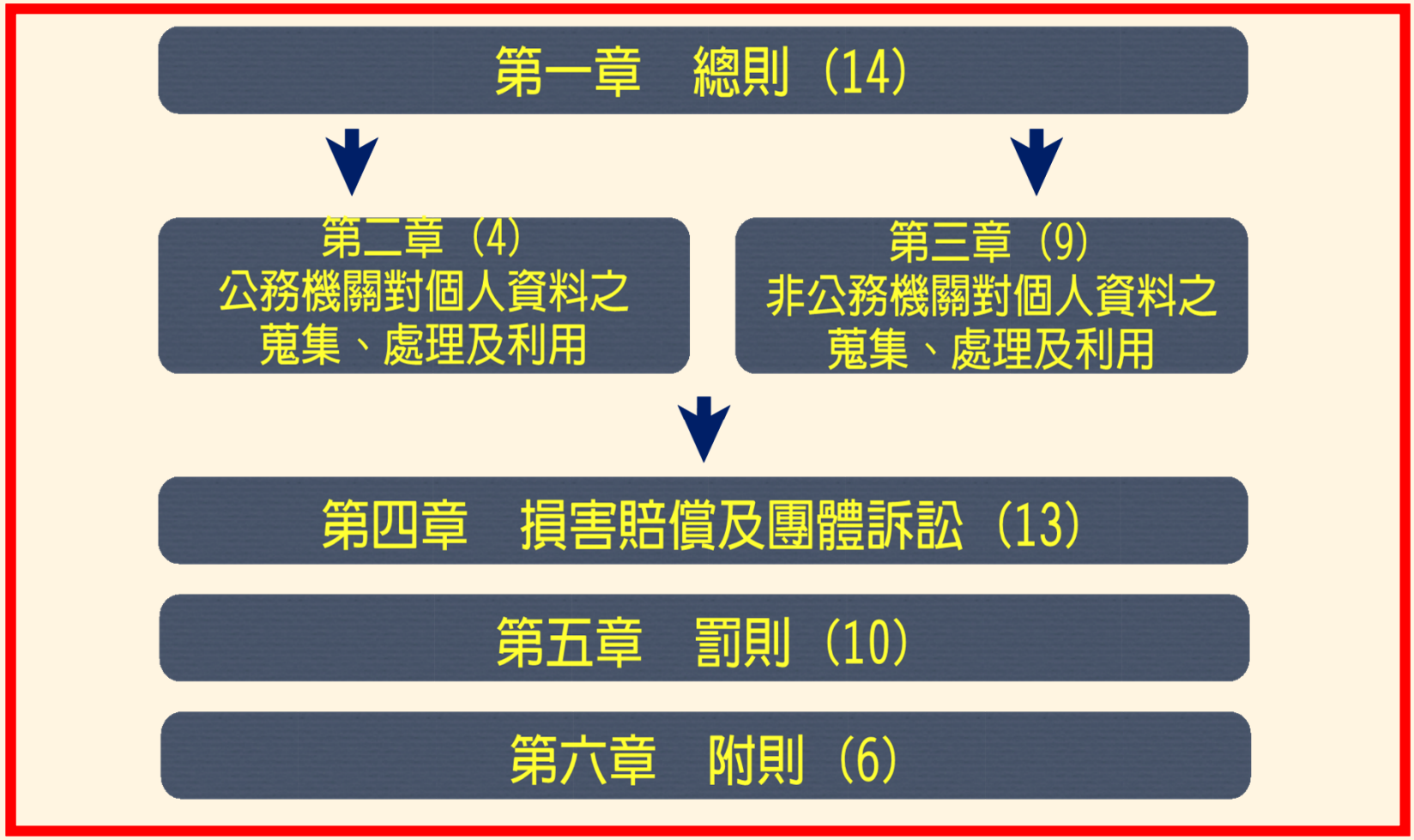
2023年12月27日

一、資訊安全及個人資料保護

何謂個人資料


家庭
教育
職業
病歷
醫療
健康檢查
犯罪前科
聯絡方式
財務情況
社會活動
生日
人名
身分證號碼
特徵
基因
指紋
護照號碼
自然人

個資法架構


第一章　總則（14）
第二章（4）
公務機關對個人資料之
蒐集、處理及利用
第三章（9）
非公務機關對個人資料之
蒐集、處理及利用
第四章　損害賠償及團體訴訟（13）
第五章　罰則（10）
第六章　附則（6）

哪些個人資料不受個資法保護?

- 自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料
  - 例如社交活動、寄送喜帖、親友通訊錄等
  - 上述資料的蒐集必須與職業或業務職掌無關
- 於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料
  - 例如運動會照片、遊樂場拍攝小孩與其他小孩一起遊玩的影片等
  - 為解決合照或其他在合理範圍內之影音資料須經其他當事人書面同意始得蒐集、處理或利用之不便，因此排除個資法對上述影音資料的適用，回歸民法規定

基本原則

- 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

教育體系資安事件案例

即時 要聞 娛樂 運動 全球 社會 地方 產經 股市 房市 生活 健康 …

學習歷程檔案遺失 蘇揆：即刻補救、專案團隊全面體檢

2021-09-26 13:48 聯合報 / 記者鄭媛／即時報導

學習歷程檔案是新課綱重頭戲，卻因廠商疏失，導致近八千位學生的學習歷程檔案消失。示意圖。本報資料照片

- 事件概要

  學習歷程系統搬遷至其他機房，重新開機後發現因設定錯誤導致硬碟資料被還原，造成使用者資料遺失。

- 發生原因

  備份機制失效、針對系統搬遷過程及結果缺乏驗證機制。

- 建議改善事項

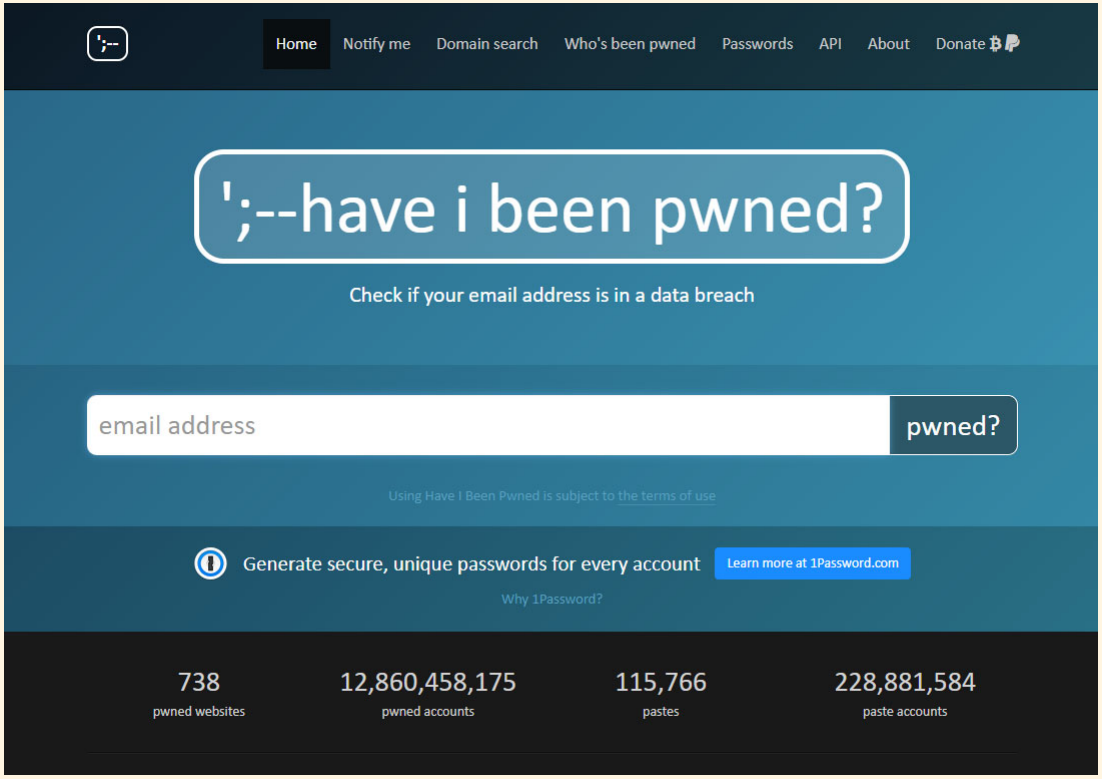
  落實變更管理、落實監控系統備份運作狀態等。

禁止帳號共用，禁止使用弱密碼

- 資通訊裝置及資通訊系統服務之帳號不得共用，以利鑑別使用者。
- 禁止使用弱密碼，弱密碼常見態樣如下：
  1. 個人生日、電話、身分證號碼。
  2. 鍵盤排列1qaz@WSX，英文單字welcome，一串數字123456等。
  3. 用外觀相似的替換符號，如簡單英文變化:I->1，0->0，a->@。
  4. 多個系統或網站平台共用同一組帳密或同一組密碼。
  5. 工作用密碼和工作相關，如”台北捷運”以注音輸入法對應英文"w961o3ru,6mp4"。

資安廠商發布2023年度十大弱密碼

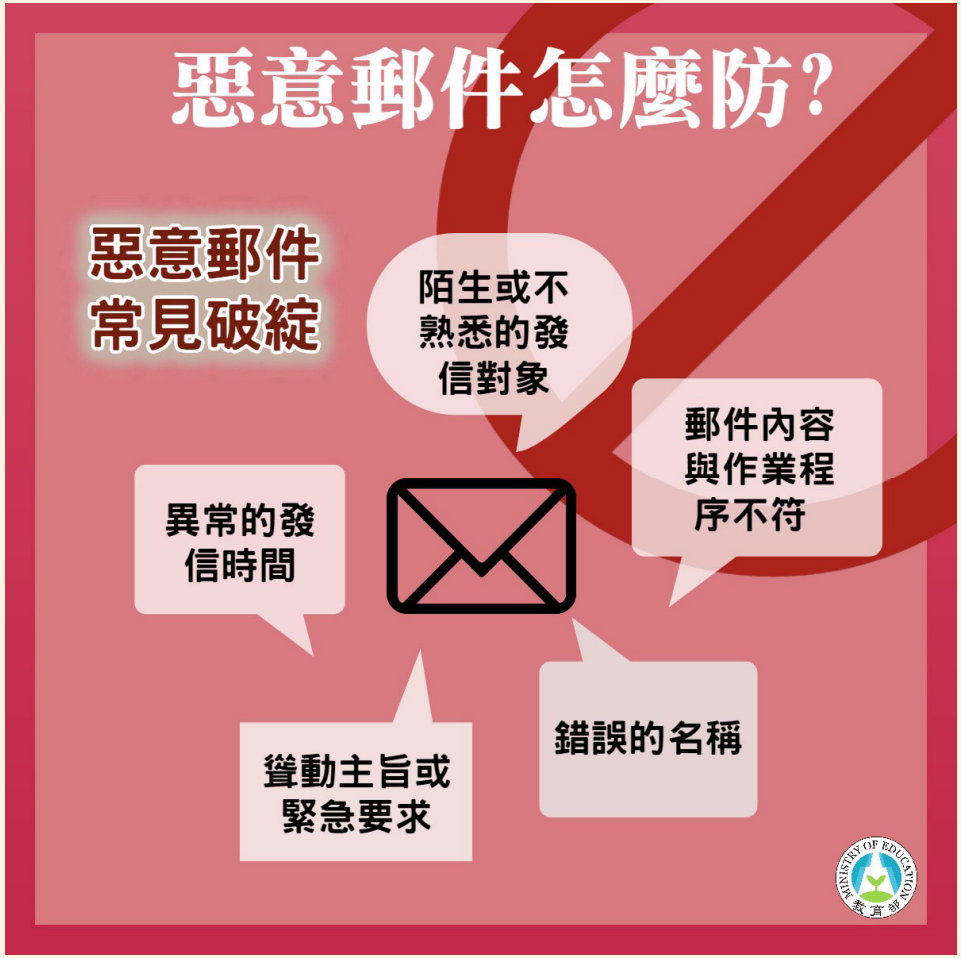
1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou
9. 111111
10. 123123



https://haveibeenpwned.com/
檢查你的E-mail 個資是否已被駭客竊取

二、社交工程攻擊防範

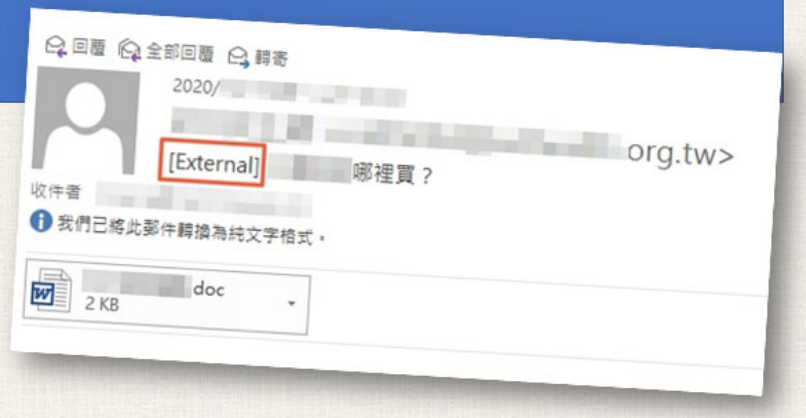
社交工程攻擊防範(1/6)


惡意郵件怎麼防?
惡意郵件
常見破綻
陌生或不熟悉的發信對象
郵件內容與作業程序不符
異常的發信時間
錯誤的名稱
聳動主旨或緊急要求

社交工程攻擊防範(2/6)

防範社交工程停看聽

- 主旨出現 [External] 表示寄件者為外部人員
- 注意陌生或不熟悉的寄件者



社交工程攻擊防範(3/6)

防範社交工程停看聽

- 寄件人與標題是否正確
- 與本身業務是否相關

不直接開啟

社交工程信件常見破綻

- 錯誤的名稱
- 異常的發信時間
- 郵件內容與作業程序不符
- 聳動或為緊急要求

社交工程攻擊防範(4/6)

防範社交工程停看聽

- 主動聯繫相關單位確認真偽
- 仍有疑義請洽機關資安窗口

若仍有業務上收信之需求，
可將可疑信件打包匯出後，
寄送資安窗口確認

社交工程攻擊防範(5/6)

惡意郵件 舉例

	旅遊休閒	親子遊孩子為何擺臭臉?調查：九成小孩想參與規畫行程
	金融財經	聖誕節送禮什麼最夯?概念股深入分析
	旅遊休閒	桃園青埔 漫遊奇幻海洋
	模擬案例	志願服務申請
	金融財經	台股後勢看漲 看好四大類別
	公務相關	公教人員健檢辦法
1	公務相關	您已接受邀請共用此行事曆
	新聞時事	夏季電費6月上路！台電估計約378萬戶不漲價，原因曝光
	新聞時事	補教狼師MeToo！最美禮生控「18歲生日遭揉胸強吻」
	生活消費	ChatGPT官方APP來了！台灣開放下載 iPhone搶先試
2	旅遊休閒	連假這樣請半個月都不用上班！快訂機票半月遊！

社交工程攻擊防範(6/6)

為防範社交工程攻擊，造成機關受駭、機密外洩，請注意並配合下列事項：

一	社交工程攻擊喜歡用「聳動標題、公務資訊、結合時事新聞、財金、健康、打折優惠促銷活動…等吸引人注意力、好奇心及混淆人心之事件」，誘騙使用者點擊釣魚信件或簡訊，騙取用戶個人資訊、密碼或下載惡意程式、檔案等，造成機敏資料外洩或遭勒索病毒攻擊等資安事件發生。
二	請關閉電子郵件預覽功能。
三	開啟郵件前，請確認主旨與本身業務相關，或與承辦人、寄件人確認來信。
四	不任意點閱郵件或簡訊中之超連結網址、附加檔案。
五	公務郵件與私人郵件應區隔，請勿將公務郵件地址用於註冊、認證其他非公務平台。
六	不隨意輸入帳號密碼資訊：輸入帳號密碼前應再三確認其正當性，避免遭假冒網站竊取。
七	若有可疑信件、簡訊或相關問題，請洽機關資訊或資安人員。

三、各機關對危害國家資通安全產品限制使用原則

機關選用資通訊產品時，請依行政院「各機關對危害國家資通安全產品限制使用原則」辦理

為避免使用有危害國家資通安全疑慮之資訊產品造成資安事件，請配合下列事項：

一	依據行政院國家資通安全會報技術中心通報，抖音(TikTok)與微信(WeChat)應用程式存在資安疑慮，可能蒐集使用者資訊並回傳至特定伺服器，為進行風險管控，請避免於公務手機與電腦中安裝與使用前揭應用程式。
二	為維護資通訊安全，避免重要資料及資訊外洩，請依行政院「各機關對危害國家資通安全產品限制使用原則」禁用有資安疑慮產品。
三	針對有資通訊安全疑慮之產品，請依上述原則第四條規定，辦理預防性防護作為：
	(一)應指定特定區域及特定人員使用，且不得傳播影像或聲音，供不特定人士直接收視或收聽。
	(二)購置理由消失，或使用年限屆滿應立即銷毀。
四	機關辦理採購合約時，應將前揭原則納入規範；亦請委外及合作廠商，處理相關公務資訊之設備，依前揭原則比照辦理。

四、資通安全教育訓練課程宣導

資通安全教育訓練課程宣導

一	應資安法要求，請機關於年底前完成資安法資安教育時數。
	(一)教育訓練法規依據：資通安全責任等級分級辦法，各級機關應辦事項—認知與訓練面向—資通安全教育訓練。
	(二)時數要求：機關應依機關資安等級要求取得訓練時數，資訊安全專職人員應取得「資通安全專業/職能訓練」要求時數，非資安資訊人員一般人員及主管應取得「資通安全通識教育訓練」要求時數。
二	課程資源：
	(一)實體課程
	(二)線上課程：臺北e大、e等公務園

五、降低電腦風險及修復作為

降低電腦風險及修復作為

1. 請勿安裝「未經授權」之軟體。
2. 更新電腦作業系統、應用程式及防毒軟體等至最新版本(個人電腦及筆電)。
3. 應定期備份電腦上的檔案及演練資料還原程序。
4. 避免連接「可疑網站」。
5. 不幸受到感染，請立即將受害電腦的網路連線及外接儲存裝置拔除，並關閉受害電腦無線網路。
6. 定期更新作業系統。