115資通安全教育訓練

國立嘉義高商

陳建文

2026.8.28

政令宣導

資通安全管理法及子法

- 107年6月6日通過，108年1月1日實施
  - 主管機關：行政院

- 數位發展部資通安署-資通安全管理法及子法
  - https://moda.gov.tw/ACS/laws/regulations/624

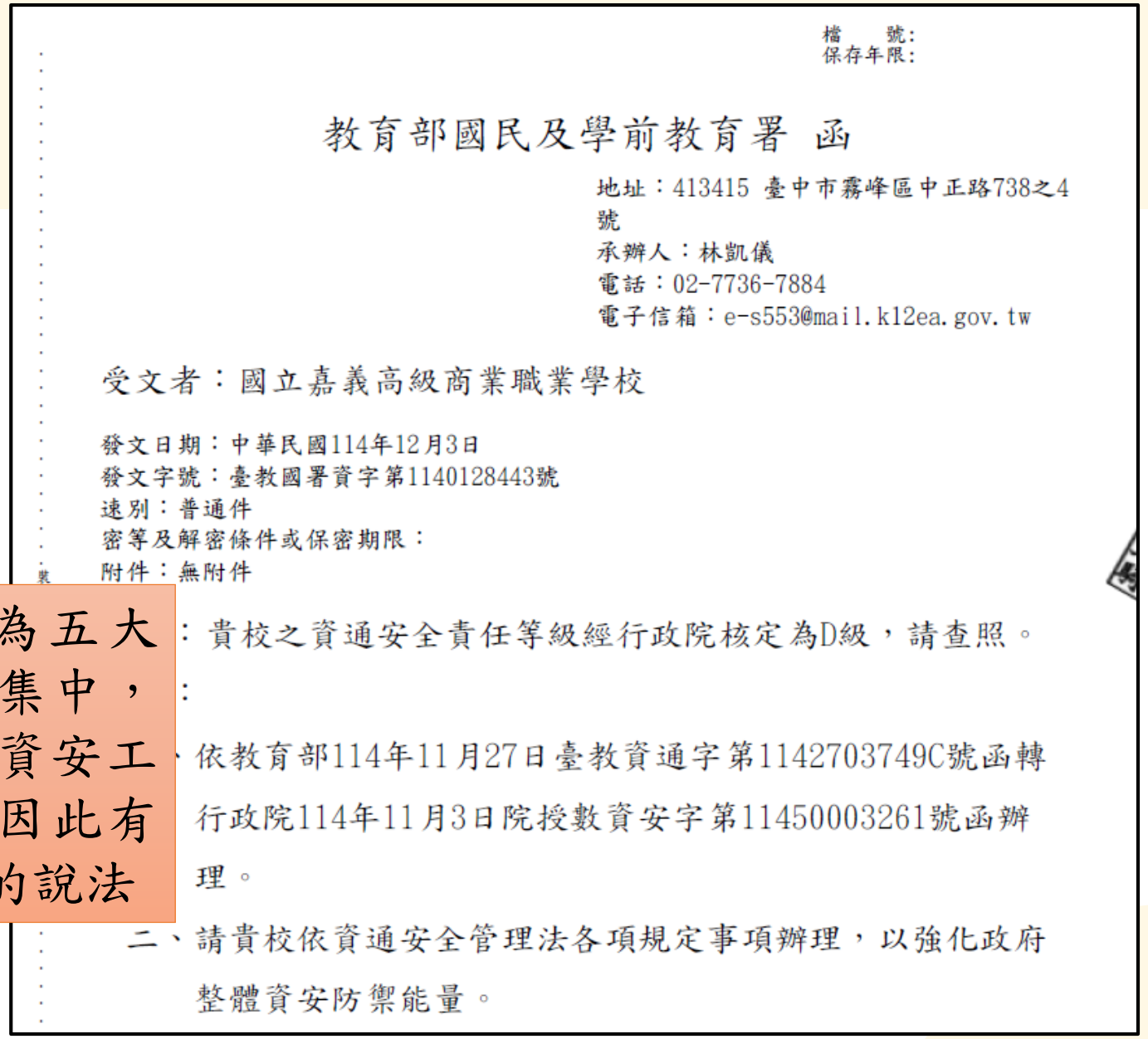
資通安全管理法及子法


資通安全管理法及子法
資通安全管理法
資通安全管理法施行細則
資通安全責任等級分級辦法
資通安全事件通報應變及演練辦法
資通安全維護計畫實施情形稽核辦法
資通安全情資分享辦法
公務機關所屬人員辦理資通安全事項作業辦法
危害國家資通安全產品審查辦法
國家資通安全會報設置辦法

資通法責任分級

- 資通安全責任等級分級辦法
- 本校核定為D級
- D級應辦事項
- C級應辦事項

核定D級是因為五大核心系統向上集中，而該做的相關資安工作仍不可少，因此有D+（C~D之間)的說法



檔　　號:
保存年限:

教育部國民及學前教育署 函

地址：413415 臺中市霧峰區中正路738之4號
承辦人：林凱儀
電話：02-7736-7884
電子信箱：e-s553@mail.k12ea.gov.tw

受文者：國立嘉義高級商業職業學校

發文日期：中華民國114年12月3日
發文字號：臺教國署資字第1140128443號
速別：普通件
密等及解密條件或保密期限：
附件：無附件

：貴校之資通安全責任等級經行政院核定為D級，請查照。

：

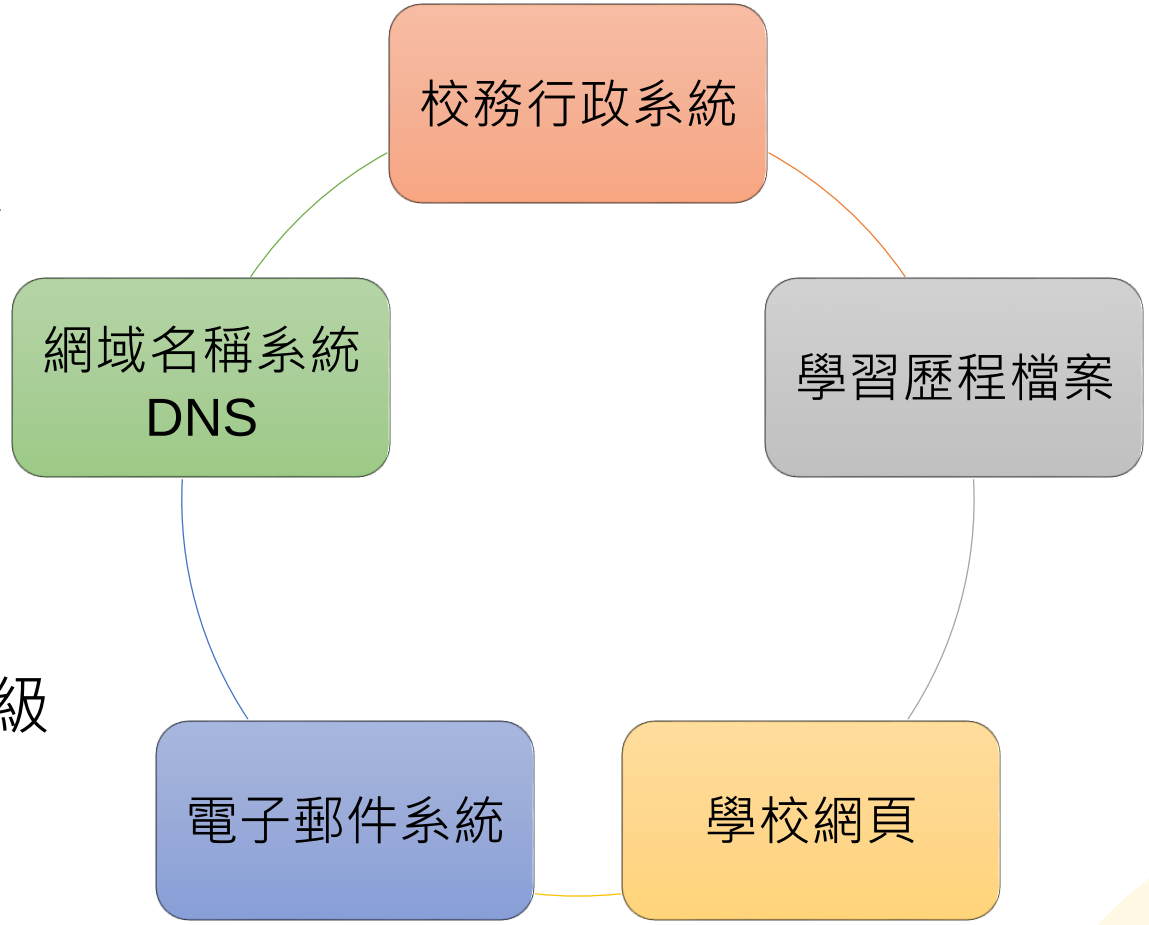
、依教育部114年11月27日臺教資通字第1142703749C號函轉行政院114年11月3日院授數資安字第11450003261號函辦理。

二、請貴校依資通安全管理法各項規定事項辦理，以強化政府整體資安防禦能量。

校園五大核心系統是那些？

- 資訊系統的安全管理重要且繁瑣
- 學校若有營運資訊系統應列C級
- C級單位應有資安專職人員1名

- 向上集中後，學校僅具使用權
- 少了主機的資訊安全管理
- 學校配合向上集中後，核定為D級



還有那些資訊系統？

- 人事室-雲端差勤系統 (雲端)
- 主計室-校務基金請購系統
- 文書組-公文線上簽核系統 (雲端)
- 圖書館-圖書查詢系統

具資訊系統後臺管理權限的人員被定義為「**資通安全專職（責）人員以外之資訊人員**」，除每年3小時資通安全通識訓練時數，每二年要有額外3小時的專業訓練時數

- 權責劃分：
  - 主機架設在校內，需負責資訊安全管理 (資安管理困難，應避免)
  - 建置在雲端，僅具有使用權或後臺管理權限 (但應做好委外廠商管理)

上級頒佈校園資安相關規定

學校網頁－校內資安訊息

- 學校使用資通系統或服務蒐集及使用個人資料指引 中華民國114年2月5日臺教國署資字第1140011715號文
- 學校使用生物特徵辨識技術個人資料保護指引 中華民國114年2月5日臺教國署資字第1140011715號文
- 行政院及所屬機關（構）使用生成式AI參考指引 中華民國112年11月08日臺教國署資字第1120155540號文
- 資通訊產品帳號權限與密碼管理原則 中華民國112年8月30日臺教國署資字第1120116472號文
- 資訊安全防護宣導資料 中華民國113年1月25日臺教國署學字第1130004579號文
- 教育體系電子郵件服務與安全管理指引 中華民國113年10月7日臺教國署資字第1130118624號文
- 臺灣學術網路兒少不當資訊資訊防護機制 中華民國114年2月25日臺教國署資字第1146500102號文
- 禁用大陸品牌資通設備及軟體 中華民國115年4月16日臺教國署資字第1156500191號文
- 公務出國（含大陸地區、香港及澳門）資通訊設備管理須知 中華民國115年7月14日臺教國署資字第1150066079號文

校內應遵循之資安相關規定

學校網頁－校內資安訊息

- 每年至少3小時資通安全教育訓練(研習)
- 資訊安全政策
- 校內人員資訊安全守則
- 個人電腦自我檢查表
- 推動開放文件格式ODF
- 公務信箱電子郵件使用說明
- 校內 Google 帳號使用說明
- 社交工程演練及防範

資通安全 - 校內所有同仁應盡責任

- 了解「學校資通安全政策及目標」
- 完成「每年3小時資通安全通識教育訓練」
- 知悉並遵守「校內人員資訊安全守則」
- 遵守「個人資料保護法」
- 了解「資安事件通報及應變辦法」
- 注意個人資安及資料保密
- 通過「教育雲電子郵件帳號社交工程演練」
- 使用「開放文件格式ODF」

請勿使用大陸品牌資通訊產品連接校內網路Wifi，如手機、平板、筆電、智慧型手錶…

資通安全 - 行政同仁及兼行政教師

- 除了前一頁「所有教職員工」應遵守事項外，還有
  - 電子郵件公務信箱使用「教育雲電子郵件」
  - 採購資通相關設備時請注意「禁用大陸廠牌」
  - 使用開放文件格式ODF(公文、網頁)
  - 個人資安防護 (電腦、文書資料...)
    - 個人行政電腦自我檢查 (每年1次)
    - 網頁公告內容自我檢核 (公告前，及每年2次定期檢查)

機敏資料不可使用Line等社群軟體傳送

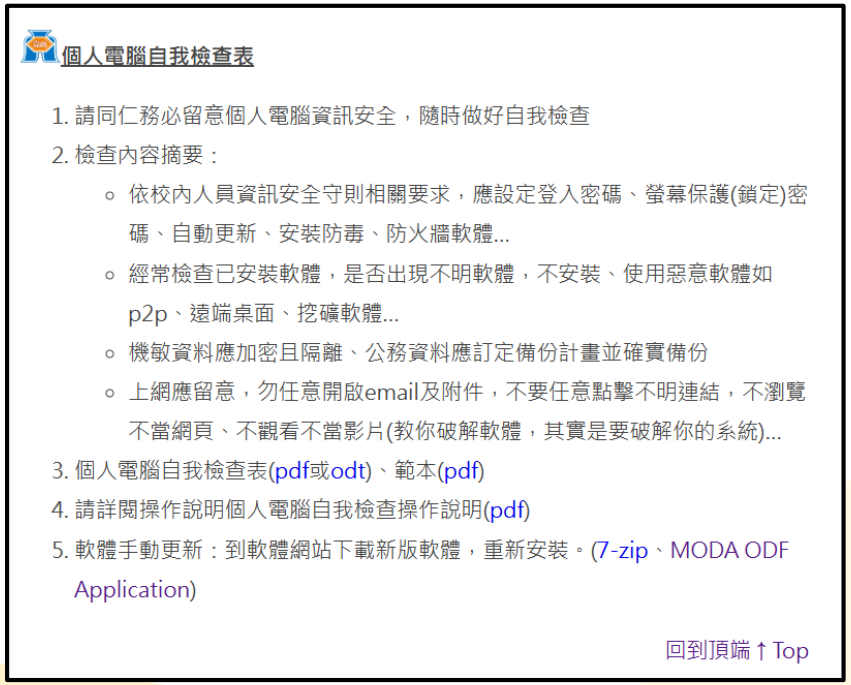
使用email傳遞時務必加密、密碼另外通知

每年至少3小時資通安全教育訓練(通識)

- 以年度計算
  - 1月1日-12月31日
- 負責校內資通系統的同仁每2年要有額外3小時的專業時數

個人電腦自我檢查表

- 簡列17列檢查項目
  - 登入密碼、螢幕鎖定密碼
  - 電腦安全性相關設定
    - 作業系統更新、關閉Autorun 、關閉不必要的帳號(Guest)
    - 關閉資源共用、杜絕SMB漏洞、遠端桌面、
    - 設定瀏覽器安全性、關閉郵件預覽
  - 軟體檢查
    - 安裝並啟用防火牆、防毒軟體
    - 常用軟體更新、版本檢查
    - 杜絕惡意軟體、未授權軟體
  - 資料保全：機敏資料、資料備份



個人電腦自我檢查表

1. 請同仁務必留意個人電腦資訊安全，隨時做好自我檢查
2. 檢查內容摘要：
   - 依校內人員資訊安全守則相關要求，應設定登入密碼、螢幕保護(鎖定)密碼、自動更新、安裝防毒、防火牆軟體...
   - 經常檢查已安裝軟體，是否出現不明軟體，不安裝、使用惡意軟體如p2p、遠端桌面、挖礦軟體...
   - 機敏資料應加密且隔離、公務資料應訂定備份計畫並確實備份
   - 上網應留意，勿任意開啟email及附件，不要任意點擊不明連結，不瀏覽不當網頁、不觀看不當影片(教你破解軟體，其實是要破解你的系統)...
3. 個人電腦自我檢查表(pdf或odt)、範本(pdf)
4. 請詳閱操作說明個人電腦自我檢查操作說明(pdf)
5. 軟體手動更新：到軟體網站下載新版軟體，重新安裝。(7-zip、MODA ODF Application)

回到頂端 ↑ Top

對外公開文件(含公文)符合 ODF

- 公務機關從文件製作、保存均以開放文件格式(ODF)處理
  - ODF-CNS15251

- 數位發展部
  - https://moda.gov.tw/digital-affairs/digital-service/app-services/248
  - 現改為MODA Application Tools

- 建議安裝軟體
  - 上述ODF文件應用工具 (**MODA Application Tools**)
  - 或 Libre Office

對外公開文件(含公文)符合 ODF

- 基本原則：使用開放格式，而不是商用格式

- 公開文件(網頁下載/公當)或公務文件(公文附件)
  - 不需要被編輯者，以 PDF 格式為主
  - 需要編輯/填寫資料，以 ODF 為主，如odt、ods

- 許多自由軟體支援ODF，建議用**MODA** Application Tools
  - **Word 可以另存 PDF**，格式沒問題
  - Word 可以另存 odt，但格式版本不對 (不建議用 word 另存 odt)
    - 別人開啟檔案時，排版會亂掉 (造成別人困擾)
  - 請**用Writer開啟.docx檔，再另存為.odt**，這樣比較不會有格式問題

ODF文件類型說明

- ODF不是單一檔案格式，而是統稱，下表臚列相關文件及副檔名
  - **.odt for Text**
  - **.ods for Spreadsheet**
  - **.odp for Presentation**
  - .odg for Graphics

軟體	ODF 軟體	ODF 副檔名	MS Office 軟體	MS Office 副檔名
文書處理	**Writer**	.odt	**Word**	.doc .docx
試算表	Calc	.ods	Excel	.xls .xlsx
簡報	Impress	.odp	Power Point	.ppt .pptx
其他類別檔案： PDF 可攜式文件格式 ZIP 壓縮檔				

公務信箱改用教育雲端電子郵件

- 依據行政院秘書長106年1月12日院臺護字第1050190287號函：「為防止公務資料外洩，各機關同仁應使用機關配發之電子信箱收發公務所需資訊，不得使用非公務信箱進行公務郵件收發。」

- 校內教職員工及學生申請 Google Workspace郵件(@cyvs.cy.edu.tw)，屬非公務信箱，**不得傳送公務郵件**(非公務內容仍可繼續使用)
  - 教師、學生除個人使用外，主要做為Google Classroom 遠距線上教學用

- 國教署建議各校採用「教育雲校園電子郵件」為公務信箱。
  教育雲端電子郵件網址https://mail.edu.tw/ 需自行申請。

行政同仁應使用 mail.edu.tw 處理公務信件

資安事件要如何通報？

- 國立嘉義高級商業職業學校資通安全事件通報及應變管理程序
- 資安事件應變措施
  - 事前防護
  - 聯絡窗口：圖書館陳建文 分機140
  - 事件分級：一、二、三、四級，三、四級為重大事件
  - 一、二級於 72 小時完成應變程序，三、四級於36小時內完成
  - 至教育機構資安通報平台填報資安事件處理辦法及完成時間

- **同仁責任：**
  遇到資安事件或可疑事件，請先通報。

政府為什麼要禁用大陸品牌資通產品？

- 只管得到政府機關，管不到一般民眾

- 資通設備：資訊+通訊設備，能連網的都是
  - 資料的存取、傳遞都會經過資通設備
  - 你的資料會被送到哪裡？合理嗎？應該嗎？

- 大疆空拍機，又便宜又好用，市佔率高，不能用真可惜？
  - 思考：為什麼大陸的攝影、監視器好用呢？

我的小米/華為/oppo手機可以帶來學校用吧？

- (手機、平板、筆電、智慧型手錶...都在討論範圍內)
  - Lenovo

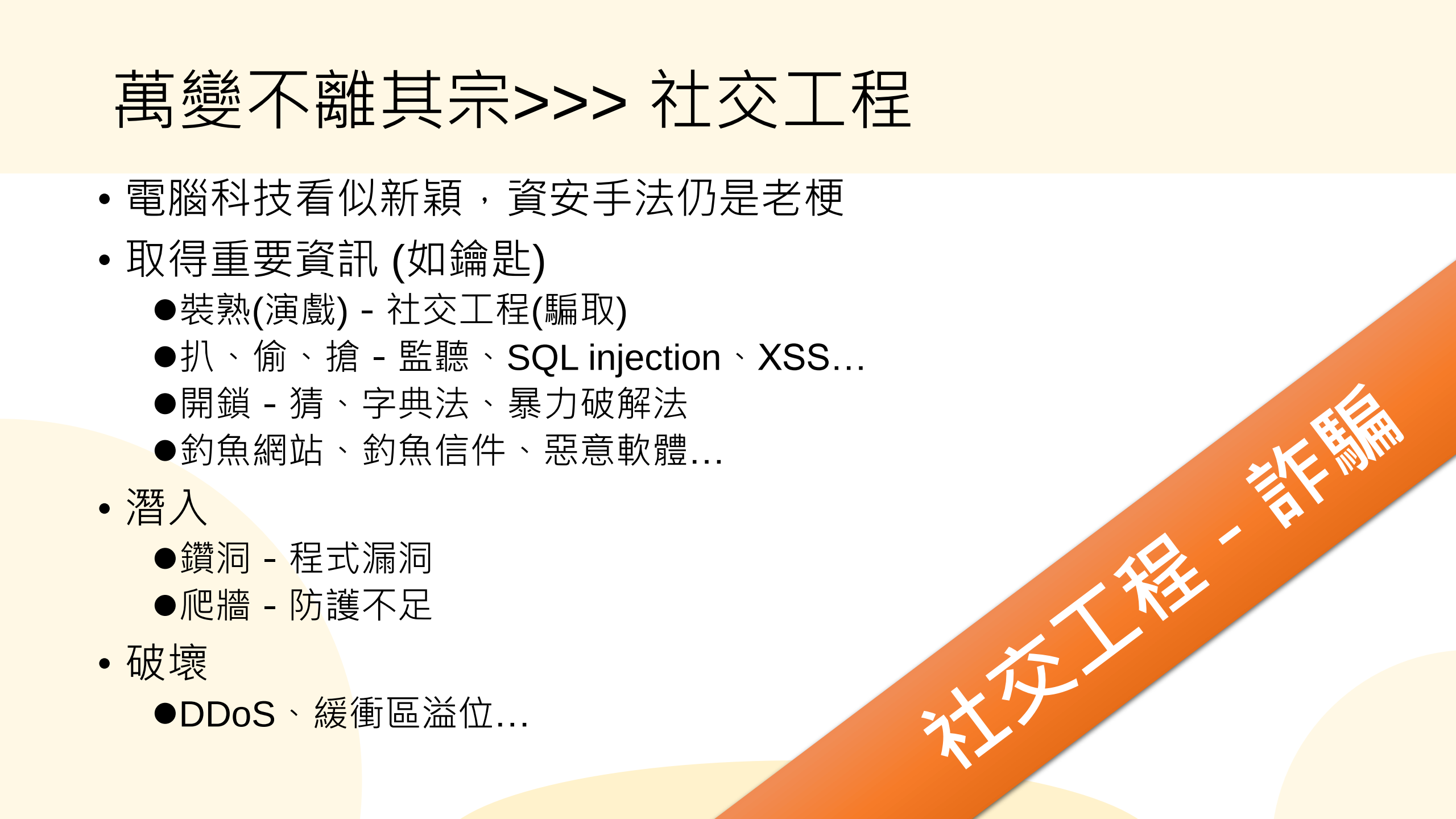
- 如果你沒有使用(連接)學校的網路(WiFi及有線)
  - 可以，但其實還是有風險(WiFi熱點蓋台攻擊...)
  - 查核不易，但有連上WiFi、有開熱點還是查得到的

- 有什麼風險嗎？
  - 使用學校WiFi，如果你的「手機」有問題，就會成為「滲透工具」
  - GPS定位，可能透漏學校的機密地點(好吧...學校沒有這種東西)
    - 即使你沒開GPS定位，還有AGPS、基地台...等
  - 其他 ~~(就是我也不知道的高科技)~~

社交工程演練

萬變不離其宗>>> 社交工程

- 電腦科技看似新穎，資安手法仍是老梗
- 取得重要資訊 (如鑰匙)
  - 裝熟(演戲) - 社交工程(騙取)
  - 扒、偷、搶 - 監聽、SQL injection、XSS…
  - 開鎖 - 猜、字典法、暴力破解法
  - 釣魚網站、釣魚信件、惡意軟體…
- 潛入
  - 鑽洞 - 程式漏洞
  - 爬牆 - 防護不足
- 破壞
  - DDoS、緩衝區溢位…



資安影片

- 【TWCERT/CC】社交工程因應之道(6'03)
  - https://www.youtube.com/watch?v=XNg8WNByShs

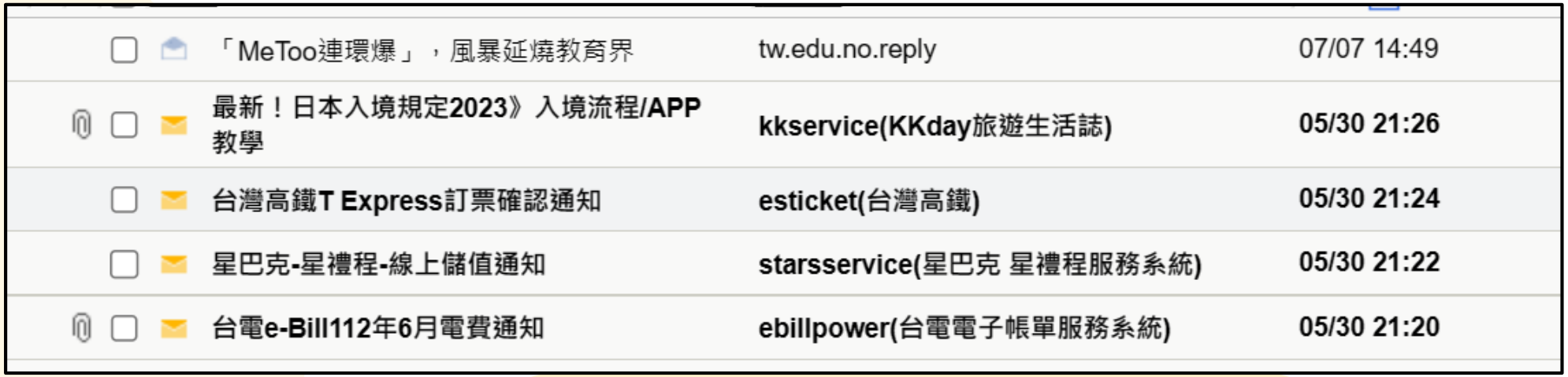
社交工程演練，那是什麼？

- 國教署於5月至11月期間辦理社交工程演練(全校至少抽出35位)
- 辦理方式以E-mail信件為主，請留意email信件

一、不點開信件：信件開啟率。

二、不點擊連結。

三、不開啟附件。



「MeToo連環爆」，風暴延燒教育界	tw.edu.no.reply	07/07 14:49
最新！日本入境規定2023》入境流程/APP教學	kkservice(KKday旅遊生活誌)	05/30 21:26
台灣高鐵T Express訂票確認通知	esticket(台灣高鐵)	05/30 21:24
星巴克-星禮程-線上儲值通知	starsservice(星巴克 星禮程服務系統)	05/30 21:22
台電e-Bill112年6月電費通知	ebillpower(台電電子帳單服務系統)	05/30 21:20

演練內容

- 時程：自本(115)年5月至11月止，期間辦理2次演練。
- 對象：全校所有教職員工(隨機抽)
  - 教育雲電子郵件帳號 XXX@mail.edu.tw
- 目標：
  - 社交工程郵件**開啟率**應低於10%(含)
  - 社交工程郵件**點閱率**應低於6%(含)
  - 社交工程郵件**附件開啟率**應低於2%(含)

- 今年已完成第1梯次演練，已知有同仁點擊信件連結及附件
- 11月初會有第2梯次演練，請同仁務必提高警覺

一般注意事項：

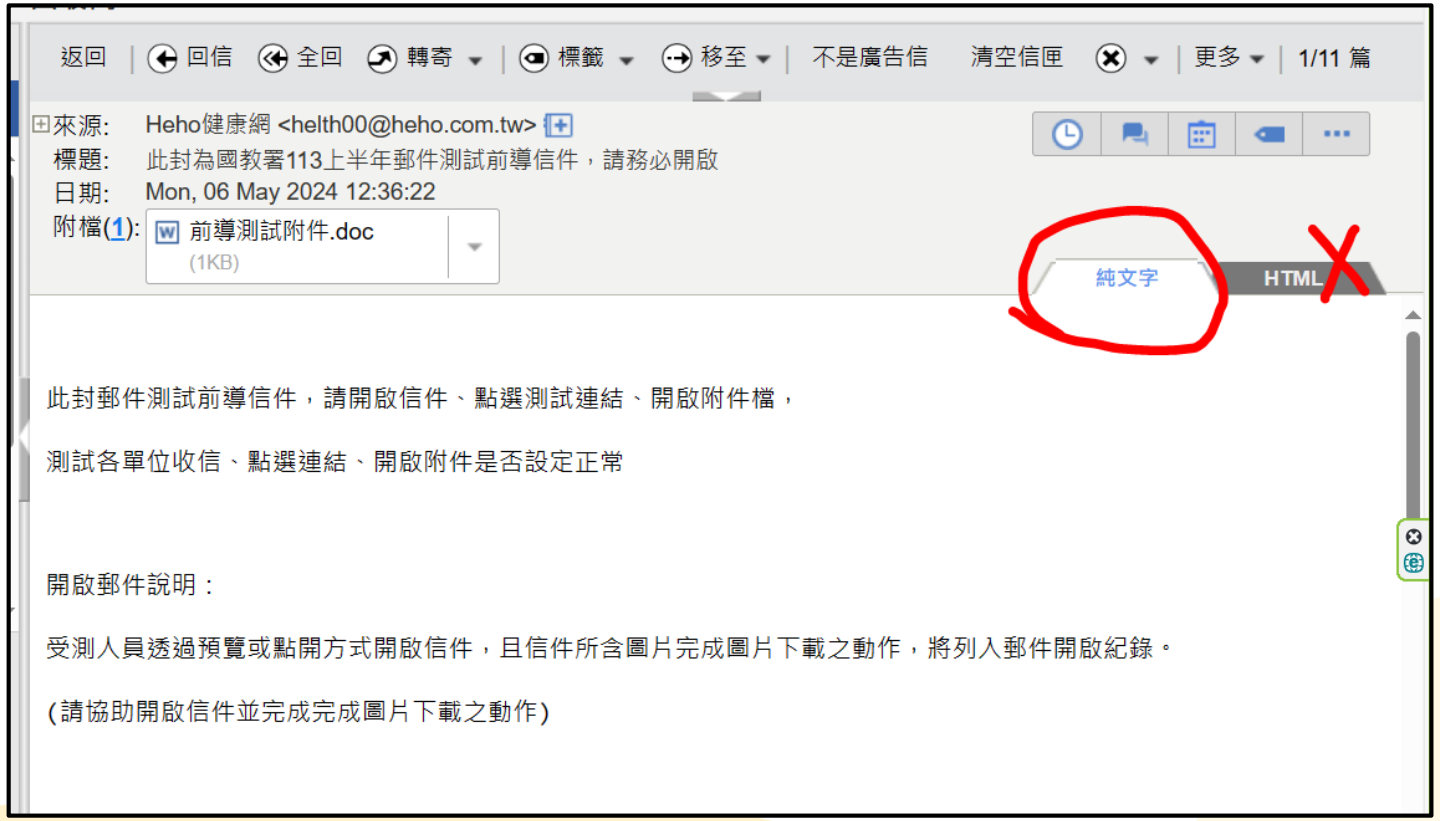
- 三不：不開郵件、不點連結、不下載附檔
- 收到信時，不要直接開啟
  - 先想一下是否應該收到此類型信件。
- 儘量不要使用教育雲端電子郵件收發非教學/學校事務之信件
  - 不要留郵件地址給其他網站...
- 手機收信，勿使用iPhone內建收信App，避免信件開啟誤判
  - 教育雲端電子郵件使用Apple手機收發信件時，請安裝Maill2000 App
- 郵件軟體，設定不【預覽】郵件內容，以純文字檢視
  - 降低風險

惡意電子郵件的危險觸發因子

- 底下內容可能隱藏有惡意程式，造成風險
  - 圖片 (內藏惡意程式)
    - 設定預設不顯示圖片
  - 附檔 (惡意程式)
    - 不要開
  - HTML內容 (執行惡意程式)
    - 設定以純文字模式顯示信件
  - 連結 (執行惡意程式)
    - 不要點
  - 不顯示【預覽窗格】
    - 預覽時已經開啟

最重要的實務操作-純文字、不顯示圖片

- 很不小心就會打開郵件 (目標1失敗)
- 以純文字模式開啟
  - 不會看到圖片
  - 不會看到連結
- 設定不顯示圖片

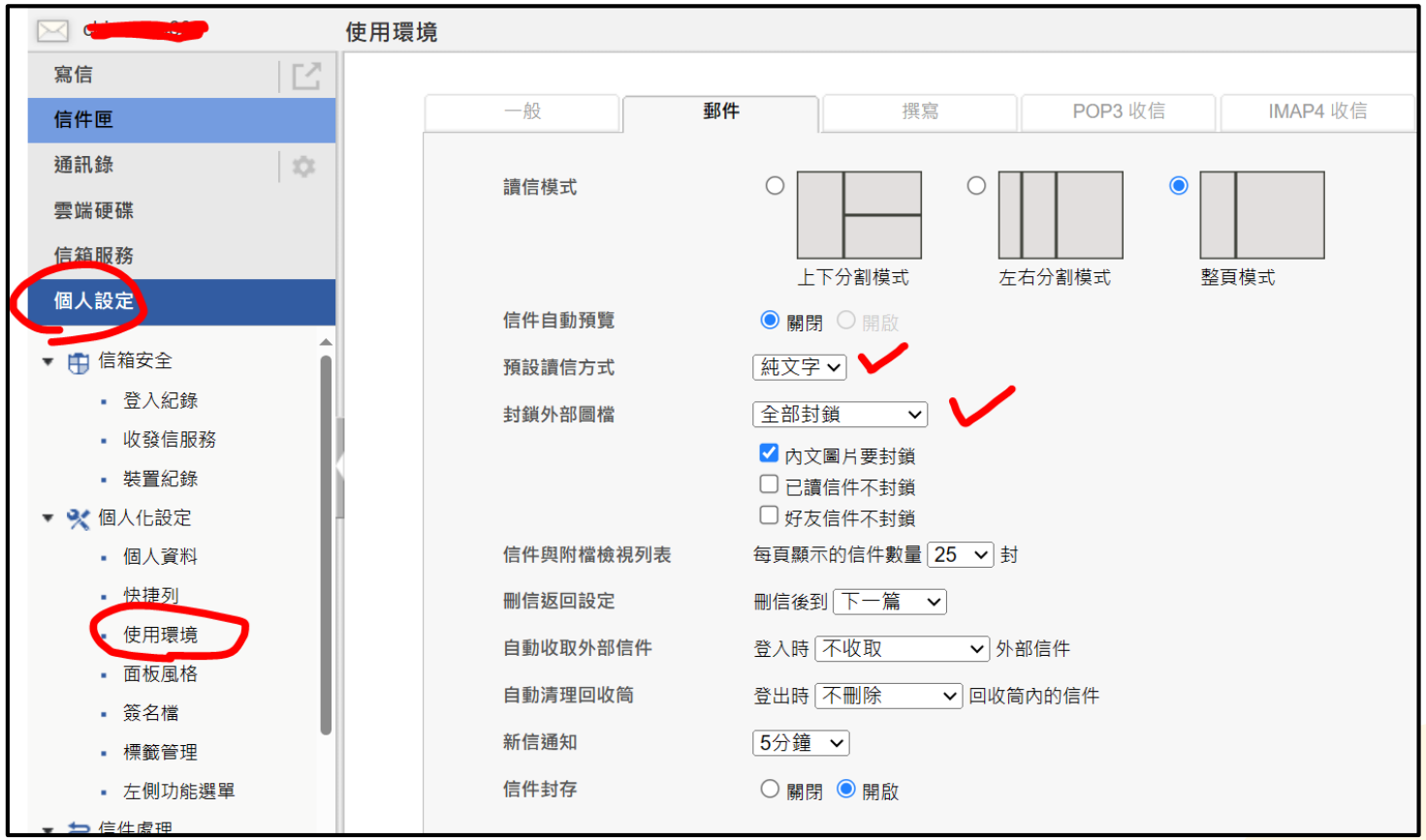


以純文字、不顯示圖片來檢視郵件

- 只有純文字內容，不具程式執行能力，風險低
  - 防止HTML內容含惡意程式
  - 做為初期判斷，確認沒問題再啟用HTML模式
  - 但是比較醜
- 啟動HTML模式後，還是不顯示圖
  - 防止圖片內含惡意程式
  - 圖片預設不顯示，確認沒問題再顯示圖片
  - 也是醜
- 誤開信件很難避免，但如果有上述兩項保護措施，就能降低風險

教育雲端電子郵件電腦版環境設定

- 其餘gmail、手機、outlook等收信程式的相關設定，請上網搜尋
- 重點是
  - 以純文字顯示
  - 關閉預覽功能
  - 不顯示圖片
  - 不自動下載圖片
- 其他
  - 更新、防毒、備份



參考別人的設定教學畫面 https://socialengineering.email.nchu.edu.tw/ (國立中興大學計算機及資訊網路中心 製作)

電子郵件的安全設定

- 設定以【純文字】檢視
  - 確認無誤後，再切換HTML (習慣後，大多不需要了)
- 設定【不要自動顯示圖片】
  - 確認無誤後，再自行開啟/檢視圖片
- 設定【不要顯示預覽信件窗格】
  - 預覽時，其實就是開啟了
- 設定【不要自動下載附件】

只是開啟電子郵件，也會出事嗎？

- 信件內容的格式如果是HTML，其中可能包含程式碼(JavaScript)或圖片
- 圖片也會有事？
  - 圖片可能隱藏資訊，Steganography(圖像隱碼)
  - https://blog.trendmicro.com.tw/?p=12510
  - 當電腦/手機讀取圖檔並顯示的時候，會觸發程式內容
- 設定【純文字】的讀信模式
  - 很醜、排版混亂
  - 確認不是惡意信件，再開啟HTML模式

點選連結以獲得更進一步的資訊？

- E-mail、簡訊、Line、留言區...常有一些有趣的連結
  - 可以點嗎？
  - 有風險嗎？為什麼
- 連結可能會
  - 執行【惡意程式碼】
  - 可能會下載安裝【木馬程式】
  - 可能會連到【釣魚網頁】
- 目的
  - 騙取個資、帳密...
  - 取得手機/電腦的控制權限(遠端操控)，然後想做什麼都可以

網路連結 - 點下去

你以為會連到官網

CYVS Web

嘉義高商
連結點下去

其實是釣魚網站

CYVS Web

嘉義高商
連結點下去

不明連結，可能跳轉至其他網站，可能執行惡意指令

網路連結 - 點下去

- 不明連結不要點
  - 晚點比早點好

- 不要任意輸入「帳號/密碼」
  - 有加密嗎？(https)
  - 是這裡嗎？(釣魚網站)
  - 有必要嗎？

- 【詐騙大百科】簡訊篇 (上)｜釣魚簡訊滿天飛！如何判斷連結是否安全？
  - https://whoscall.com/zh-hant/blog/articles/241

- 台灣首例！男子架設假基地台發送詐騙簡訊　NCC重罰400萬元不排除再罰
  - https://www.storm.mg/article/4850867

電子郵件有一個abc.exe的附檔，可以開嗎？

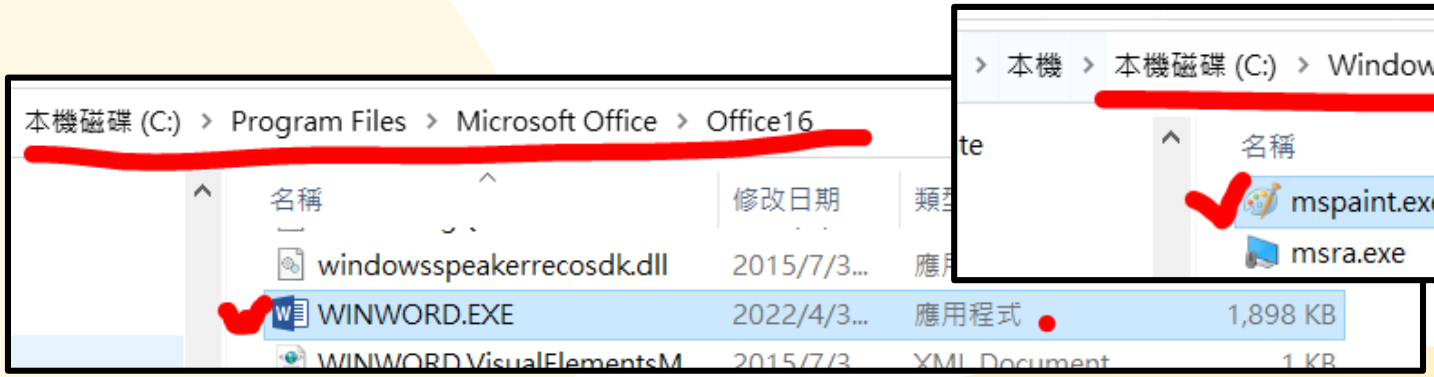
- 官方說法：千萬不要

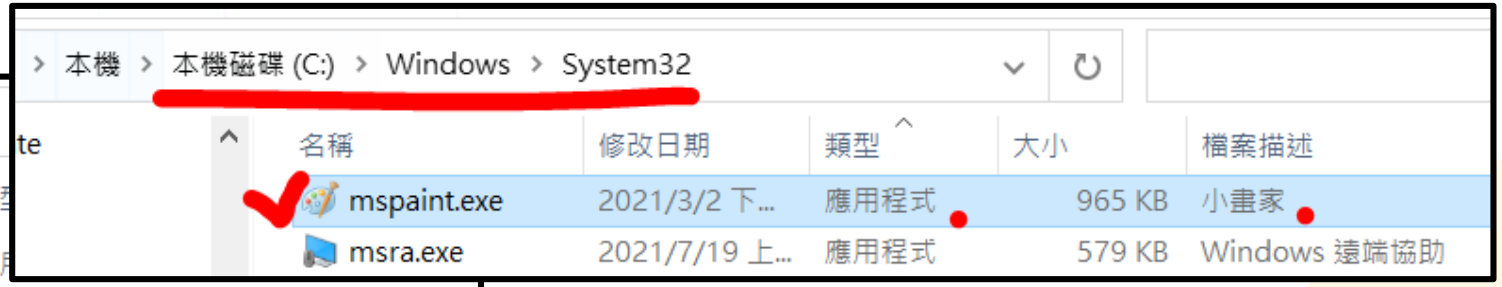
- 那如果是spicy.jpg呢？
  - 官法說法：不要開
  - 大眾說法：不開怎麼知道辣不辣？

- 對於圖片，gmail是有些保護措施的，至於exe檔，gmail根本不允許你寄exe類的檔案，但有些郵件系統則沒有限制...

了解電腦檔案

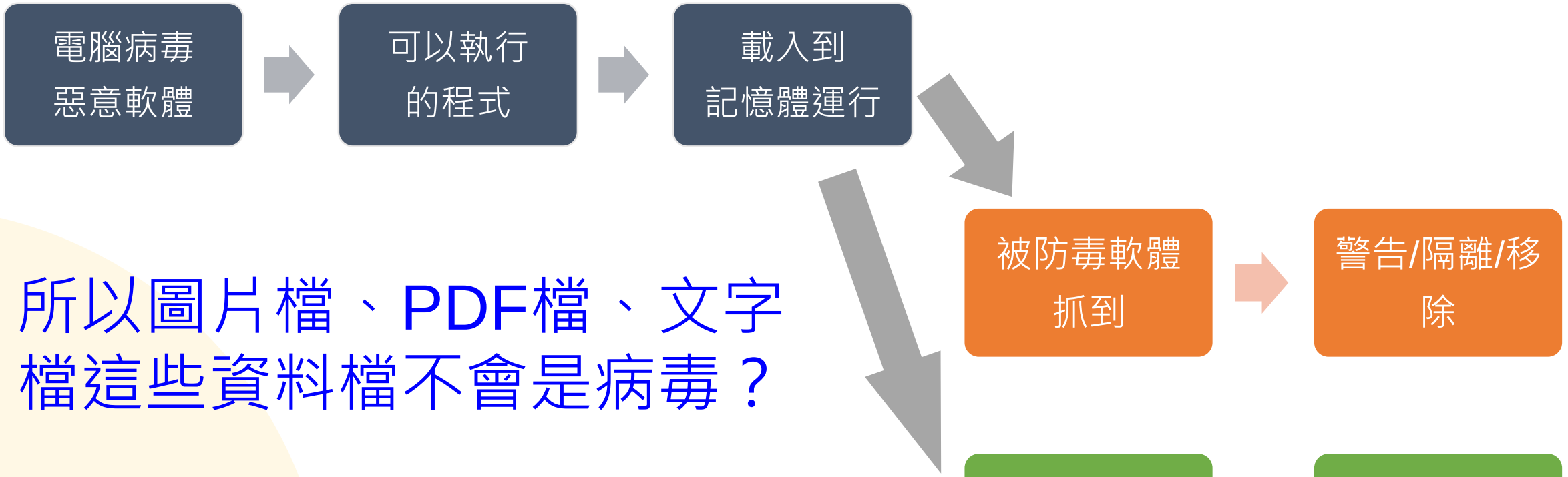
- 電腦內的檔案簡單來講有兩大類
  - 執行檔，應用程式，依程式設計可做的事情很多
  - 資料檔，儲存資料的檔案，就是單純記錄資料
- 使用特定的應用程式來處理資料檔案
- 用小畫家(mspaint.exe)來開啟圖片檔案(.jpg)
- 用winword.exe來開啟.docx檔案





防毒軟體的運作 – 電腦病毒

這裡指的病毒可擴大為惡意軟體
因為有些防護軟體功能滿強大的

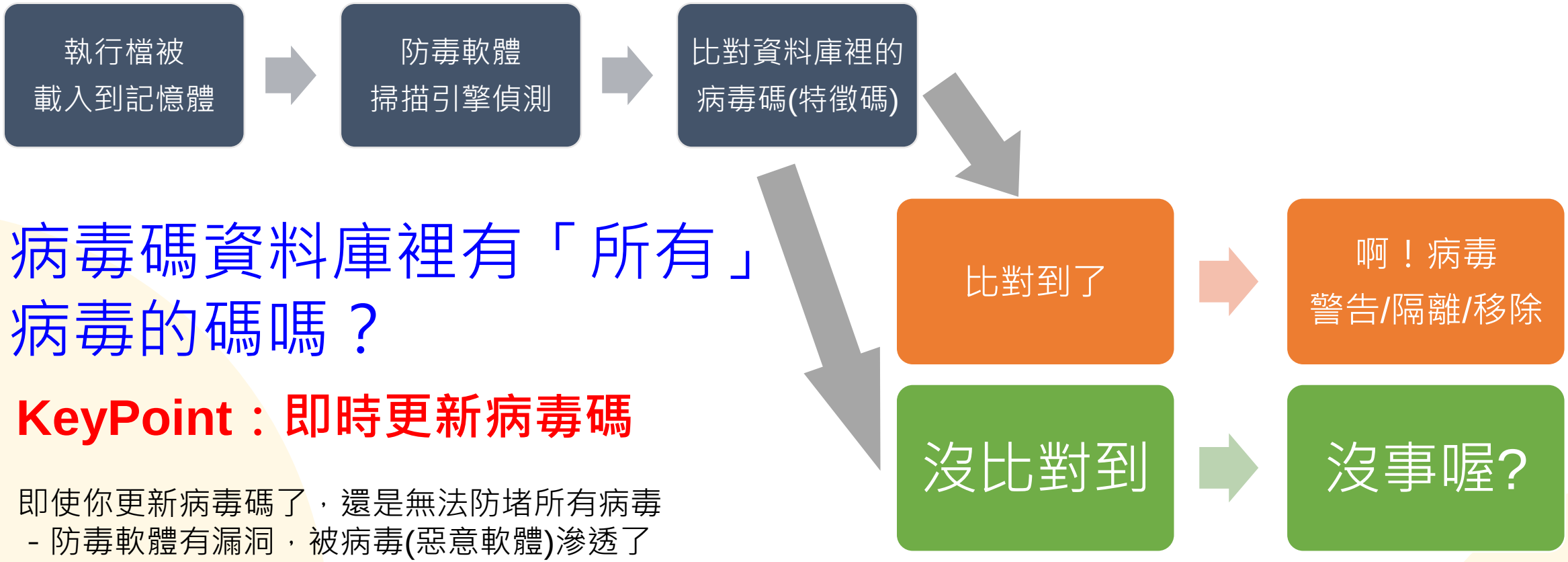


所以圖片檔、PDF檔、文字檔這些資料檔不會是病毒？

KeyPoint：執行檔可能被偽裝成資料檔

比如，電子郵件附檔看到abc.pdf，你以為是文件檔，但可能是偽裝的執行檔(木馬、病毒…)

防毒軟體的運作-掃描引擎與病毒碼



病毒碼資料庫裡有「所有」病毒的碼嗎？

KeyPoint：即時更新病毒碼

即使你更新病毒碼了，還是無法防堵所有病毒
- 防毒軟體有漏洞，被病毒(惡意軟體)滲透了
- 變種病毒會改變自己造成特徵碼的變異

...

被偽裝的檔案？

- 大家都認識小畫家 mspaint.exe
  - 但是小畫家是真正的小畫家嗎？
- 如果病毒將自己偽裝成小畫家或依附在小畫家裡
  - 使用小畫家時，其實是執行病毒程式！
- 你在某官網下載了一個好用的應用程式
  - 那是真的官網嗎？ (釣魚網站？)
  - 官網有沒有被駭客竄改過？ (真實案例)
- 你在email附件中看到一個PDF或JPG檔
  - 檔案的圖示是可以改的
  - abc.jpg.exe 因為隱藏副檔名的關係，看到的是abc.jpg
  - PDF檔案夾帶Word、Excel，而Word、Excel可能有巨集病毒
  - 圖像隱碼 Steganography

進階技能：防竄改- 雜湊 md5、sha256

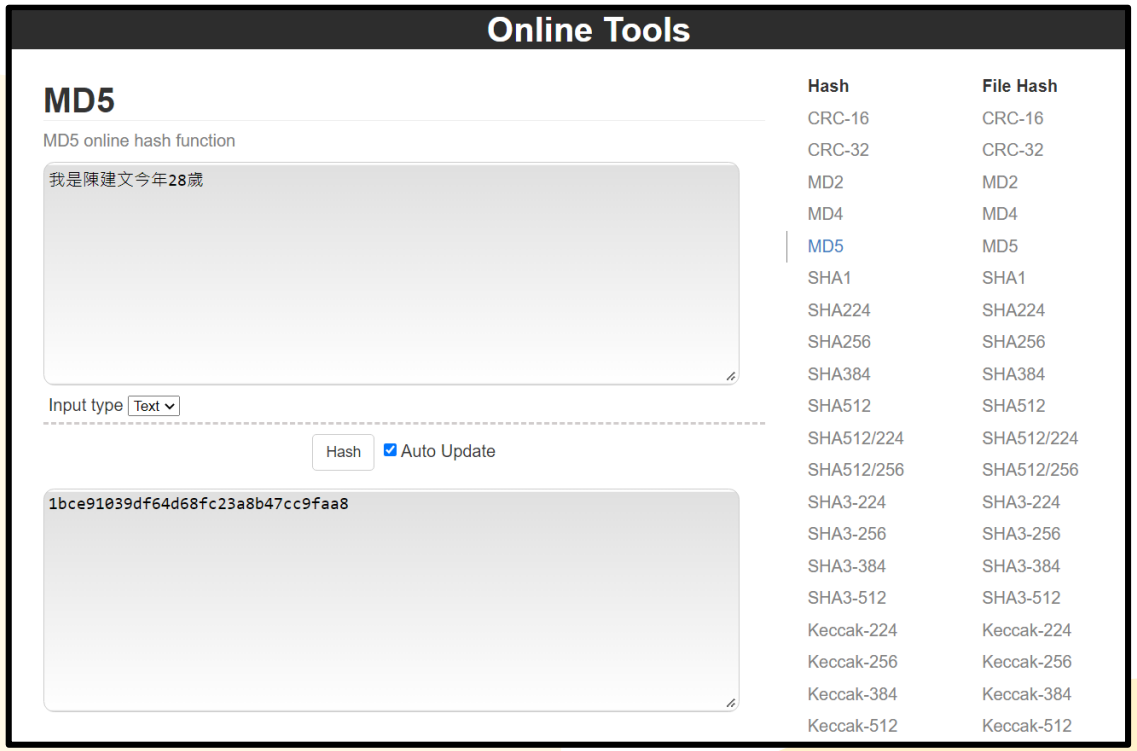
- https://emn178.github.io/online-tools/

檔案
或資料

雜湊函數運算

雜湊值
通常是16進位

雜湊演算法也是【數位簽章】中重要的一份子



MD5 online hash function

我是陳建文今年28歲

1bce91039df64d68fc23a8b47cc9faa8

偷偷改一下資料內容

MD5 online hash function

我是陳建文今年18歲

c05a1d3f529224140761f4da4ad9d30a

只要資料有任何變動，
得到的雜湊值就會有明顯的變化

電子郵件的安全設定

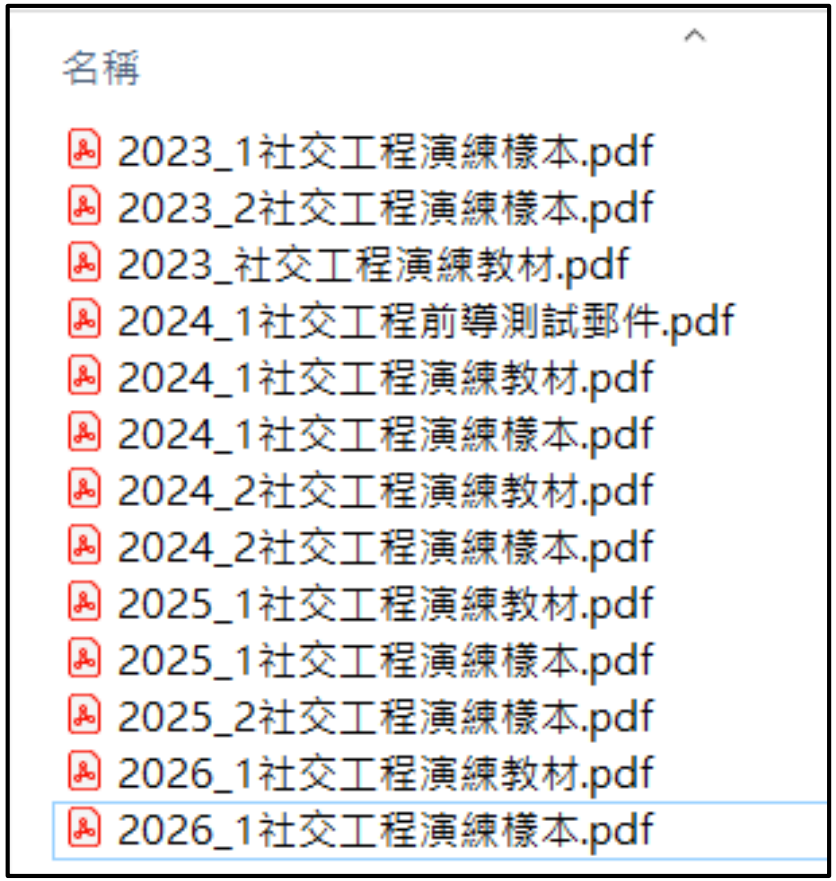
- 設定以【純文字】檢視
  - 確認無誤後，再切換HTML (習慣後，大都數不需要)
- 設定【不要自動顯示圖片】
  - 確認無誤後，再自行開啟/檢視圖片
- 設定【不要顯示預覽信件窗格】
  - 預覽時，其實就是開啟了
- 設定【不要自動下載附件】
- 管好大腦及手，別亂點連結、開附檔

不要將教育雲電子郵件
自動轉寄到gmail，
容易降低警覺而誤開信件
手機收信請安裝Mail 2000 APP

參考別人的設定教學畫面
https://socialengineering.email.nchu.edu.tw/
(國立中興大學計算機及資訊網路中心 製作)

國教署社交工程演練樣態

- 國教署不給公告在網路中
- 研習時可以拿出來討論一下



資安通識

資安概念-零信任

- 我只是看看影片，不會中毒吧
- 我只是下載免費軟體，應該沒關係吧
- 那是小明寄來的信，我當然要看啊
- 都合作那麼多年的廠商了，沒問題吧
- Line群裡都是朋友，不會有人外洩吧
- 我只是去上個廁所，不會有人偷用我電腦吧
- 我門都上鎖了，不會有小偷吧？

物聯網 – 萬物皆連網

這台機器的作用是？

監視別人

還是讓別人監視你？

http://www.insecam.org/

物聯網 – 不安全的設備

- 為了維護方便，所以留下後門
- 為了設定方便，所以使用「單一預設密碼」 或 「密碼留空白」
- 設計不良，留下漏洞
- 降低成本，無法更新
- 殭屍網路生力軍，量大、好駭、又不會引起注意

物聯網
還是
勿連網

密碼 Q & A – 暴力破解1

- 什麼是暴力破解法？
  - 把所有可能性，全都試過一次
- 那什麼方式可以防止暴力破解？
  - 在被破解之前，換掉密碼，再加上一些運氣
- 所以密碼
  - 要夠長
  - 要複雜
  - 要常改
  - 拒絕反覆嘗試

只要是密碼，暴力破解一定能解開

關鍵：解得快不快？

密碼 Q & A – 暴力破解2

- 暴力破解要快？
  - 雲端運算：多部機器運算
    - 如何取得大量的運算資源
  - 量子電腦：聽說現有密碼技術都無法阻止
    - 目前量子電腦還在研究階段？

- 如果你是駭客，你會選擇暴力破解嗎？

- 還是：直接取得密碼 或是 跳過密碼驗證

密碼 Q & A – 不是唯一辦法

- **破解 6 位數驗證碼!! 駭客如何入侵你的帳號? 漏洞技巧解析! | 在地上滾的工程師 Nic**
  - https://www.youtube.com/watch?v=CgKXyYDvtkk

  - 繞過破解密碼→重設密碼
  - 限速？
  - 有效期限
  - 不安全的-雲端服務供應商

- **專攻資安的白帽駭客帶你看懂：暗網是什麼？駭客也分黑白兩道？ | 名人專業問答 | GQ Taiwan**
  - https://www.youtube.com/watch?v=qnAbsuNW1Wc

密碼 Q & A – 不是唯一辦法

- 破解不了，可以跳過/繞過
  - 猜密碼
  - 重設密碼
  - 利用系統漏洞，直接取得權限
  - 社交工程，用騙的/偷的...

- 省思：
  - 前述密碼策略，有用但還是會衍生問題
    - 會忘記
    - 或反覆使用同一密碼
    - 密碼管理工具？

生物特徵辨識？

密碼撞庫攻擊Credential Stuffing Attacking

- 網站A的帳號/密碼外洩了
- 網站B也發現了相同的帳號？

- 那網站C、D、E...呢？有沒有重要的系統呢？

無密碼驗證

- 多因子認證
  - What you know：密碼/PIN碼/外遇次數
  - What you have：手機/健保卡/硬體金鑰
  - Who you are：指紋/臉

- 如何做「無密碼驗證」
  - 利用多因子認證
  - 綁定手機+手機指紋+OTP…
  - 重點：要事先設定…

突破三方認證機制

- 電信業者小額付款機制
  - https://aaaservice.hinet.net/User/AAA/serviceInfo.jsp

- 安全交易關鍵
  - 三方認證
  - 以認證碼進行授權
  - 認證碼每次隨機產生
  - 有開通此服務

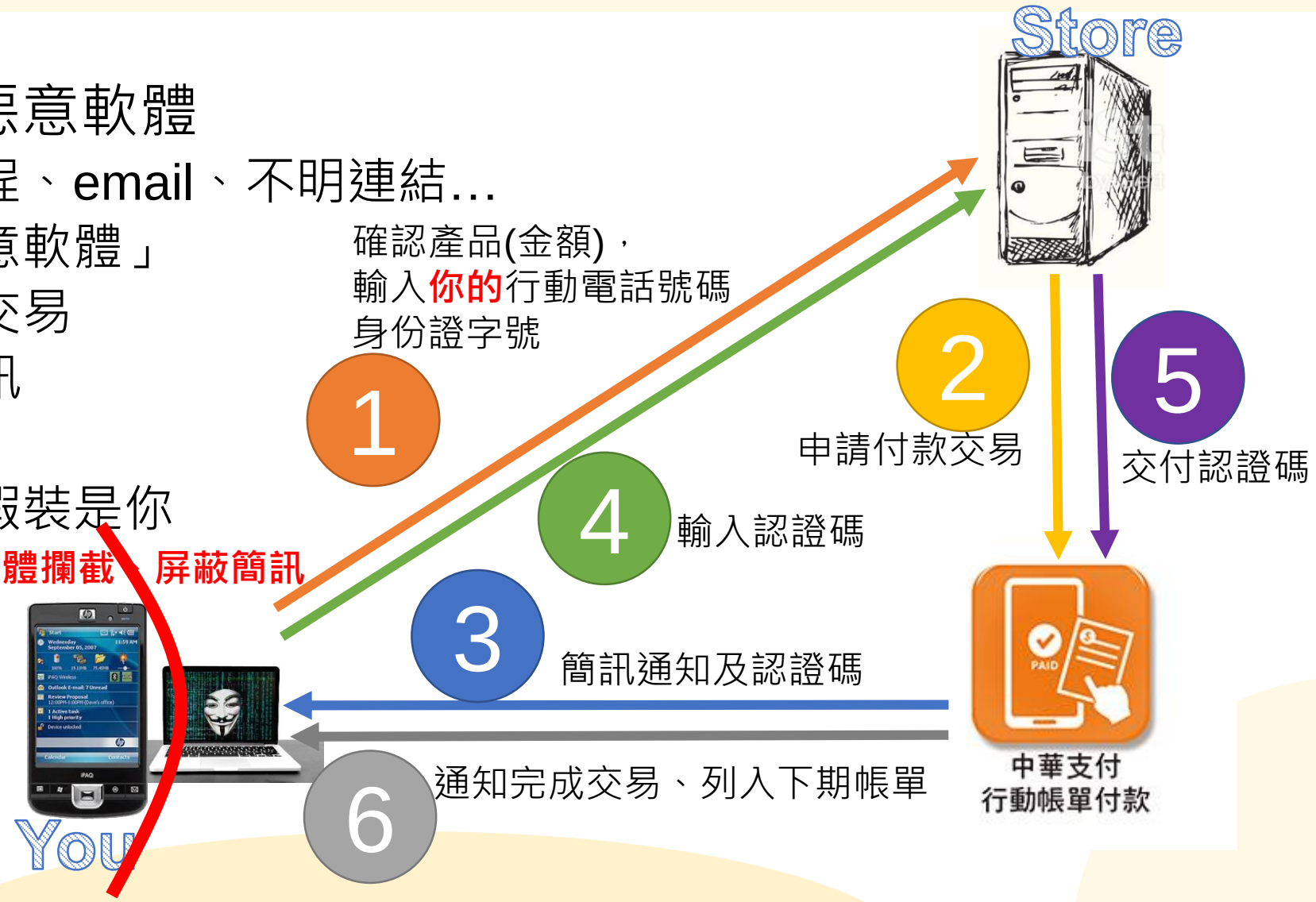
突破三方認證機制1

- 駭客突破口 - 認證碼
  - 取得個資、謊稱是你朋友
  - **你...相信了...我是你朋友**
  - 我手機壞了，請你幫忙一下
  - 借你手機號碼，店家傳認證碼
  - 你再告訴我認證碼
  - ...
  - 最後商品當然是
送到駭客指定位置

突破三方認證機制2

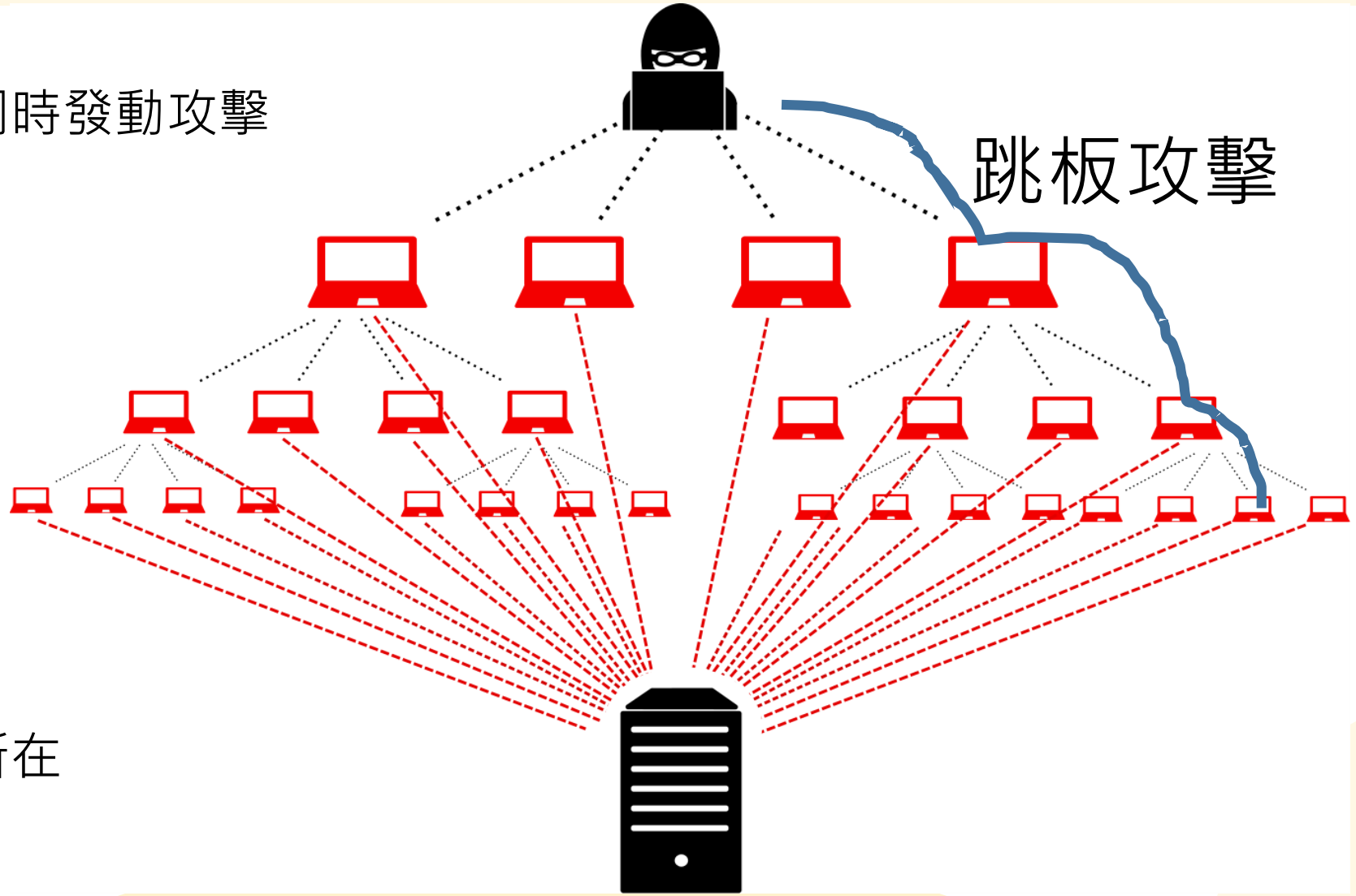
- 駭客突破口 - 植入惡意軟體
  - 釣魚手法、社交工程、email、不明連結...
  - 在你手機植入「惡意軟體」
  - 透過惡意軟體進行交易
  - 期間**攔截、屏蔽**簡訊

- 駭客透過惡意程式假裝是你
- 而你並不知道 **惡意軟體攔截、屏蔽簡訊**



攻擊手法 – DDoS 分散式阻斷服務

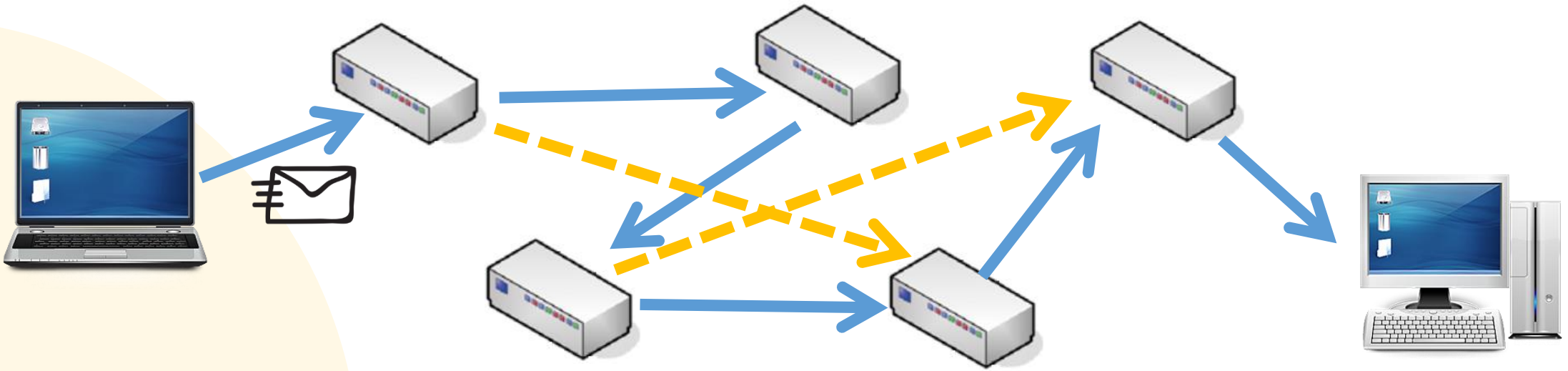
- 攻擊者
  - 操縱多個機器同時發動攻擊
  - 殭屍網路
- 被攻擊者
  - 網路頻寬被堵
  - 對外服務中斷
  - 機器硬體損耗
- 跳板攻擊
  - 不易反查駭客所在



網路通訊 – 資料(封包)傳遞

你以為資料是這樣傳的

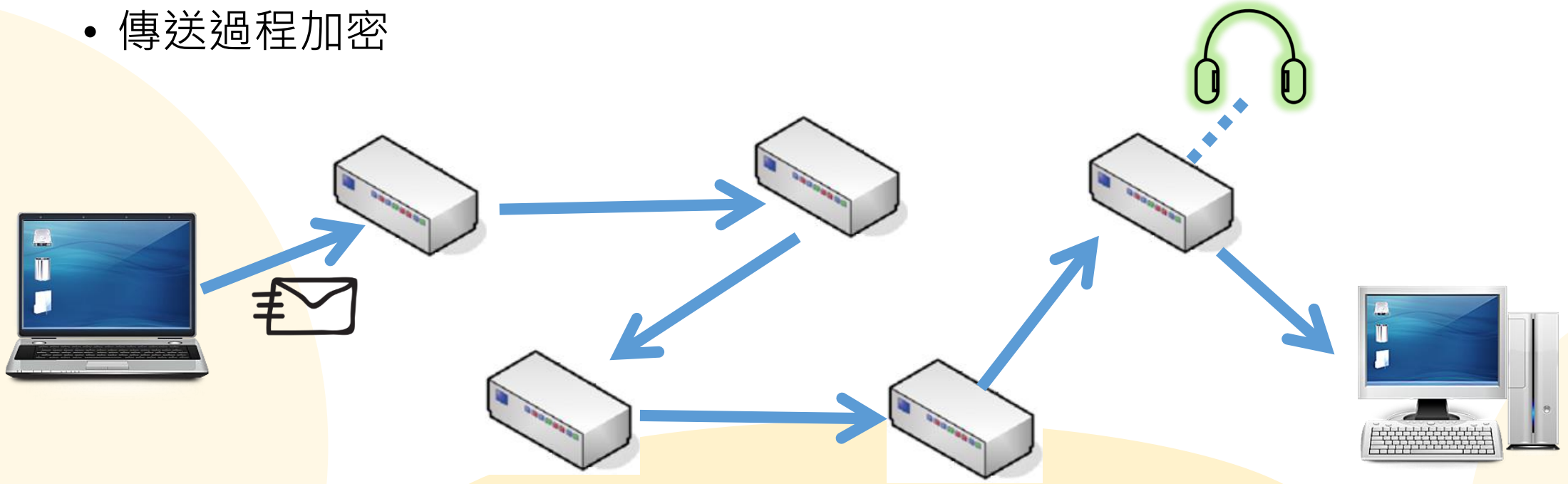
實際上是這樣傳的



➡中間會經過非常多的節點

網路通訊 – 資料(封包)傳遞

- 風險？
  - 中間如果有人監聽，甚至竄改
- 保全？
  - 傳送過程加密



攻擊手法 – MitM 中間人攻擊

你以為通訊是加密的

其實是別人幫你加的

網路交易 – 資料為什麼外洩

你的問題

木馬/側錄

Https加密了
But MitM

HTTP 沒有s
(沒加密傳輸)

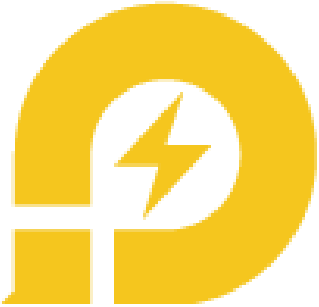
人為○○

廠商資安
防護不足

軟體下載

- 一律從官網下載
  - 小心！也有假官網(釣魚網站)

- 風險很高的行為
  - 中文化、破解版、優化版...
  - 宣稱「防毒軟體會誤判」，要求關掉
  - 手機程式以 APK 方式安裝
  - 電腦安裝手機模擬程式
  - 從非官網或不明連結下載

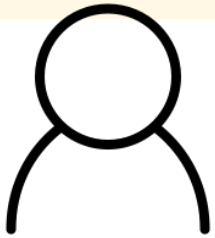


- 官網最好有提供 MD5 / SHA1 / SHA256 驗證碼

螢幕保護程式 / 鎖定畫面(密碼解除)

離開多久以後才鎖定畫面呢？

公用電腦 登出/ 安全瀏覽模式



登入

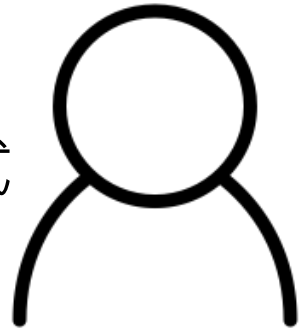
未登出就離開

還沒登入

擁有  的權限

公用電腦 登出/ 安全瀏覽模式

- Chrome
  - 無痕模式
- Edge
  - InPrivate 模式
- Firefox
  - 隱私瀏覽
- Safari
  - 私密瀏覽



使用無痕模式，也要記得關閉視窗

《資安漫畫》聚餐後,手機遺失了怎麼辦?

- https://blog.trendmicro.com.tw/?p=71917
- 摘錄自資安趨勢部落格
  - 臺灣知名趨勢科技公司建置
  - 推薦資安小百科

- 手機遺失緊急處理五步驟
  1.以其他裝置登入帳號,遠端確認手機位置
  2.遠端刪除登錄在手機內的信用卡資料
  3.到所屬電信業者辦理暫停通話或掛失
  4.變更社群網站等帳號的密碼
  5.持有手機的IMEI碼,到警局備案遺失

手機遺失緊急處理五步驟
/04/手機遺失07-2.jpg

LINE 安全性設定檢視宣導

- https://www.twcert.org.tw/tw/cp-15-4956-c8d26-1.html
- 摘錄自TWCERT/CC 資訊安全宣導
- 開啟Letter Sealing
  - 加密，保障對話雙方才能閱讀訊息
- 檢視【允許自其他裝置登入】
  - 其他人從電腦等其他裝置登入，如果只有使用手機Line，請關閉
- 檢視【登入中的裝置】
  - 如果允許自其他裝置登入，請隨時檢視是否有陌生機器登入...

相關資源

資通安全署
yber Security, moda

關於資安署 資安法規專區 業務專區 行政院國家資通安全會報 訐

公務機關資通安全業務績效評核

資安政策與法規

臺灣電腦網路危機處理暨協調中心

臺灣學術網路危機處理中心TACERT

- https://cert.tanet.edu.tw/

NICS

國家資通安全研究院
National Institute of Cyber Security

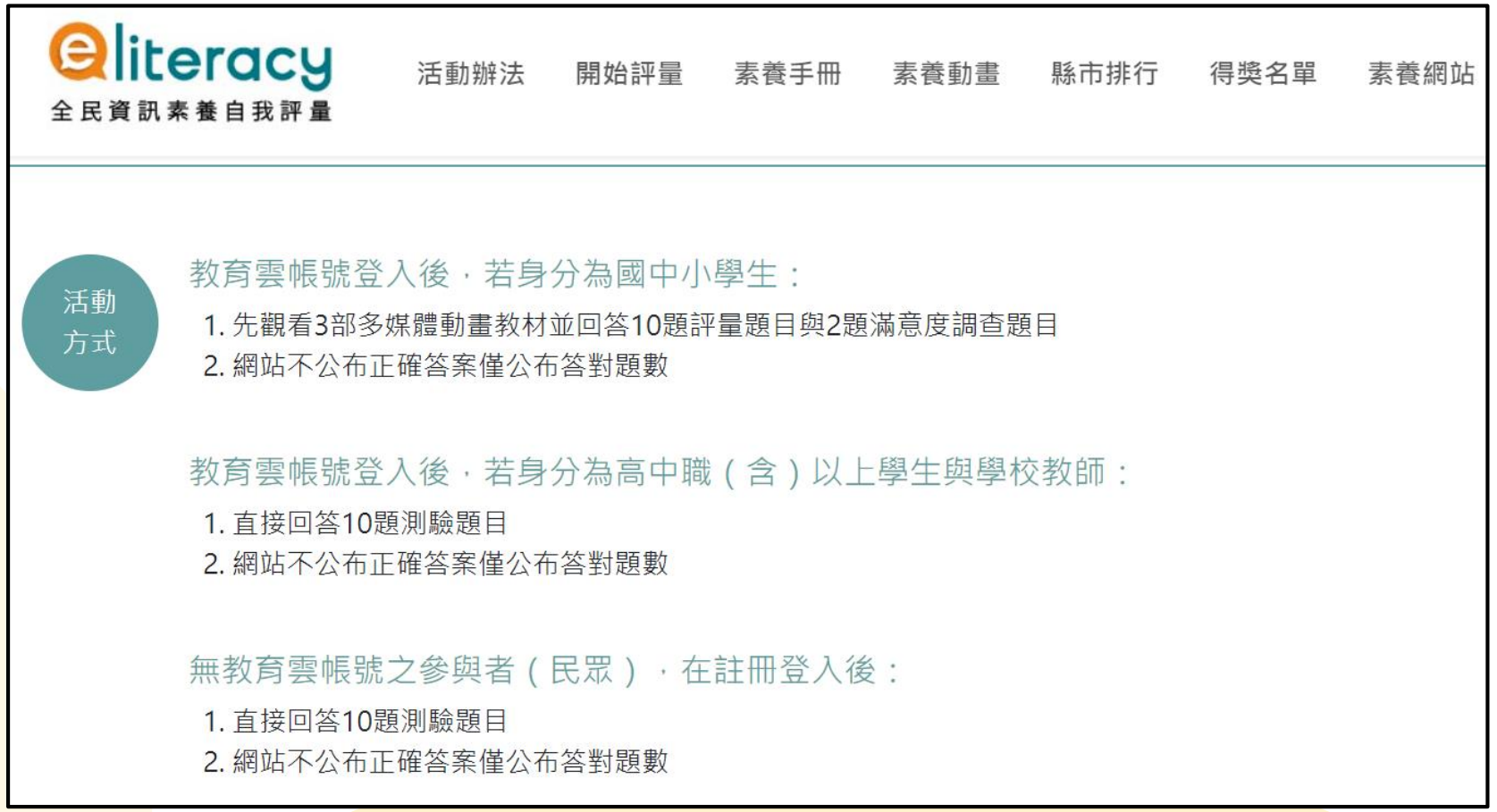
- https://www.nics.nat.gov.tw/

iWIN網路內容防護機構

- https://i.win.org.tw/

全民資安素養自我評量

- https://isafeevent.moe.edu.tw/



資安訊息網站

- iThome資安
  - https://www.ithome.com.tw/security

- 資安趨勢部落格
  - https://blog.trendmicro.com.tw/

- ESET新聞中心/資安快訊
  - https://www.eset.tw/html/list/182

- TechNews 科技新報/網路/
  - https://technews.tw/category/internet/資訊安全

資安評量

- https://forms.gle/Di8VYMvPp9ivF8AT7
- 請登入學校 @cyvs.cy.edu.tw 帳號，進行評量
- 沒有學校 @cyvs.cy.edu.tw 帳號者，請索取紙本