# 112資通安全教育訓練

國立嘉義高商
陳建文
2023.8.29

# 內容

- 政令宣導
- 基本觀念
- 資安事件
- 相關資源

# 資安宣導影片

- 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(10:45)
  - https://www.youtube.com/watch?v=CgKXyYDvtkk
- 駭客如何利用員工的社群網站入侵公司?(5:04)
  - https://www.youtube.com/watch?v=UcIFYQzXt-4
- 《個資風暴：劍橋分析事件》| 正式預告 | Netflix(2:16)
  - https://www.youtube.com/watch?v=qRQEXmg3RaE
- 手機、電腦被駭也沒什麼大不了？小心刑事警察帶你進牢房！快用四招資安習慣讓駭客退散！ | 美國在台協會 X 臺灣吧(3:48)
  - https://youtu.be/XaDeuYIQMOs
- 社交工程詐騙(2:24)
  - https://www.youtube.com/watch?v=ZgbC8DjbrgQ

# 資安宣導影片

- 【TWCERT/CC】社交工程因應之道(6:03)
  - https://youtu.be/XNg8WNByShs
- 【TWCERT/CC】網路釣魚防詐資安宣導(8:31)
  - https://www.youtube.com/watch?v=febFgI_CJX0
- 【TWCERT/CC】APP下載安全指南(6:40)
  - https://youtu.be/RkOr92CSpTI
- 【TWCERT/CC】無所不在的物聯網威脅(14:23)
  - https://youtu.be/bypA8CG2zLI

- 更多內容
- 【TWCERT/CC】資安宣導影音
  - https://www.twcert.org.tw/tw/lp-17-1.html

# 資安宣導影片

- 【NCCST】111年資安影片第1名：搗蛋鬼(2:26)
  - https://youtu.be/xv4dbeJdclI
- 【NCCST】111年資安影片第2名：資安戰隊之邪惡駭客的入侵(2:49)
  - https://youtu.be/LclA56BLNRs
- 【NCCST】111年資安影片第3名：資己資彼(2:54)
  - https://youtu.be/O4FqzfqwgmE
- 還有更多
- NCCST資安系列競賽影片
  - https://www.youtube.com/c/NCCSTwebmaster

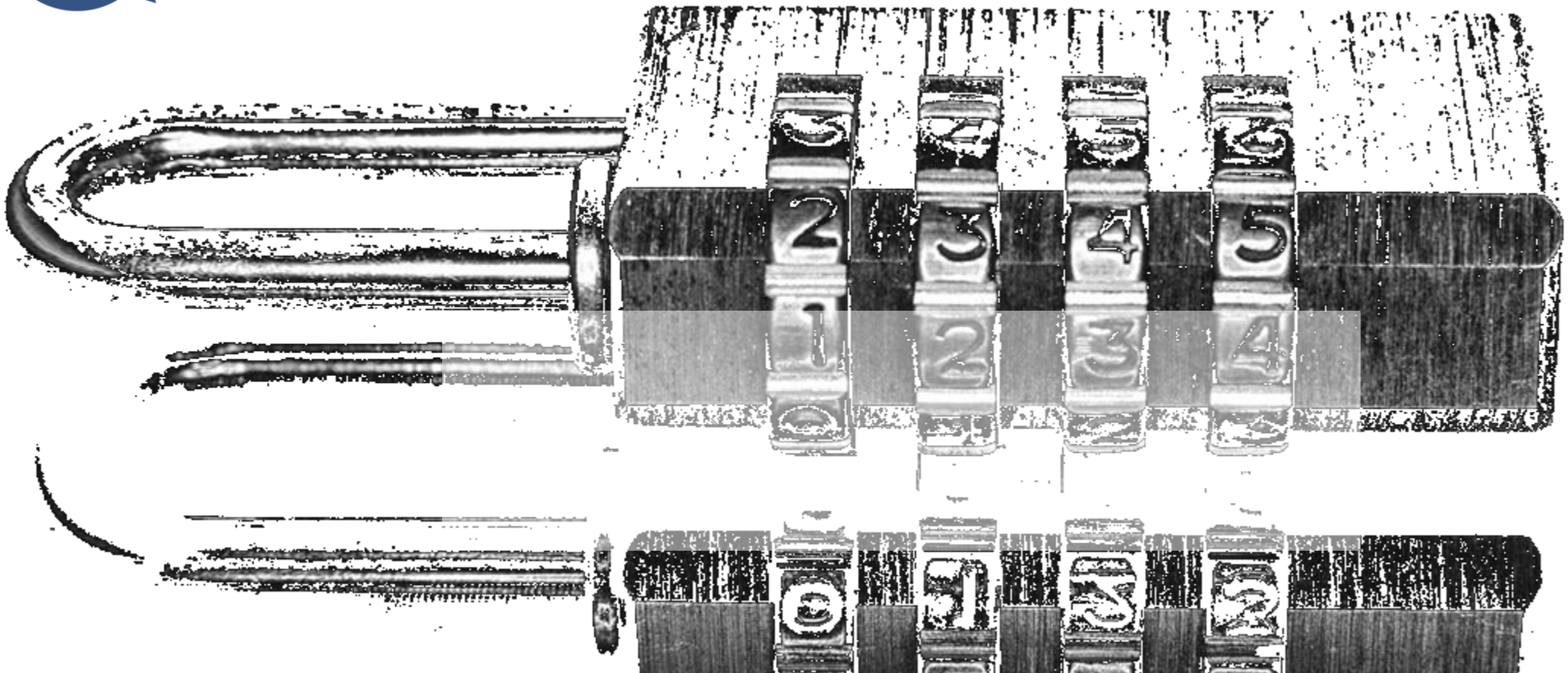
# 資安宣導影片

- 趨勢科技網安學堂(播放清單)
  - https://www.youtube.com/playlist?list=PLxl8TYwVSMhnZempwmxViIXGWNtB8CLMj
- 2020》網路危機(TrendMicro)
  - https://www.youtube.com/playlist?list=PLxl8TYwVSMhkwQ4yppkV7QNQ1TP-S5sO1
- 《Project2030 (2030 專案)》(1:26:47)
  - https://youtu.be/GTLLhuD_0M8?si=ILMLjSscRo7PVuew

# 資安宣導影片

- APT攻擊:一場沒有中立國的戰爭(真實案例模擬) (5:47)
  - https://youtu.be/RyQiz8AudQo?si=3ANbBWPk-qhrE6bX
- 108年資安故事微電影獎 佳作 ：詐騙的手作小教室(2:01)
  - https://youtu.be/0GoGxo2Svio?si=YohykywRmn6U-Bqj

# 政令宣導



# 資訊安全有相關法規嗎？

- 資通安全法，108年1月1日實施
- 行政院國家資通安全會報資安法專區
  - https://nicst.ey.gov.tw/Page/EB237763A1535D65
- 適用於各級公務機關及特定非公務機關
- 資安入法，應做未做，應報未報 - 罰

# 資通安全法及其子法

# 資通安全法和我們有什麼關係？

- 行政同仁責任
  - 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
  - 資安事件通報

  - 個人資安防護（電腦、文書資料...）
    - **個人行政電腦自我檢查**
    - **網頁公告內容自我檢核**

- **電子郵件公務信箱改用「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」**

# 我沒有接行政工作，也有責任嗎？

- 教師同仁責任

  –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**

  **–資安事件通報**

# 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。**

# 學校是的資通安全責任等級是那一級？

附表七　資通安全責任等級D級之各機關應辦事項

| 制度面向 | 辦理項目 | 辦理項目細項 | 辦理內容 |
| --- | --- | --- | --- |
| 管理面 | 限制使用危害國家資通安全產品 | | 一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。<br>二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。<br>三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務（業務）網路環境介接。 |
| 技術面 | 資通安全防護 | 防毒軟體 | 初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。 |
| | | 網路防火牆 | |
| | | 具有郵件伺服器者，應備電子郵件過濾機制 | |
| 認知與訓練 | 資通安全教育訓練 | 一般使用者及主管 | 每人每年接受三小時以上之資通安全通識教育訓練。 |

# 每年至少3小時資通安全教育訓練

NEW

## 重要資訊

- 行事曆
- 線上差勤系統
- FB 學校粉絲專頁
- 電子郵件
- 學籍系統
- 圖書查詢
- 入學資訊
- 升學資訊
- 獎助學金資訊
- 優質認證
- 優質化資訊網
- 均質化資訊網
- 教師進修研習
- 教師專業評鑑
- 進校學籍系統
- 內部控制聲明書
- 課程計畫書
- 選課輔導手冊
- 校內資安訊息

- 每年至少3小時資通安全教育訓練(研習)
- Google WorkSpace - 校內 Google 帳號說明
- 公務信箱電子郵件使用說明
- 校內人員資訊安全守則 (摘要)
- 個人電腦自我檢查表
- 推動開放文件格式ODF
- 其他相關連結、說明、檔案下載

### 每年至少3小時資通安全教育訓練(研習)

1. 依資通安全責任等級分級辦法，每人應接受三小時以上資通安全職能教育訓練
   - 參加校內資安研習
   - 參加校外資安研習
   - 參加e等公務園+學習平臺的線上研習 可參考此說明
2. 請儘可能於每年10月底前完成研習，並繳交相關研習證明(證書、全教網研習時數...)至圖書館

回到頂端 ↑ Top

### Google WorkSpace - 校內 Google 帳號說明 @cyvs.cy.edu.tw

1. 校內帳號本於「教育目的」提供做為教學使用，公務信箱或涉及機

## 本校防疫專區

↑停課不停學期間↑
請留意相關訊息

本校因應確診或居隔應變流程及注意事項

聯絡窗口：學務處衛生組
(05)2782421 分機340

## 目前空氣品質

嘉義市
[2022/06/29 10:00:00 ]更新

指標污染物 AQI 36
() 良好

資料來源：政府資料開放平臺
詳細資料：環保署空氣監測網
詳細資料：即時空氣品質資訊

## 活動相片

# 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

# 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

- ~~國家發展委員會說明網頁~~ 數位發展部
  - https://moda.gov.tw/digital-affairs/digital-service/app-services/248
  - 原來稱NDC Application Tools，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

- 學校首頁資安訊息「**宣導網站/開放文件格式宣導**」有相關說明

# 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
  - .odb for Database

| 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：<br>PDF 可攜式文件格式<br>ZIP 壓縮檔 | | | | |

# 學校網站內容內部查核機制(摘要)

## 一、實施方式及日期

1.定期查核：每年 5 月初及 10 月初啟動各處室網頁內容查核。
2.即時查核：各網頁相關負責人發佈公告或網頁時，應先行審視是否有不合宜內容，各處室主任亦應隨時留意所屬網站內容是否合宜。
3.即時通報：師生發現網站內容有不合宜之處，可向網頁所屬單位進行通報。

## 二、重點檢查項目

1.內容過期：超過 3 年(請各處室自行決定資料期限)，過期下架或加以標註。
2.內含個資：內文、檔案、連結...是否含有足以識別個人資料之內容，應移除。
3.不符 ODF：提供下載之檔案是否符合 ODF 格式(PDF、ODT、ODS…) 。
4.不當內容：網頁內容文字、圖片、影片...是否適宜，請備註說明。
5.連結失效：內部或外部連結可能因變更設定、停止服務...等各項因素，造成連結失效，請更正或移除。

# 校內資安守則 - 作業守則

3 作業守則

3.1 公務電腦應設定登入密碼並確實保密。

3.2 使用校內各項資訊系統時，禁止共用帳號密碼。

3.3 電腦應使用螢幕保護程式(鎖定畫面)，設定螢幕保護密碼(勾選繼續執行後，顯示登入畫面)，並將啟動時間設定為 10 分鐘以內。

3.4 電腦之作業系統應設定為自動更新，漏洞應即時更新修補。

3.5 電腦應安裝防毒軟體，設定即時更新病毒碼，並定期執行電腦掃描。

3.6 應定期將重要資料備份存放，避免硬體損毀及防範勒索病毒的威脅。

3.7 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.8 開啟來路不明之電子郵件及其附件或下載檔案時應謹慎小心，利用防毒軟體或惡意軟體清除工具檢查，以防電腦中毒或駭客入侵。

3.9 當有跡象顯示系統可能中毒時，應儘速通知相關人員。

3.10 禁止私自架設或變更校內網路設備，禁止私自連接網路。

# 校內資安守則 - 資料保護

4 資料保護

4.1 個人辦公桌面應避免存放機敏性文件，工作結束後，應妥善收藏保密。

4.2 應遵守「電腦處理個人資料保護法」規範，保護個人資料使用之合法性及機密性。

4.3 不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本校資訊細節。

4.4 在丟棄任何曾經儲存本校資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。

4.5 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

4.6 重要機密文件或合約，應妥善保存；若為電子檔案應設定保護密碼。

# 校內資安守則 - 密碼使用原則

5 密碼使用原則

5.1 應保護通行密碼，維持通行密碼的機密性；應至少每 6 個月更換一次密碼，並禁止重複使用相同的密碼。

5.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

5.3 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

5.4 通行密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

5.5 密碼設置原則，應包含大小寫字母、數字、符號，並儘量避免使用易猜測或公開資訊為設定：

5.5.1 個人姓名、出生年月日、身分證字號、電話號碼。

5.5.2 機關或單位名稱識別代碼或是其他相關事項。

5.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

5.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

5.5.5 空白、專有名詞、英文或是其他外文字典的字彙。

# 校內資安守則 - 其他

6 電腦軟體版權之使用與管理

6.1 禁止濫用系統及網路資源，複製與下載非法軟體。

6.2 禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定，有些軟體僅授權家用，不可安裝於學校電腦，請務必詳讀軟體授權說明。

6.3 本校電腦所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

6.4 本校人員若有安裝機房伺服器軟體需求時，需填寫「資訊服務申請表」，經權責主管以上核准後，始得執行安裝。

7 資通安全教育訓練

7.1 依「資通安全管理法」子法「資通安全責任等級分級辦法」規定，每人每年應接受三小時以上之資通安全通識教育訓練。

8 保密協定

8.1 本校人員應填具「資訊安全保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

# 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

簡報後會留時間進行詳細的操作說明

# 詳閱「校內資安訊息」

- 學校首頁左側「重要資訊/校內資安訊息」提供詳細訊息及文件

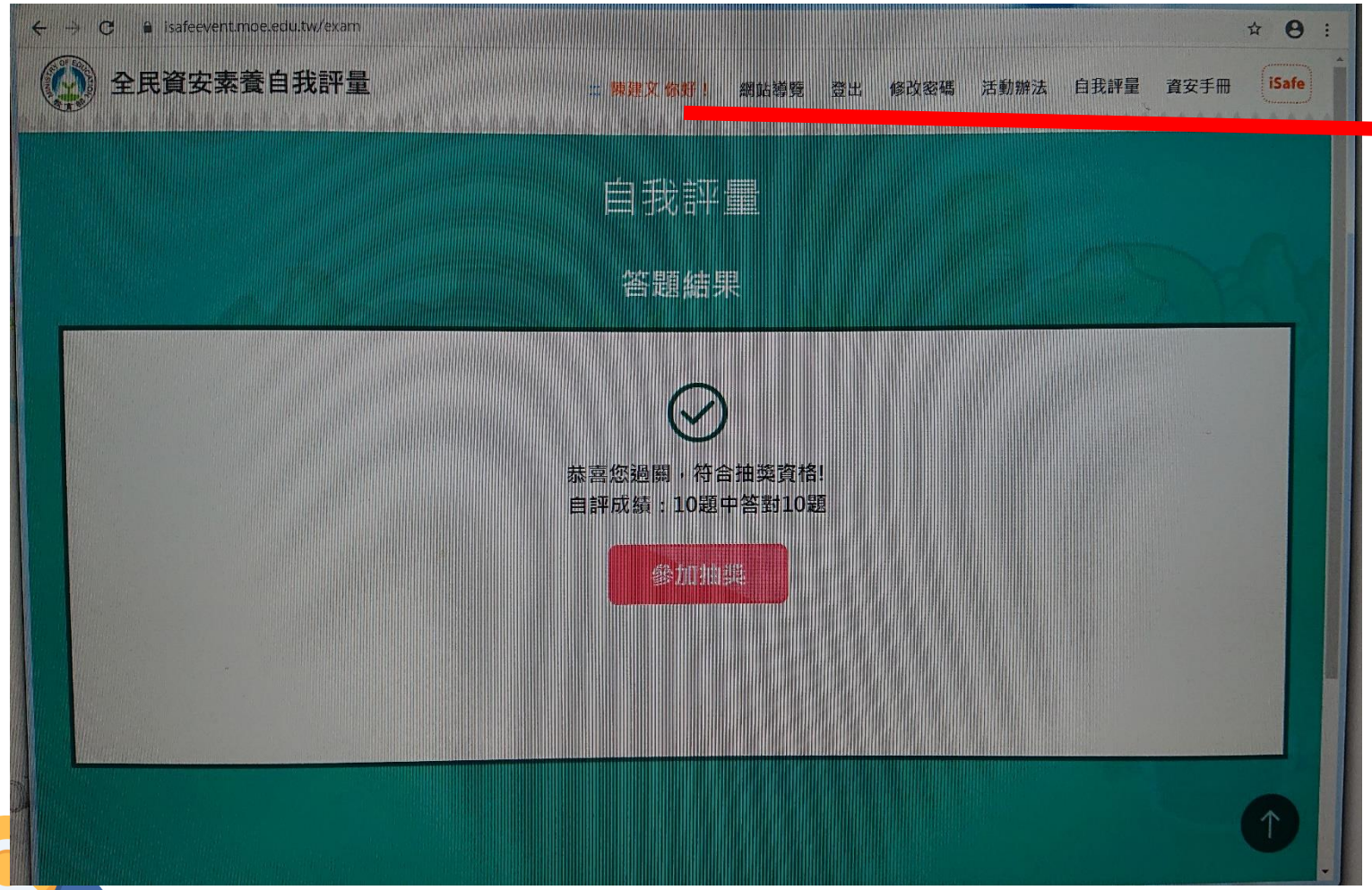


重要

# 全民資安素養自我評量


請校內師生上網參加
9/1 ~ 10/30
全民資安素養自我評量

- 每年一次，屆時會在首頁右上角設置連結，有抽獎喔




# 問題小集錦

- 那裡可以找到本校詳細的【個人資訊安全守則】？
- 為什麼要規定使用ODF呢？MS Word 不是用得好好的嗎？
- 教育雲端電子郵件（@mail.edu.tw）用得不是很習慣，為什麼不用gmail就好呢？
- 校內資通安全教育訓練安排的時間我無法參加，怎麼辦？

# 資安法怎麼管這麼多，好麻煩喔！

- 咦，到對面買個東西，走斑馬線還要繞很遠，所以直接穿越吧！

- **行人穿越馬路注意事項–過路篇**
  - https://youtu.be/bHC4DhRc-xU
- **千萬不要直接從車道穿越過馬路，危險！**
  - https://youtu.be/SwUY9OovrcA

- 安全議題不是三言兩語能講清楚的，
  - 交通安全、國防安全、資訊安全、施工安全(冷氣裝修)

# 基本觀念

資安概念：生活常見疑問

社交工程、

# 資安新概念-零信任

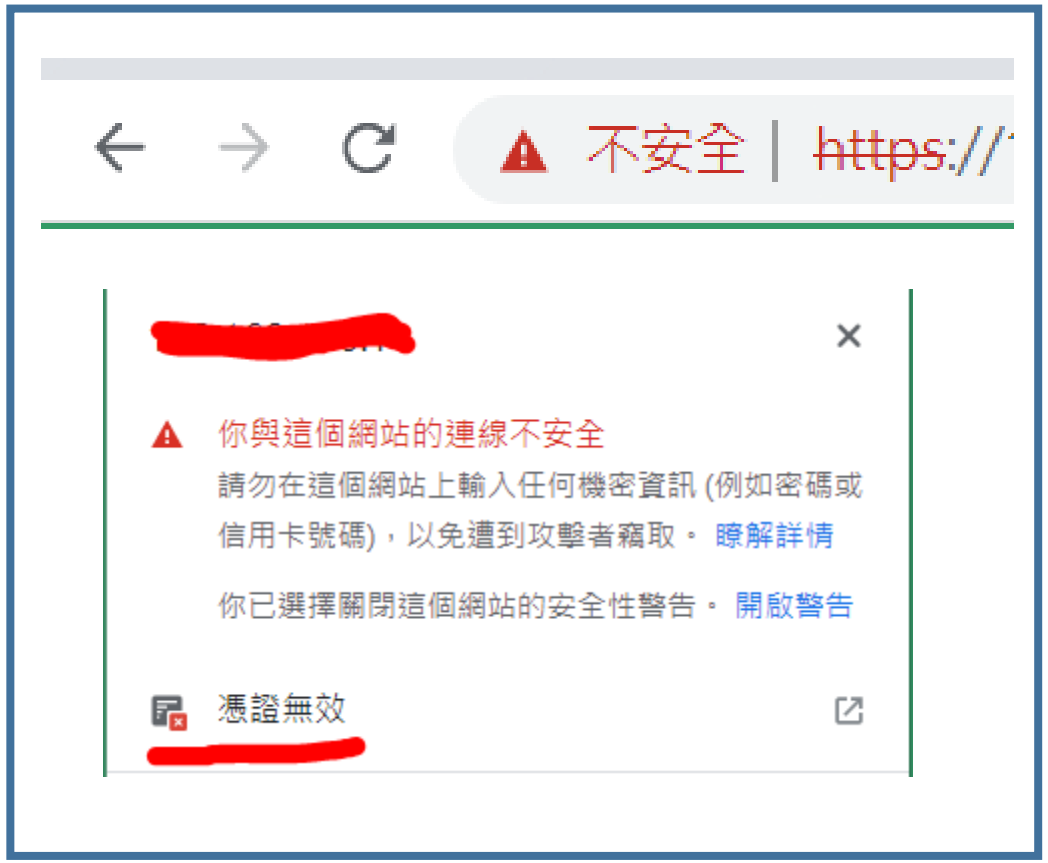
- 我只是看看影片，不會中毒吧
- 我只是下載免費軟體，應該沒關係吧
- 那是小明寄來的信，我當然要看啊
- 都合作那麼多年的廠商了，沒問題吧
- Line群裡都是朋友，不會有人外洩吧
- 我只是去上個廁所，不會有人偷用我電腦吧
- 我門都上鎖了，不會有小偷吧？

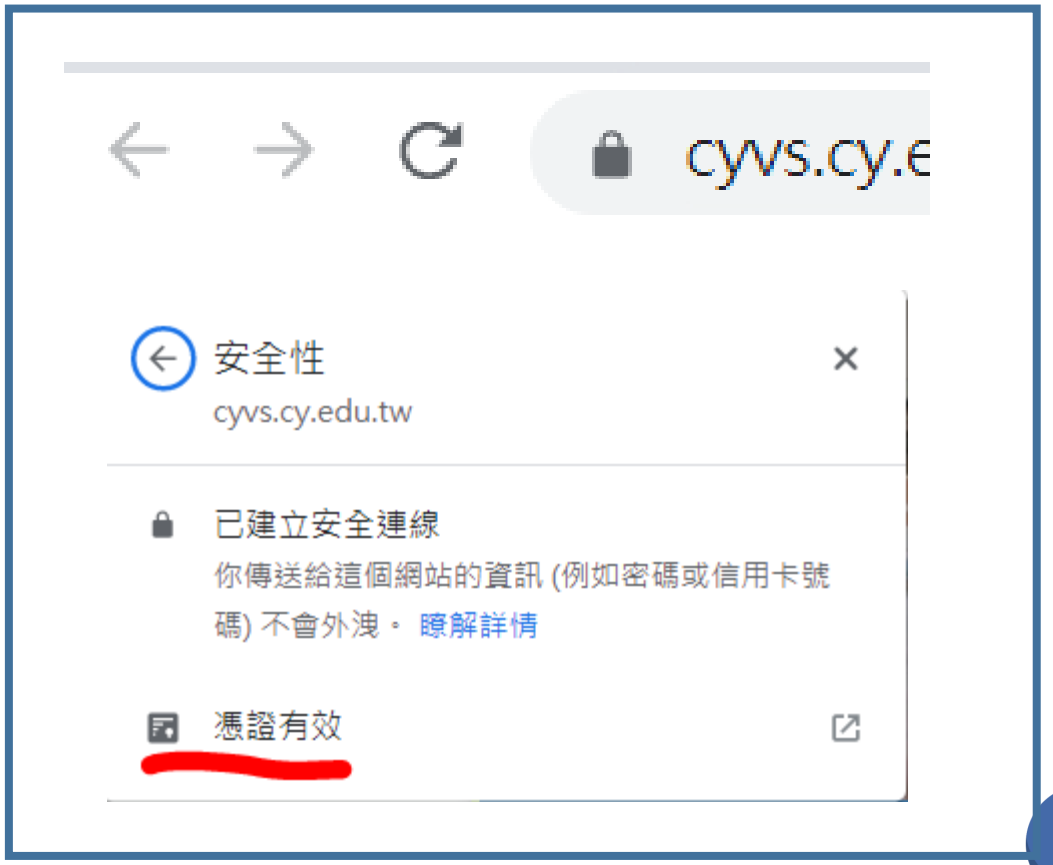
# 你的連線不是私人連線？

NEW

# 你的連線不是私人連線-小常識

- 合法的 https 連線應該要有合法的憑證
- 不合法的原因可能是，私設憑證或憑證過期



# 你的連線不是私人連線-那可以點嗎？

- 官方說法：不安全的網頁不要點
- 大眾說法：~~你想點就點~~你覺得安全就點進去，怕就不要點
- 關鍵思考點：
  - 有必要嗎？
    - 果斷關掉，側面了解這個網站目前的狀況(回報)。(如：找網站負責人問清楚)
  - 沒必要 - 果斷關掉

# 常見的資安問題

我的電腦/手機沒有什麼重要的資料

**被駭...沒什麼大不了吧！**

**？**

# 我又不是什麼重要人物，被駭就被駭？

- 你用的是公用的電腦？有登入過帳號嗎？
- 你用的是公司的電腦？
- 你用的是自己的手機？手機會使用公司WiFi連線嗎？
- 我在家裡電腦被駭，不會影響到公司/學校吧？
- 思考：
  - 你不是駭客的主要目標，但可能是間接目標，或是可利用的工具

- 手機、電腦被駭也沒什麼大不了？小心刑事警察帶你進牢房！快用四招資安習慣讓駭客退散！ | 美國在台協會 X 臺灣吧(3:48)
  - https://youtu.be/XaDeuYIQMOs

# 資安影片

- 【科技大觀園】資訊安全威脅與防護(2:37)
  - https://www.youtube.com/watch?v=zKFAtPkvRkM

# 駭客攻擊思維 - 前置作業

- 搜集資料 ( 暗網、社群軟體... )
- 尋找漏洞、製造漏洞、利用漏洞
- 網頁植入木馬、惡意軟體、釣魚網站/信件、社交工程、APT...
- 侵入系統

# 駭客首要目標 - 取得權限

- 取得帳密
  - 猜的、騙的、監聽(側錄)、預設密碼、找到的(貼在螢幕前那種...)
  - 暴力破解、社交工程、釣魚...

**123456**

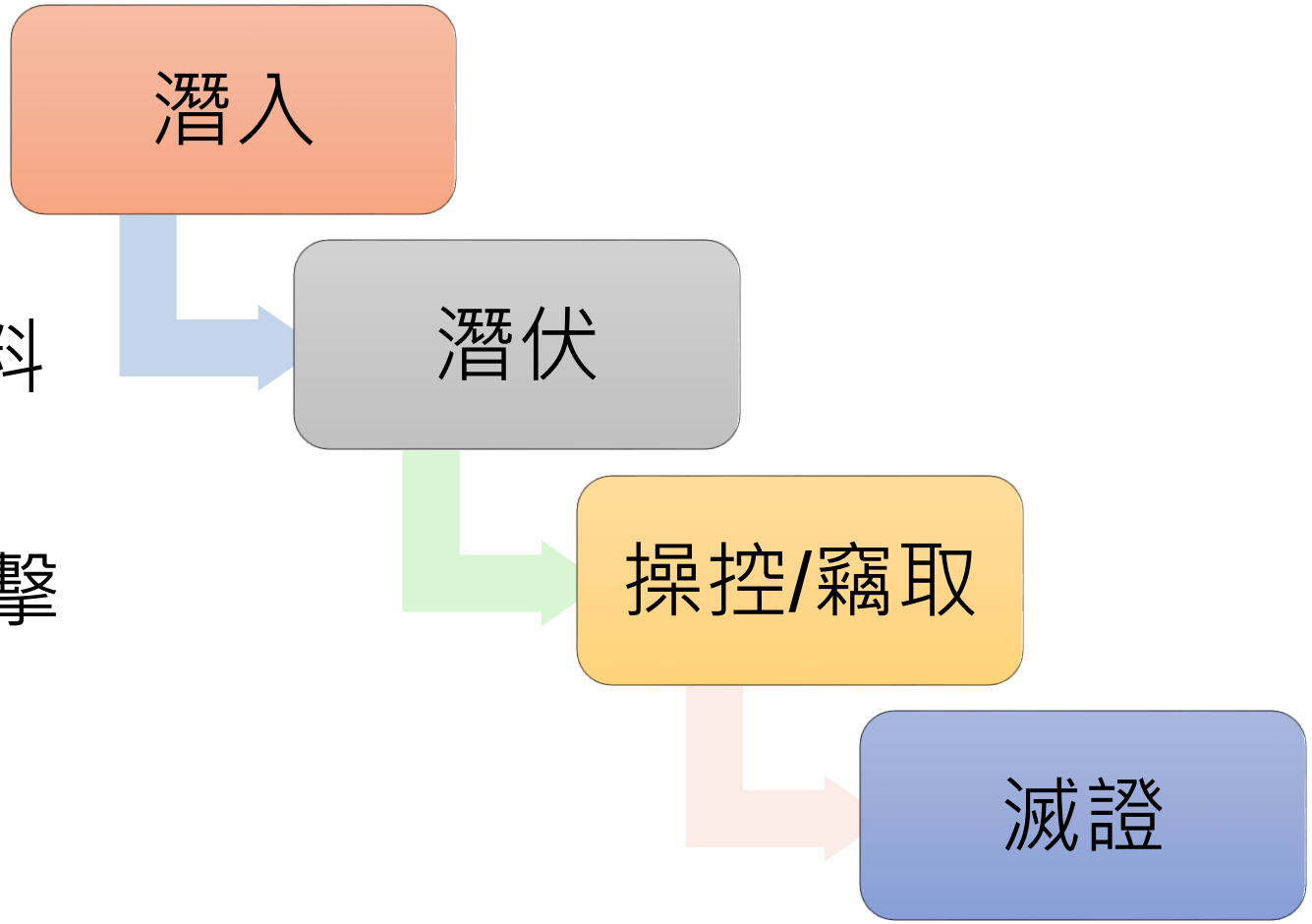
- 利用系統漏洞
  - 掃描已知漏洞並利用工具程式入侵
  - 緩衝區溢位、SQL injection...
  - 預設後門

**更新**

- 惡意軟體、木馬程式、釣魚網站/信件
  - 下載的、電子郵件附件、不明連結...

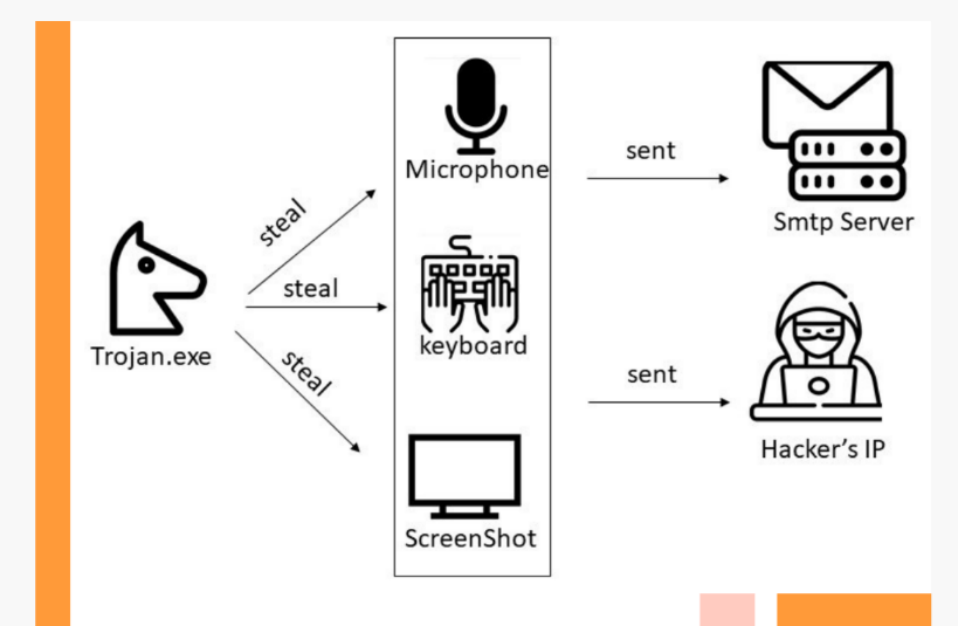
# 駭客攻擊思維

- 入侵並取得最高權限
- 建立後門 / 默默搜集資料
- 竊取資料或進行各項攻擊
- 清除入侵痕跡



# 潛伏 - 建立後門 – 發動

- 駭客入侵後...
- 建立後門
  - 方便駭客進出(操控)你的電腦
- 默默收集你的資料
  - 鍵盤側錄程式
    - 也有硬體版的(不過通常是內賊偷插的)
    - https://www.youtube.com/watch?v=m9SaAz
  - 電腦內的資料、圖片...
  - 你的攝影機/麥克風...



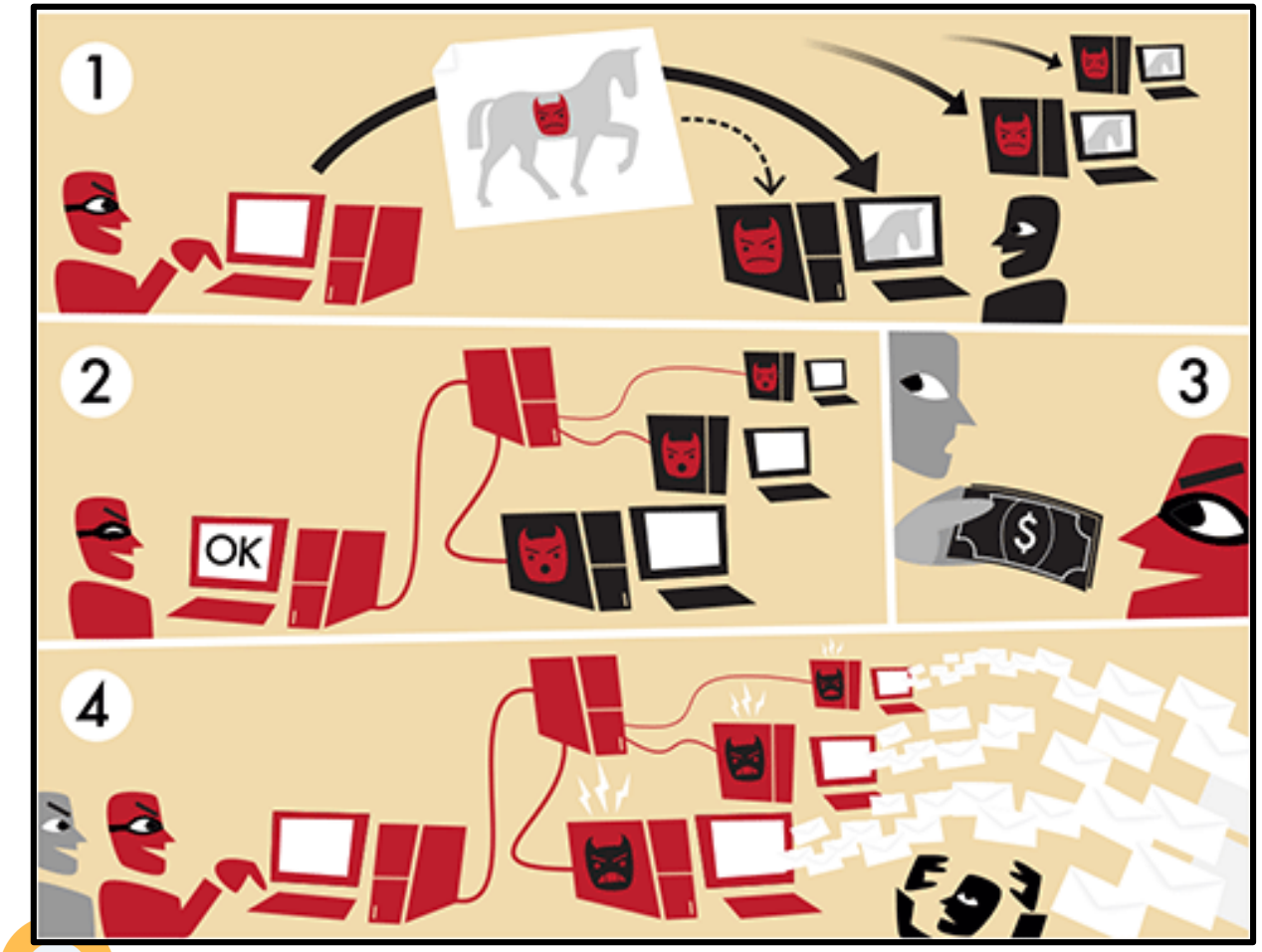
# 潛伏 - 建立後門 – 發動

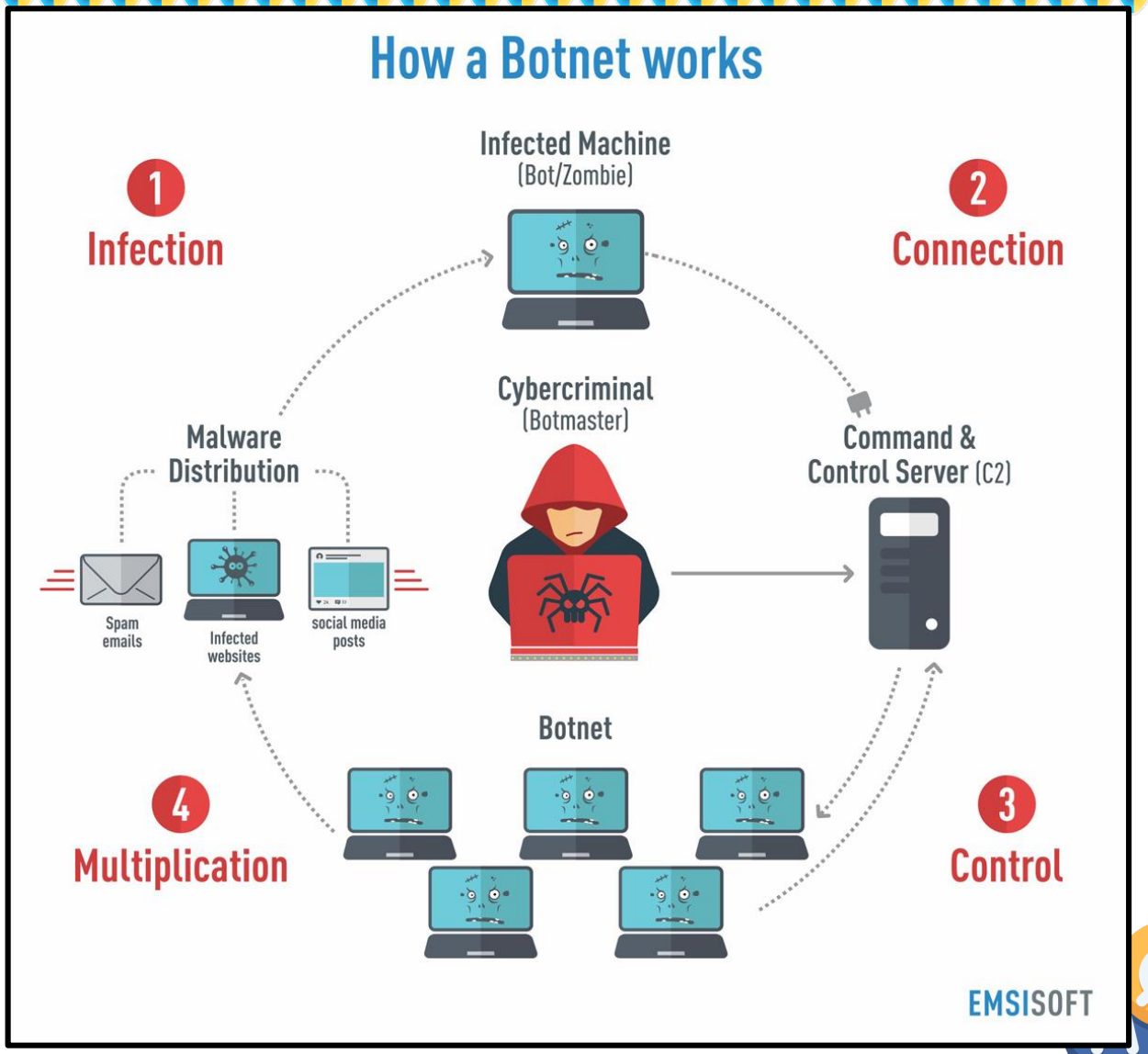
- 僭伏，等...駭客下命令
  - 攻擊 (彊屍網路 / 跳板 / DDoS...)
  - 傳送資料給駭客
  - 偷偷挖礦 (比特幣...)

- 也可能直接發動攻擊
  - 檔案加密 (勒索病毒)
  - 散佈/傳染 (蠕蟲)

# 駭客的目標通常不是你...

- 你只是被利用的工具



# 生活不易，公共場所免費的服務，可以用嗎？

- 免費冷氣，可以用
- 免費椅子，可以用

- 那免費WiFi呢？
  - 《看漫畫談資安》在公共場所使用無線網路( WiFi )的五個安全須知 https://blog.trendmicro.com.tw/?p=60901

- 免費充電呢？
  - 什麼是充電陷阱（Juice Jacking）？FBI 建議避免使用公共充電站 https://blog.trendmicro.com.tw/?p=77318

# 網路通訊－無線傳遞

你以為WiFi是這樣

實際上 WiFi 是這樣

同一內網

# 網路通訊 – 無線傳遞

- 不明/免費WiFi有風險？
  - 假WiFi？被入侵？
- 不用密碼的 WiFi 更危險？
- 開熱點分享無線網路給別人
  - 要設密碼
  - 常改密碼

# 無線分享器 – 基地台

- 使用預設密碼/空白密碼
- 你以為只有你在用？
- 你以為只是頻寬被搶了？(變慢)
- 駭客可能已經入侵你家中的所有資訊設備了

# 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


NEW

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？

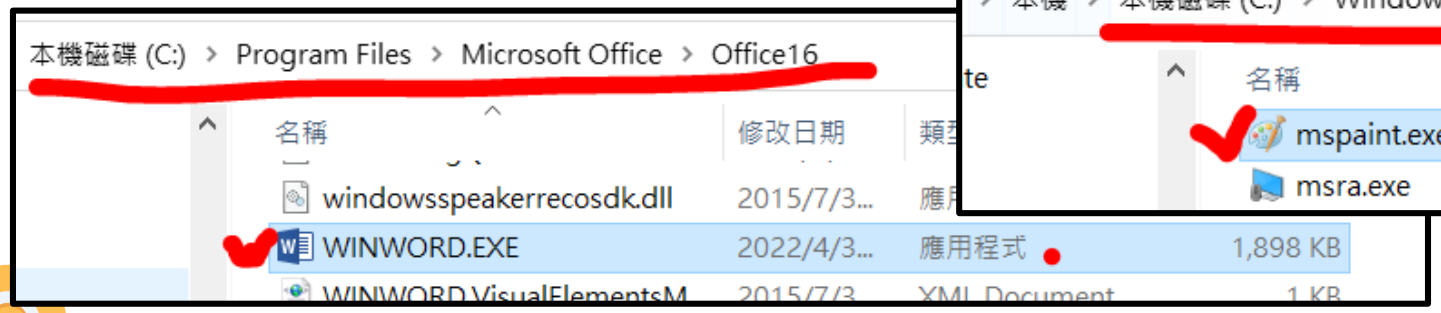
- 官方說法：千萬不要

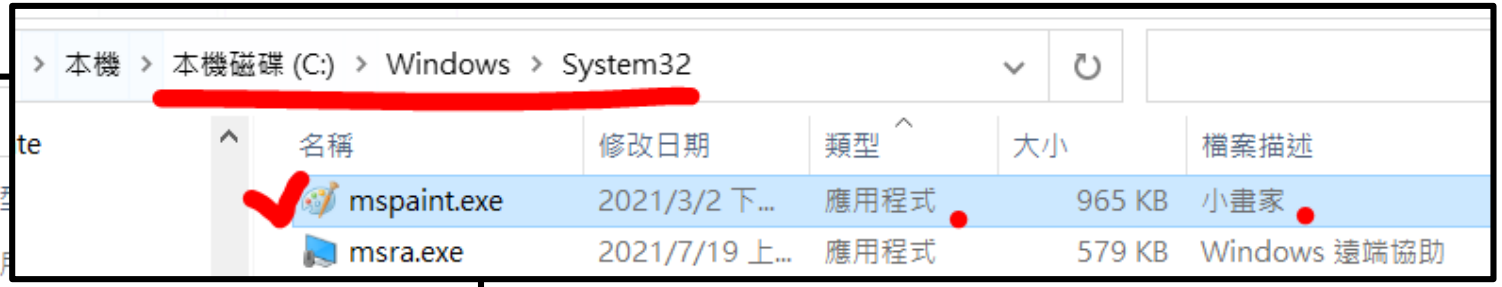

- 那如果是spicy.jpg呢？
  - 官法說法：不要開
  - 大眾說法：不開怎麼知道辣不辣？

- 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
因為有此防護軟體功能滿強大的

電腦病毒
惡意軟體 → 可以執行
的程式 → 載入到
記憶體運行

載入到記憶體運行 → 被防毒軟體
抓到 → 警告/隔離/移
除

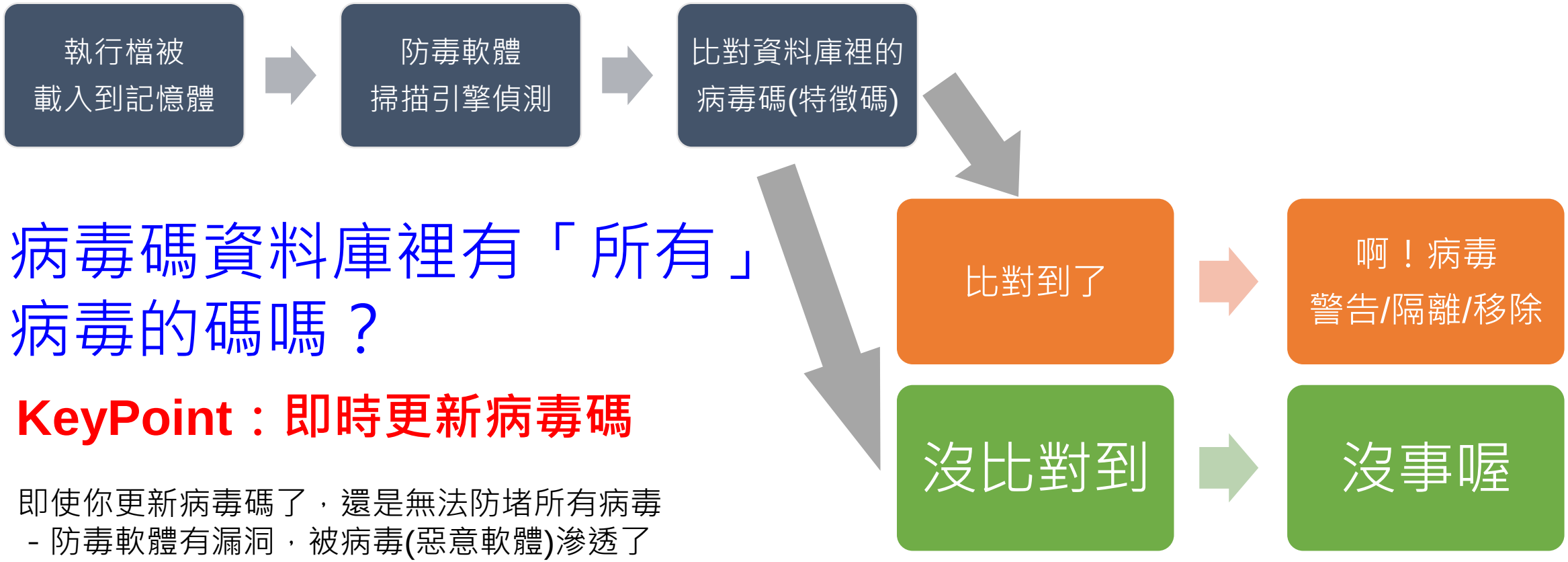
載入到記憶體運行 → 沒有被防毒
軟體抓到 → 潛藏/發作
散播/感染

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？

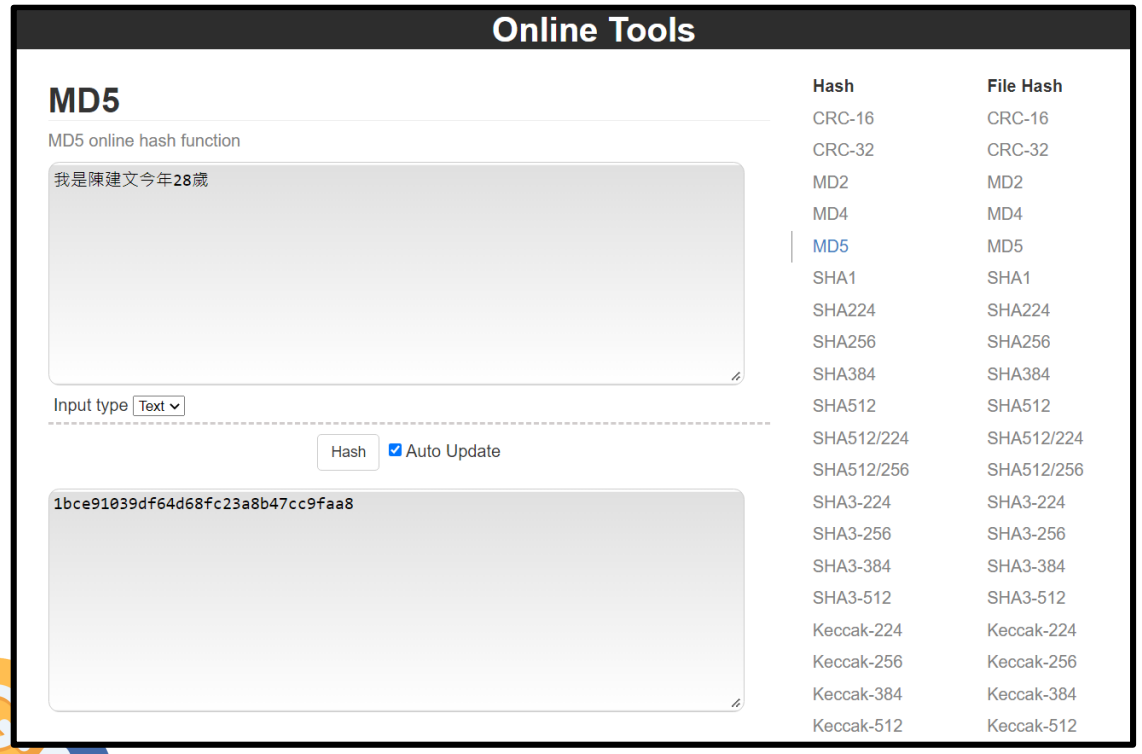
- 大家都認識小畫家 mspaint.exe
  - 但是小畫家是真正的小畫家嗎？
- 如果病毒將自己偽裝成小畫家或依附在小畫家裡
  - 使用小畫家時，其實是執行病毒程式！
- 你在某官網下載了一個好用的應用程式
  - 那是真的官網嗎？ (釣魚網站？)
  - 官網有沒有被駭客竄改過？ (真實案例)
- 你在email附件中看到一個PDF或JPG檔
  - 檔案的圖示是可以改的
  - abc.jpg.exe 因為隱藏副檔名的關係，看到的是abc.jpg
  - PDF檔案夾帶Word、Excel，而Word、Excel可能有巨集病毒

# 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

# 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？

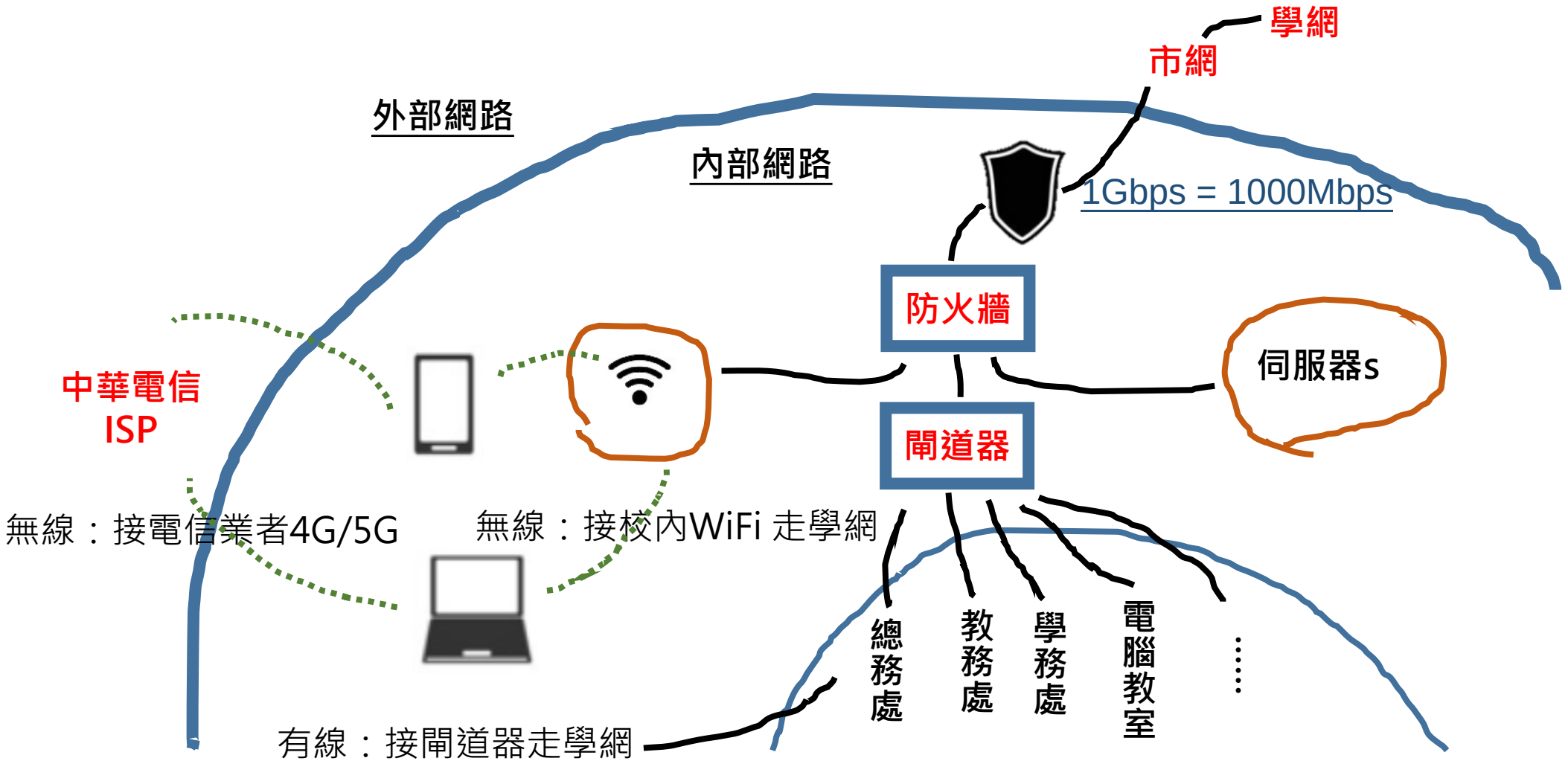
# 我的小米/華為/oppo手機可以帶來學校用吧？

- (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)~~

# 校園網路示意圖


學網
市網
外部網路
內部網路
1Gbps = 1000Mbps
防火牆
伺服器s
閘道器
中華電信
ISP
無線：接電信業者4G/5G
無線：接校內WiFi 走學網
總務處
教務處
學務處
電腦教室
有線：接閘道器走學網

# 內部網路 / 外部網路

- 內部 / 外部 是以「**連網方式**」來區分，不是地理位置

- 由內至外的連線較不設限

你家的大門，會隨時記得關
但是你家裡面的門呢？

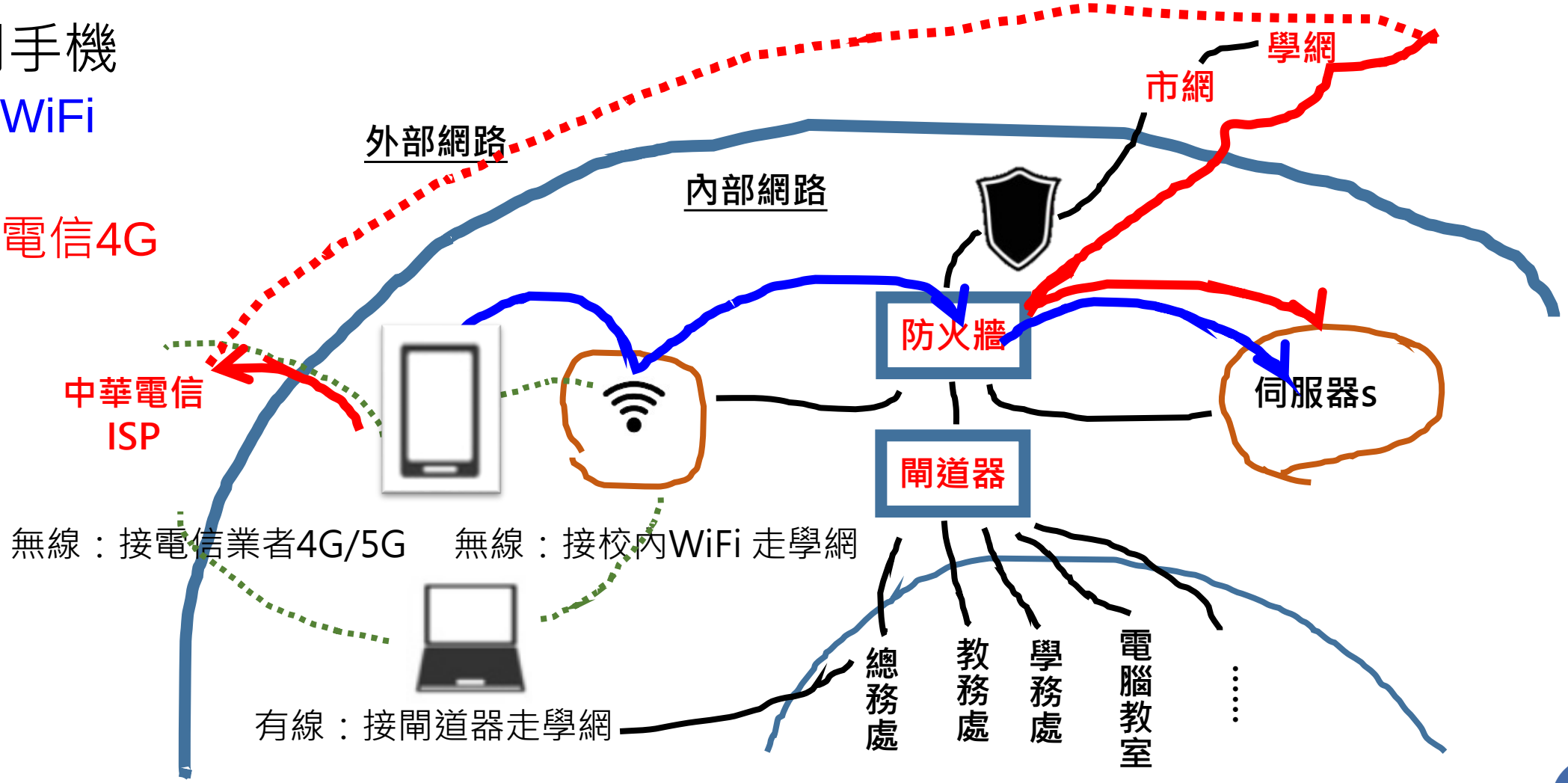
- 由外至內的連線嚴格限制
  - 只開放特定伺服器 / 特定服務(通訊埠 port) (防火牆的主要作用)

- 有些服務只有校內能用，校外網路不行，如：
  - 校內電視廣播系統
  - 校內WiFi密碼修改

網路連線取決於防火牆的設定

# 內部網路 / 外部網路

- 校內使用手機
  - 接學校WiFi
  - 接中華電信4G



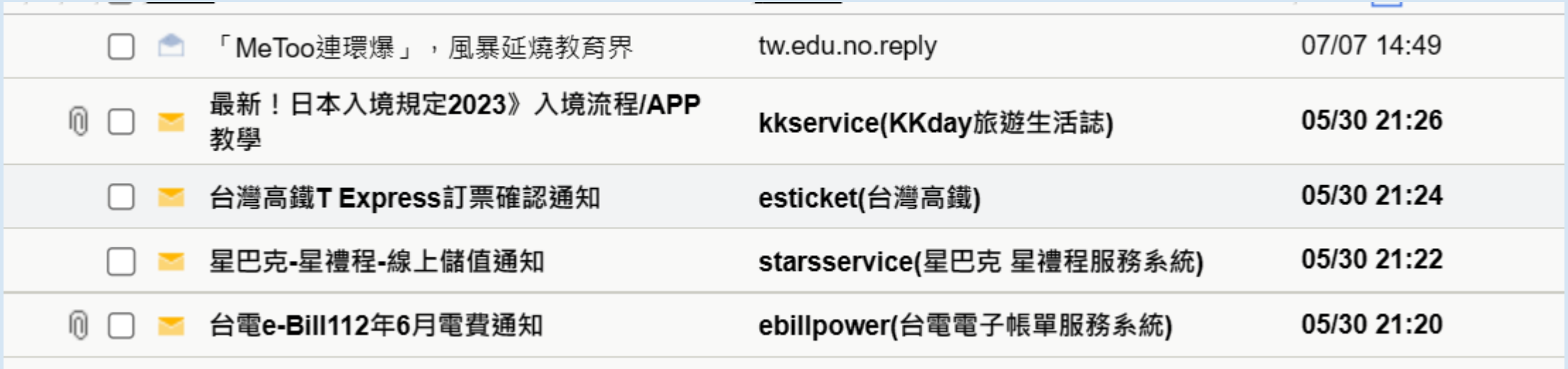
# 上學期末提到的社交工程演練，那是什麼？

- 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。

二、不點擊連結。

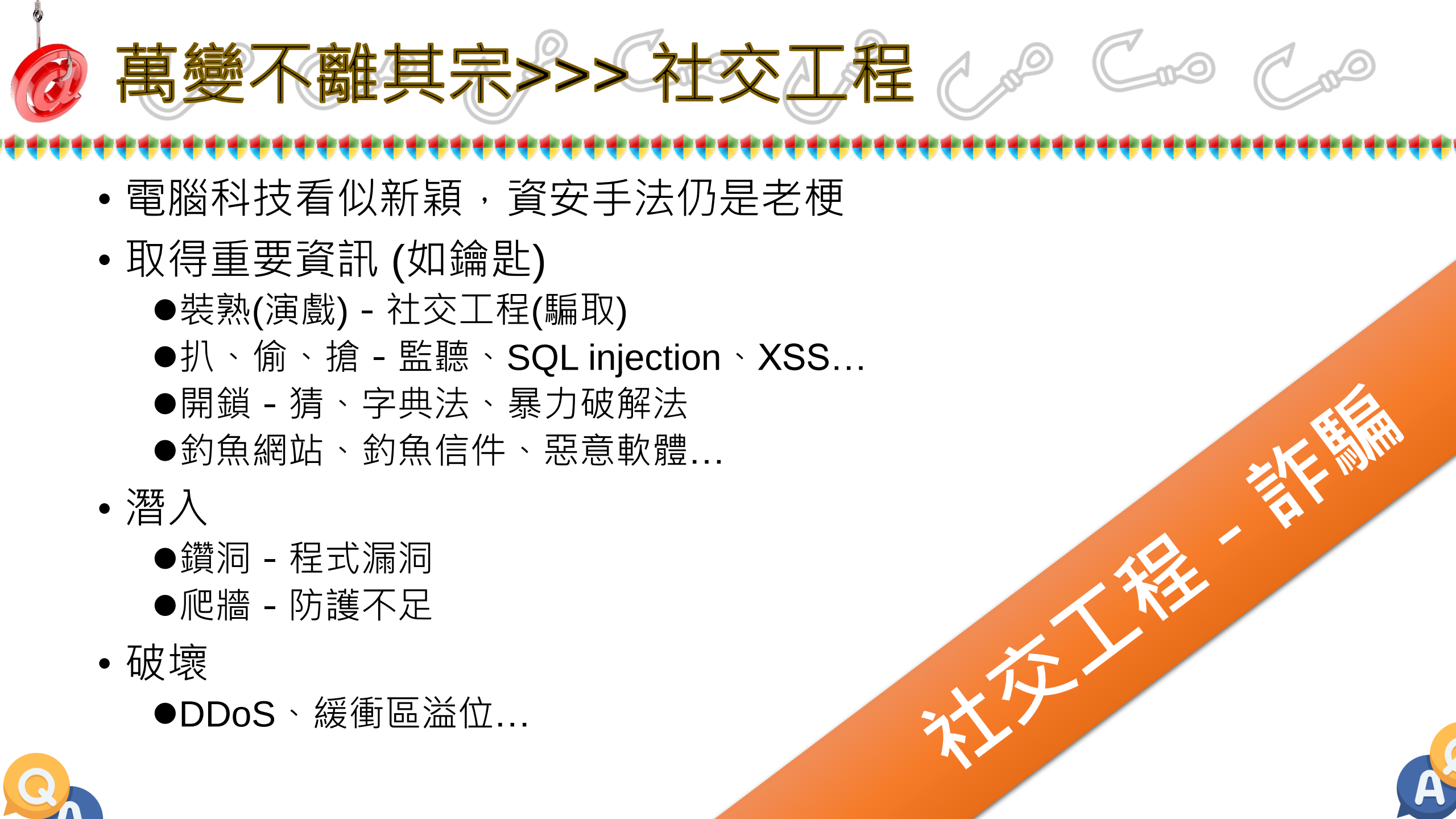
三、不開啟附件。



| | | |
|---|---|---|
| 「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 |

# 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

# 從影片細談各項資安知識

- 知名駭客現身分析好萊塢26部電影真實性：美國國安局能看到所有人的隱私 Hacker Breaks Down 26 Hacking Scenes | 經典電影大解密 | GQ Taiwan
- https://www.youtube.com/watch?v=1jdsosLM_Jg

- 有興趣的人可以網路搜尋一下 Samy Kamkar 的故事
  - 微基百科 薩米蠕蟲
  - 一個中二少年的MySpace英雄夢 Samy Kamkar事件

# 從影片細談各項資安知識-1

- 駭客行為不會有太酷的畫面、跳動太快的視窗
- 紅綠燈-沒有密碼就可以連入
- 多態性代碼，透過改變來隱藏自己(電腦病毒變種)
- 在16進制系統中，只有0123456789ABCDEF，學過計概的都知道，這算是基本常識。電影吧！總是很正經的講著荒謬的事。
- 社交工程
- 有2個駭客同時駭進這個系統...
  (少見嗎？事實上一個漏洞很多的電腦，可能同時被很多駭客操控)

# 從影片細談各項資安知識-2

- 後門程式
- 他們每幾週都會改密碼，但我知道他們在哪裡寫下
- 門禁，一旦能實體接觸到主機，就沒有任何安全可言
- 老舊系統
- 網域名稱與IP位址、網域管轄權、twnic
- 網頁置換、駭入官網植入有毒程式

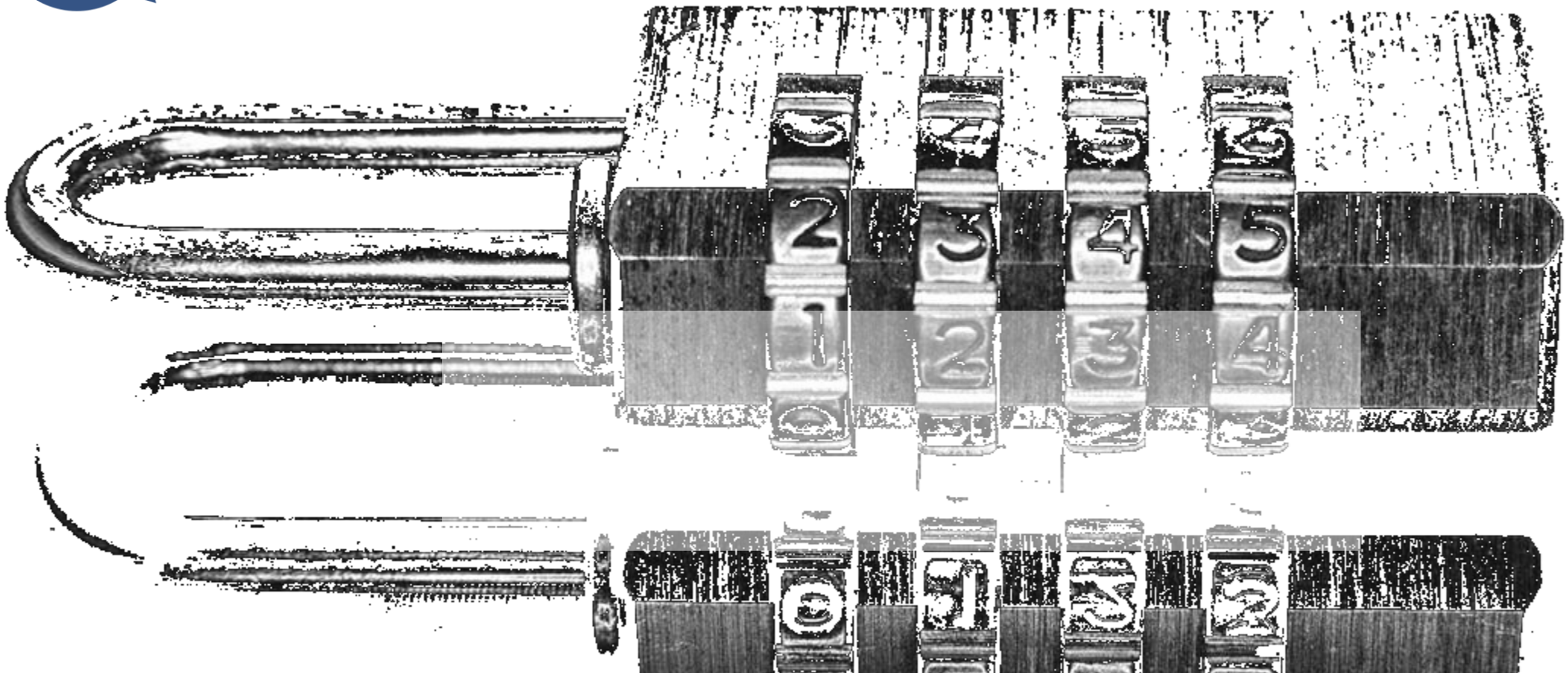
# 從影片細談各項資安知識-3

- 病毒反組譯，把執行檔案轉回程式碼，這樣才能明確知道程式(病毒)會做什麼
- 讓駭客駭入的速度慢下來？除非你正在駭客身邊...，但是你可以拔掉網路線，這樣所有人都連不進來
- ssh遠端登入連線
- 電網系統如果連上網路...@#&%$@#$%^&(
- chromecast、APPLE tv，手機連電視、投影機...通常透過(區域內的無線網路)
- 電腦效能竊取，利用你的，自願的DNA序列重組及SETI@home、 非自願的挖礦病毒、不小心的自願 oCam

# 從影片細談各項資安知識-4

- 個資、重要又不重要的東西、XKeyscore
- 駭客攻防、1年1度駭客大會
- 防止駭客用聽的？利用無線電波的攻擊事件
- 下載檔案(email附件)？你看到的是一張圖，其實是一個病毒程式
- 鍵盤側錄器

# 其他



# 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

# 電信業者小額付款詐騙

- 電信業者小額付款機制
  - https://www.emome.net/channel?chid=909

- 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

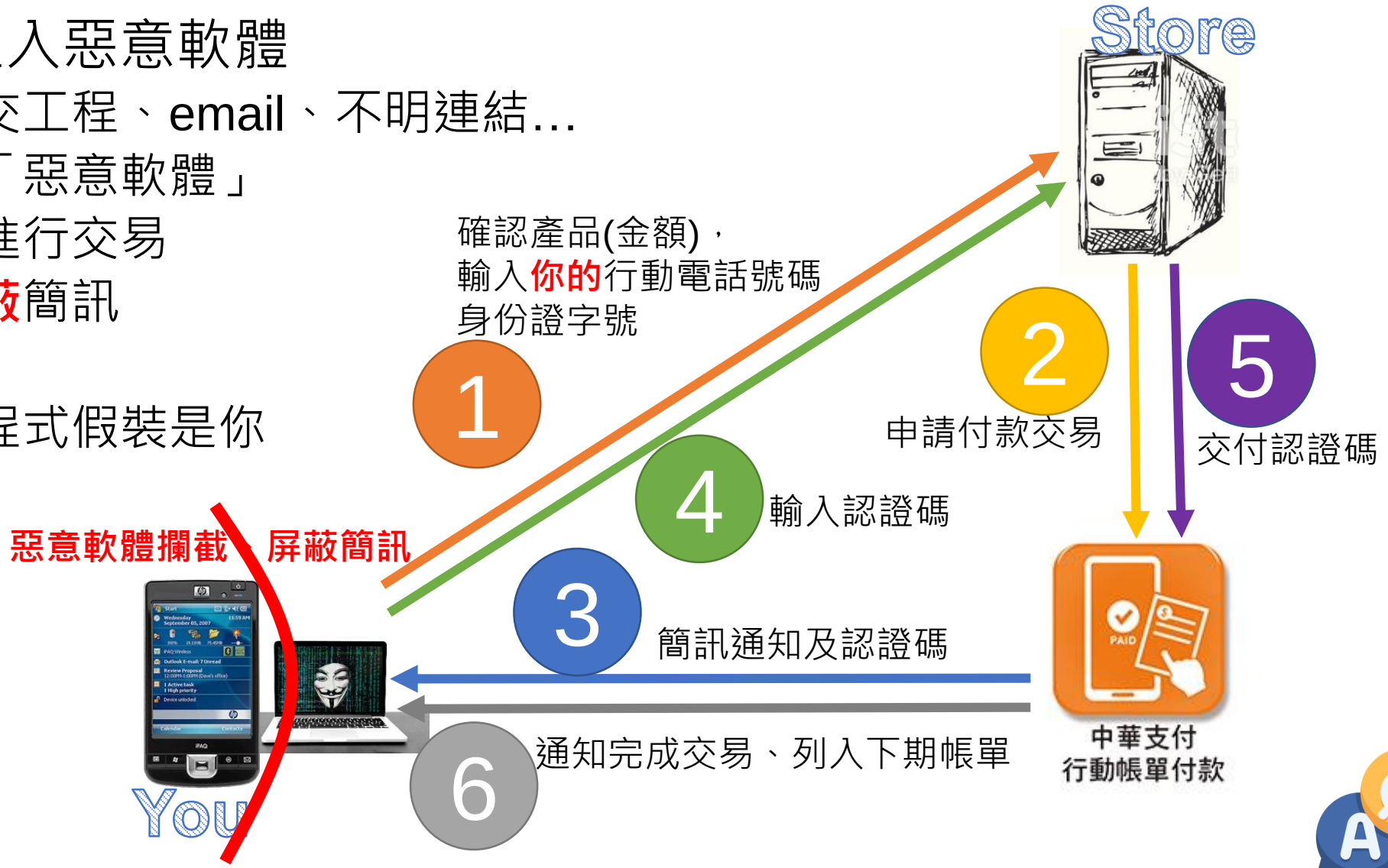
# 電信業者小額付款詐騙示意1

- 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

# 電信業者小額付款詐騙示意2

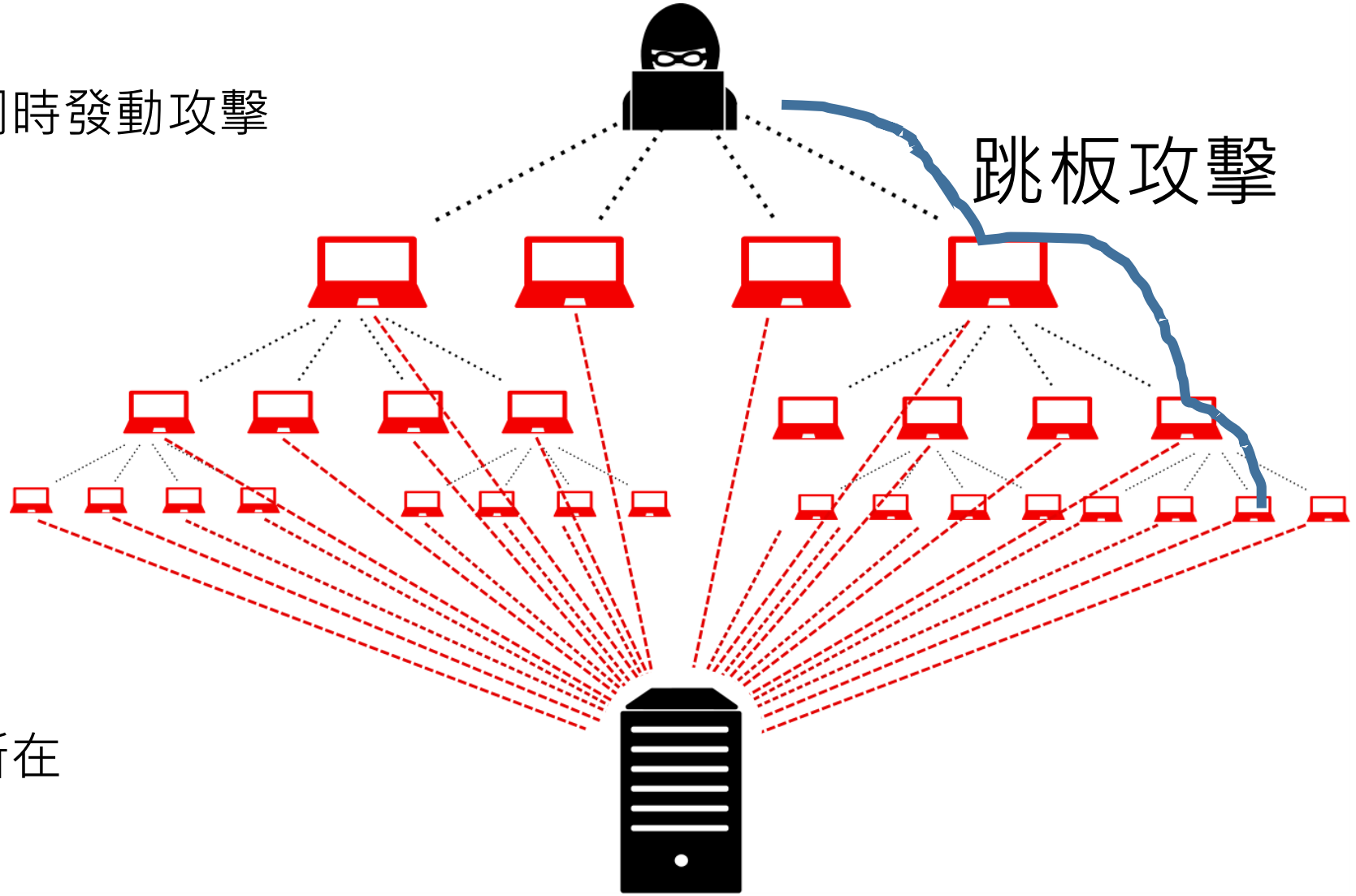
- 駭客突破口 - 植入惡意軟體
  - 釣魚手法、社交工程、email、不明連結...
  - 在你手機植入「惡意軟體」
  - 透過惡意軟體進行交易
  - 期間**攔截、屏蔽**簡訊

  - 駭客透過惡意程式假裝是你
  - 而你並不知道



# 攻擊手法 – DDoS 分散式阻斷服務

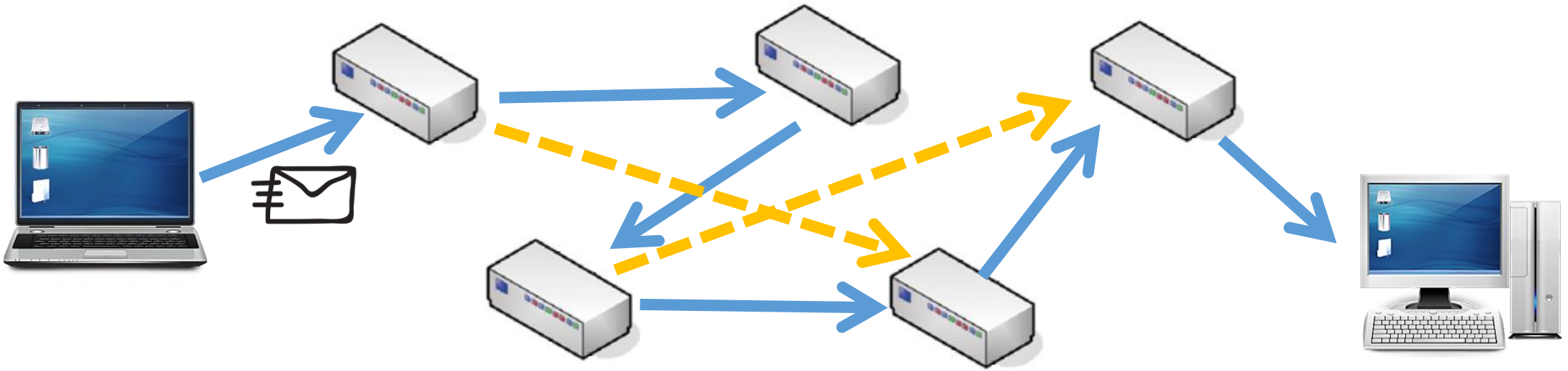
- 攻擊者
  - 操縱多個機器同時發動攻擊
  - 殭屍網路
- 被攻擊者
  - 網路頻寬被堵
  - 對外服務中斷
  - 機器硬體損耗
- 跳板攻擊
  - 不易反查駭客所在



# 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

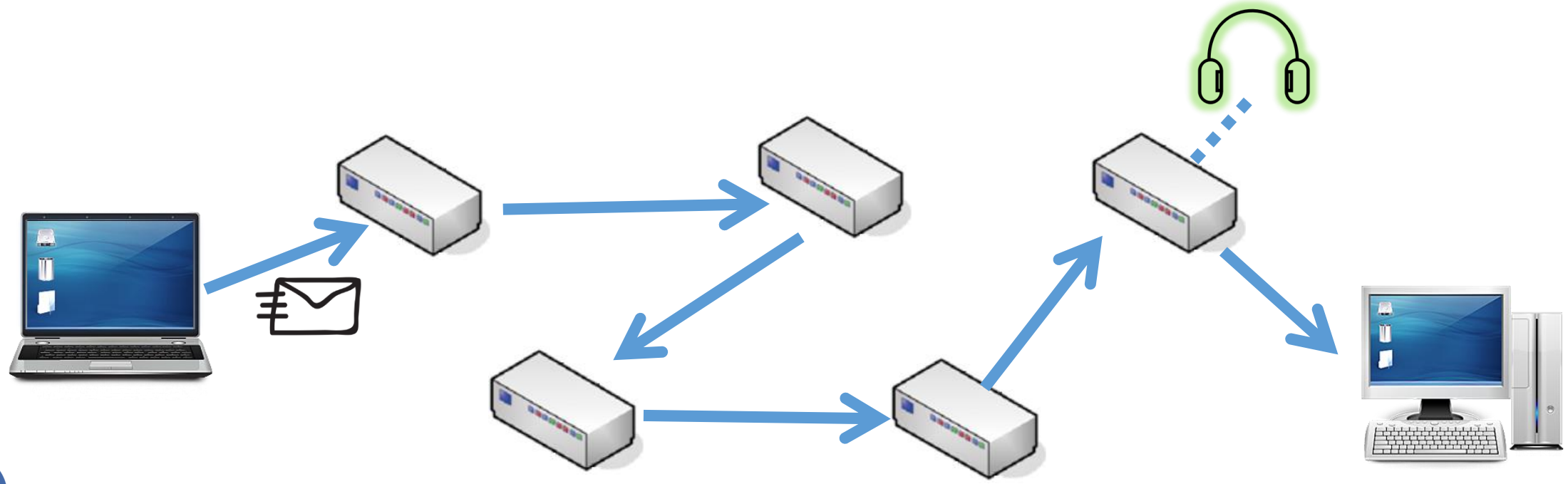


➡中間會經過非常多的節點

# 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

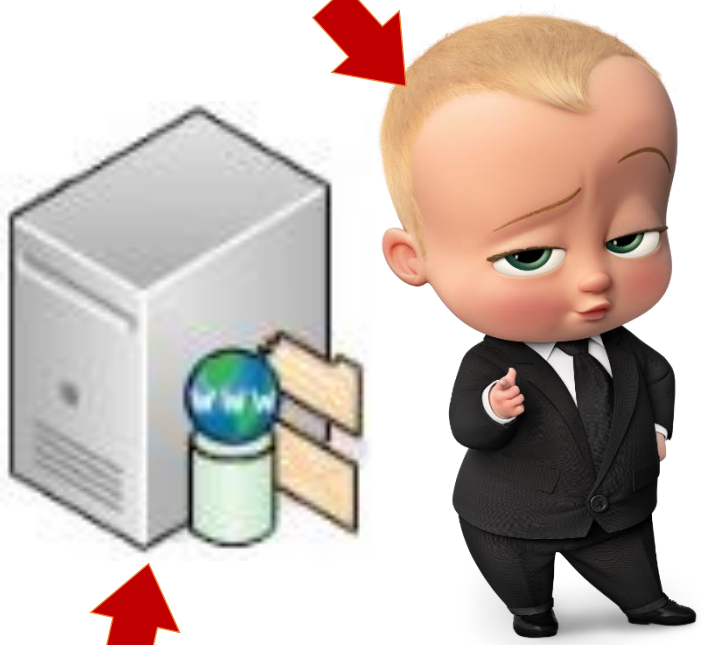
你的問題

木馬/側錄

Https加密了
But MitM

HTTP 沒有s
(沒加密傳輸)

人為○○

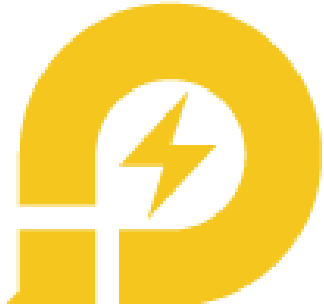


廠商資安
防護不足

# 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)

操作中

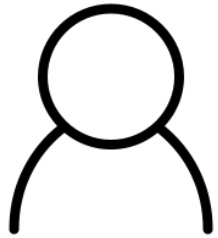
離開了

無法操作
看不到秘密

隨意操作
什麼都能看

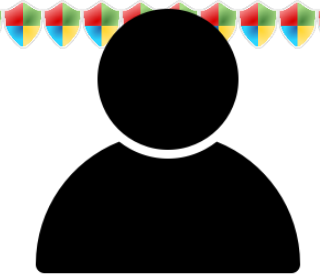
## 離開多久以後才鎖定畫面呢？

# 公用電腦 登出/ 安全瀏覽模式



登入

未登出就離開

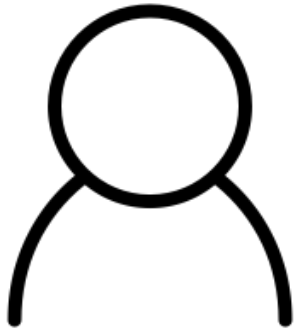


還沒登入

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

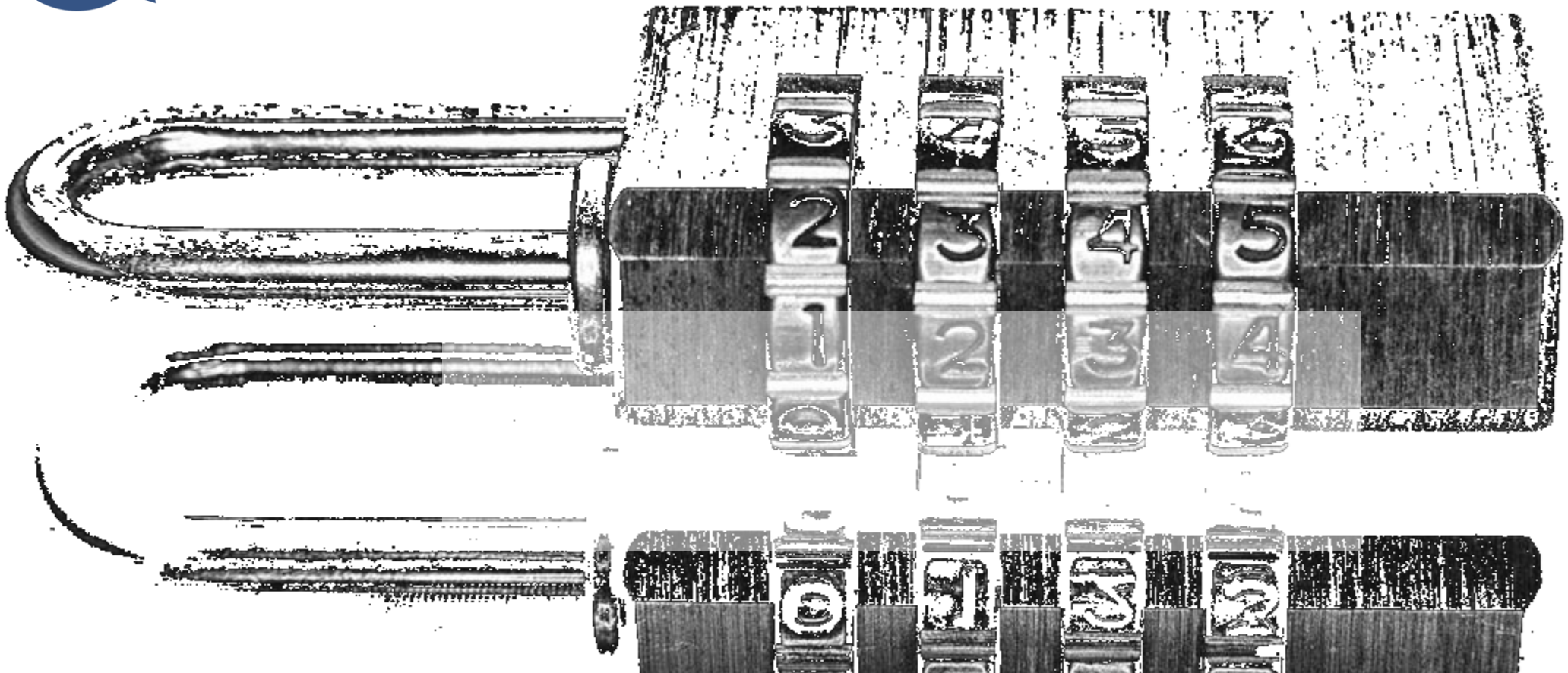
1.以其他裝置登入帳號,遠端確認手機位置
2.遠端刪除登錄在手機內的信用卡資料
3.到所屬電信業者辦理暫停通話或掛失
4.變更社群網站等帳號的密碼
5.持有手機的IMEI碼,到警局備案遺失


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…

# 資安事件



# 案例分享

- 參考
  - 資通安全威脅防護與科技犯罪案例分享-李耀中
  - 111年度從新聞事件看資安及法規要求的影響_王俊凱

# 真的會有這樣的案例

INSIDE 5G AI 新創 評論 焦點 線上課程 Jobs 好工作 繁 / 簡 訂閱 : LINE

趨勢

## 員工被騙內部權限！Twitter 名人盜帳號事件為「社交工程」攻擊

2020/07/20 ▪ 蜜雅 ▪ Twitter 、 資訊安全 、 駭客 、 推特 、 攻擊 、 歐巴馬 、 資安

俗話說得好，資安最大的漏洞就是「人」。社交工程攻擊用的不是高深的電腦技術，而是用詐騙的方式要到關鍵人物的驗證資訊，進而取得登入權限。

INSIDE 5G AI 新創 評論 焦點 線上課程 Jobs 好工作 繁 / 簡 訂閱 : LINE

趨勢

## 【快訊】比爾蓋茲、馬斯克、歐巴馬與蘋果官方都遭殃！Twitter 爆發超大規模帳號被盜

2020/07/16 ▪ Chris ▪ Apple 、 駭客 、 Jeff Bezos 、 比特幣 、 資安 、 elon musk 、 Bill Gates 、 Twitter 、 歐巴馬

他們的帳號被駭後，全部都被換上了比特幣詐騙訊息，要求看到的人向特定位置發送 1,000 美元的比特幣！

# 資安新聞-technews.tw

NEW

- 詐騙集團騙個資綁卡盜刷，金管會提醒留意 1 元簡訊
- https://technews.tw/2022/06/29/otp-warning-fraudulent/

## 詐騙集團騙個資綁卡盜刷，金管會提醒留意 1 元簡訊

發布日期 2022 年 06 月 29 日 10:30 | 分享 分享 讚 14 分享

分類 第三方支付 , 網路 , 資訊安全

有民眾在網路買芒果，卻遇到詐騙集團偽冒小編騙取個資後綁定第三方支付，遭盜刷 8 筆、損失新台幣 19 萬元，金管會提醒民眾留意 1 元試刷簡訊通常發生在綁卡，也請銀行公會研議發卡機構發送 OTP 簡訊時，進一步註明是進行綁卡或消費行為。 繼續閱讀..

# 資安新聞-twcert/cc

NEW

- **間諜軟體業者與 ISP 合作駭侵 iOS 與 Android 用戶**
- https://www.twcert.org.tw/tw/cp-104-6250-0d95b-1.html

**Google 旗下的資安威脅分析小組（Threat Analysis Group, TAG）日前發表資安通報，指出有若干網際網路服務供應商（Internet Service Provider, ISP），涉嫌與間諜軟體業者合作，在用戶的 iOS 與 Android 手機中植入監控工具。**

出現在 Google TAG 報告中的商用間諜軟體業者，是義大利的 RCS Labs；該公司與一些 ISP 業者涉嫌透過詐騙手法，在用戶的 iOS 與 Android 手機中以側載方式安裝惡意軟體。受害者主要是義大利與哈薩克用戶。

Google 指出，在某些案例中，發現涉案的 ISP 業者會先中斷目標用戶裝置的行動連線服務，接著駭侵者會將惡意連結發送到受害者的裝置上，假稱點按連結即可恢復行動連線服務，引誘受害者點按連結。

對 iOS 裝置，駭侵者發送的連結，可透過企業認證簽署來安裝惡意軟體；惡意軟體利用的都是在 2021 年以前發現的多個 iOS 漏洞，可用以提升執行權限，並自用戶的 iOS 裝置中竊取機敏資訊。

對 Android 裝置，駭侵者則直接發送一個惡意 Android App，沒有用到任何已知漏洞，而是直接透過 DexClassLoader API 來下載並執行額外的惡意程式碼。

駭侵者另外也製作假冒的支援網站，聲稱可以幫用戶回復其 Facebook、Instagram、WhatsApp 被停權的帳號，藉以誘使用戶安裝惡意軟體。

建議行動裝置用戶應避免在非 Apple、Google 官方的應用程式商店中下載安裝任何軟體，以避免遭到類似的詐騙訊息誘騙，在手機上安裝惡意程式碼。

# 資安新聞-NCCST

NEW

- **資安研究人員警告應小心夾帶惡意Word檔案之PDF檔**
- https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=16746

## 資安新聞

### 資安研究人員警告應小心夾帶惡意Word檔案之PDF檔

資安研究人員近期發現新型態攻擊手法，該攻擊於PDF內放入惡意Word檔案，並附於電子郵件中傳送。現今大多數攻擊手法為惡意電子郵件附帶Word或Excel檔案，並於檔案內嵌入惡意之巨集，誘騙使用者點選執行，但隨著大眾越來越了解Office附加檔案之威脅性，駭客開始找尋其他方法躲避檢測，PDF檔案即為其中一種。

HP Wolf Security公布之報告中，駭客嘗試寄送內含PDF檔案之釣魚信件，檔案命名為匯款發票，打開PDF後，Adobe Reader會提示使用者打開Word檔，因此行為很罕見，易令使用者感到困惑。提示框內說明「此檔案已被驗證」，此訊息易使受駭者相信Adobe已驗證該檔為合法檔案，並可安全地打開。使用者打開後將啟用巨集功能，並自遠端下載RTF(Rich Text Format)檔案，內含特製物件連結與嵌入(Object Linking and Embedding, OLE)物件。研究人員分析OLE物件後發現，其含有企圖開採CVE-2017-11882漏洞且加密之Shellcode。

微軟於2017年修補之CVE-2017-11882位於Equation Editor工具中，為Office預設工具，可於文件中插入與編輯方程式，在微軟修補該漏洞前，其存在已長達17年。透過利用CVE-2017-11882，RTF檔案中之shellcode可下載並執行Snake Keylogger，其為模組化資訊竊取工具，具有躲避檢測、資料收集及資料洩露等多種功能。

# 資安新聞-iThome

NEW

- 中國駭客集團以勒索軟體攻擊來掩飾間諜行動
- https://www.ithome.com.tw/news/151612

## 中國駭客集團以勒索軟體攻擊來掩飾間諜行動

從勒索軟體特性、受害單位屬性，再加上使用的工具與基礎設施，都與中國政府贊助的網路攻擊行動有所牽連，讓研究人員強烈懷疑中國駭客集團Bronze Starlight其實是利用勒索軟體來隱藏真實間諜行動

文/ 陳曉莉 | 2022-06-24 發表

讚 44 分享

| HUI Loader filename | Payload filename | Cobalt Strike C2 domain | Ransomware |
|---|---|---|---|
| active_desktop_render.dll | desktop.ini | sc . microsofts . net | LockFile |
| Lockdown.dll | mfc.ini | update . ajaxrenew . com | AtomSilo |
| Lockdown.dll | sets5s.ini | Unknown (payload file unavailable for analysis) | Rook |
| Lockdown.dll | Lockdown.conf | api . sophosantivirus . ga<br>sub . sophosantivirus . ga | Night Sky |
| libcef.dll | utils.dll | api . sophosantivirus . ga | Night Sky |
| LockDown.dll | vm.cfg | peek . openssl-digicert . xyz | Pandora |

Secureworks研究人員在2021年初發現駭客集團Bronze Starlight正在部署HUI Loader，HUI Loader可用來解密與載入各種遠端存取木馬，成功

# 順序不對價值52億

- 台積電產線中毒大當機事件簿(Day1~Day4時程懶人包 )
  - https://www.ithome.com.tw/news/125118
- 【臺灣史上最大資安事件】深度剖析台積產線中毒大當機始末
  - 上 https://www.ithome.com.tw/news/125098
  - 下 https://www.ithome.com.tw/news/125101

- 還原台積電中毒關鍵 45 小時始末
  - https://technews.tw/2018/08/27/tsmc-virus-trouble/

# 台積電想哭事件


- 未依 SOP 先掃毒再連線
  - 非駭客攻擊 (有高程度的資安防護)
  - 資安最大的問題是：人
- 初傳 USB 感染，後證實是新機台未進行電腦掃毒所致
- 作業系統 Windows 7，新舊系統都未安裝更新(也無法更新)
  - 特殊用途軟體，可能會因更新而造成軟體無法正常運作
- 北、中、南未進行網段區隔，導致交換感染、擴散
  - 有防火牆設計(會延遲)，但為了「生產效率」...
- 應變得當，所以損失比預估的 78億少...(只有52億)

# 中山大學師生 email 遭駭，被監控長達3年

- iThome 新聞 https://www.ithome.com.tw/news/134105

- Open Webmail 在email盛行之初，是免費而熱門的Webmail系統
  - 免費、架設容易、豐富的說明文件，許多大學仍在使用

- 原官網 https://openwebmail.org/ 最後版本 2.53版(2008年)
  - 原官網仍在，有些Mirror站也在，仍正常提供下載
  - 似乎有人接手 http://openwebmail.acatysmoof.com/ (從sourceforge)，但看起來仍是停了，相關下載連結失效了

# Open Webmail – Thomas Chung 董仲凱


**Open WebMail Project Mirrors**

**Please use mirror sites near you to avoid overload on official sites!**

| Sites | URL | Location | Maintainer |
|---|---|---|---|
| Official Site | http://openwebmail.org/openwebmail/ | US | Thomas Chung |
| Development Site | http://turtle.ee.ncku.edu.tw/openwebmail/ (No Longer Available) | Taiwan | openwebmail |
| Canada | http://openwebmail.forsale.plus/ | Quebec, Canada | Boryslav |
| France | http://openwebmail.europnews.de/openwebmail/ | Paris, France | Tobias Schmitz |
| Germany | http://openwebmail.ewpm.eu/ | Kiel, Germany | ewpm.eu |
| USA | http://openwebmail.lagmonster.org/ | | |
| USA | http://openwebmail.adminii.ro/ | | |
| USA | http://www.go-parts.com/mirrors-usa/openw | | |

現在Open Webmail有諸多優點，而且是一套自由的開放原始碼程式(其正式網站http://openwebmail.org)，也是全球研發人員共同維護的免費軟體。 現在主要是成功大學董仲愷先生負責研發與維護。 雖然還有一些缺點，但是因為他們不斷的改進，我們可以期待這套軟體的進步。

www.phys.sinica.edu.tw › computer_lab › brow

科學運算 - 中央研究院物理研究所

# 由中山大學 Open Webmail 事件談起

- Open Webmail – Thomas Chung (董仲凱)


- 開放源碼Open Source/自由軟體/免費軟體...可能的資安問題
  - 程式編寫不夠嚴謹，容易出現漏洞
  - 作者(團隊)停止更新了...導致漏洞無法修復
  - 缺乏完善的自動更新機制，需手動下載更新/重新安裝
  - 使用者裝了以後，從沒更新過
  - 上述，不代表這類型軟體就不安全，但仍要慎選

# 名人推特帳號遭駭

- 14年來「災難級」資安事件！馬斯克等名人推特遭駭入發詐財文
  - https://www.gvm.com.tw/article/73722

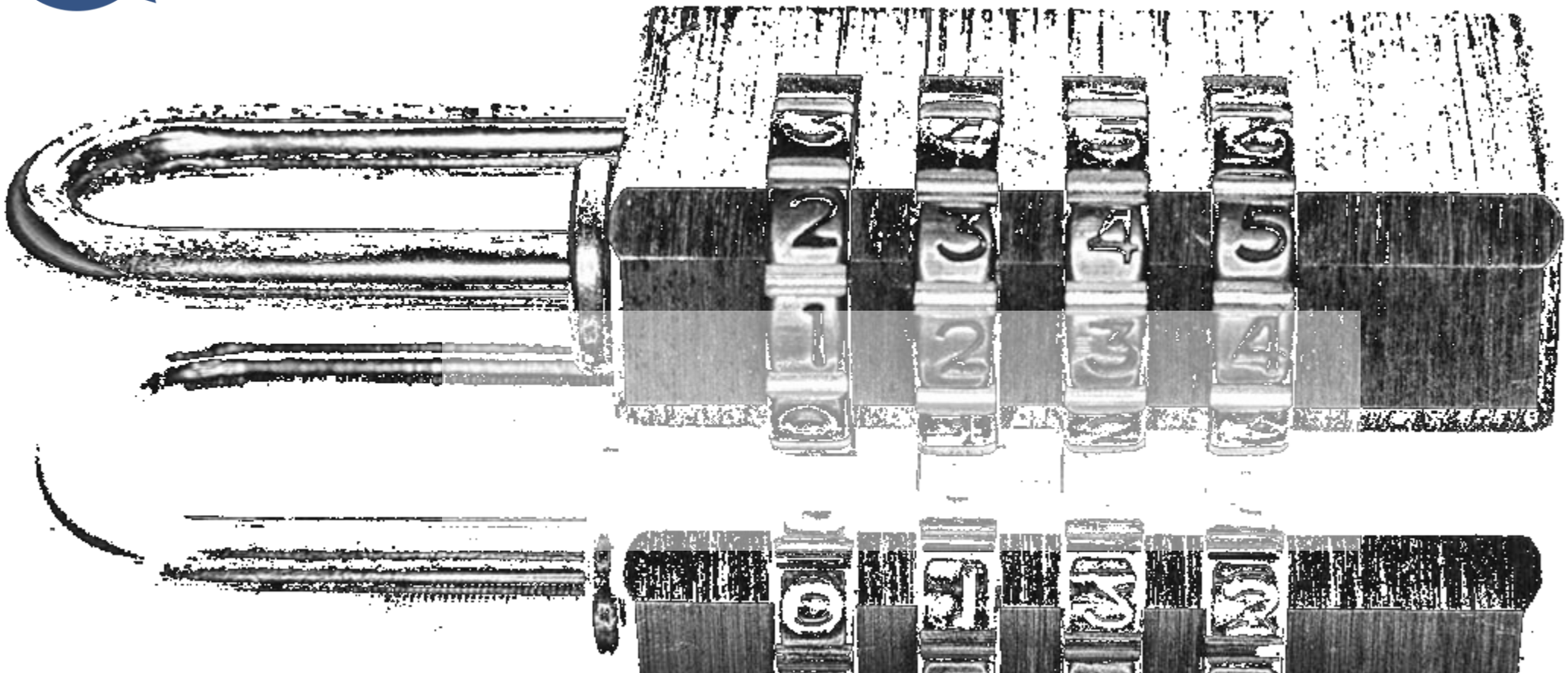
社群網站推特（Twitter）15日發生成立以來最嚴重的資安事件，多個加密貨幣交易所相關帳號被駭客入侵，災情接著迅速擴大，包括特斯拉汽車執行長馬斯克在內，多個名人帳號遭駭並張貼加密貨幣詐騙推文。推特已緊急關閉受害帳號及啟動內部調查，但犯案組織、方法及動機仍不明。

# 名人推特帳號遭駭－社群軟體資安

- 台灣常用社群軟體 fb、ig、Line，常傳帳號被盜事件
  - 帳號被盜很少是系統的問題，通常是本人的問題

- 見帳號如見本人，擋點鋃兒來花花
- 好友推薦酷連結，不點不看不義氣
- 團購賣得很便宜，趕快下單忙匯款
- 獵巫行動別落後，發洩情緒好管道
- 盲目跟風趕流行，這票還不快點投


# 相關資源



# 臺灣學術網路危機處理中心TACERT

- https://cert.tanet.edu.tw/prog/index.php

# 全民資安素養網

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

# iWIN網路內容防護機構

網路內容防護機構
Institute of
Watch Internet Network

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

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

# 資安訊息網站

- twcert/cc台灣電腦網路危機處理暨協調中心
  - https://www.twcert.org.tw/
- 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

# 提醒大家

- **社交工程演練...千萬不要點...**
- 不要在學校電腦、網路連結不當網站...
- 不要在社群軟體中(如Line)，傳遞個資及機敏資料，尤其是帳密
- 詳閱校內人員資訊安全守則，確實做好個人電腦自我檢查
- 不要使用Email傳遞個資(包含學生資料、成績...)，萬不得已，一定要使用複雜密碼加密再傳，且「密碼」另外告知。
- 帳密要保全、資料要備份，才能避免或降低損失。

# 資安評量

- https://forms.gle/v1fbX8zMzCdW14Pv9
- 請登入學校 @cyvs.cy.edu.tw 帳號，進行評量