

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...

社交工程 - 詐騙

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：

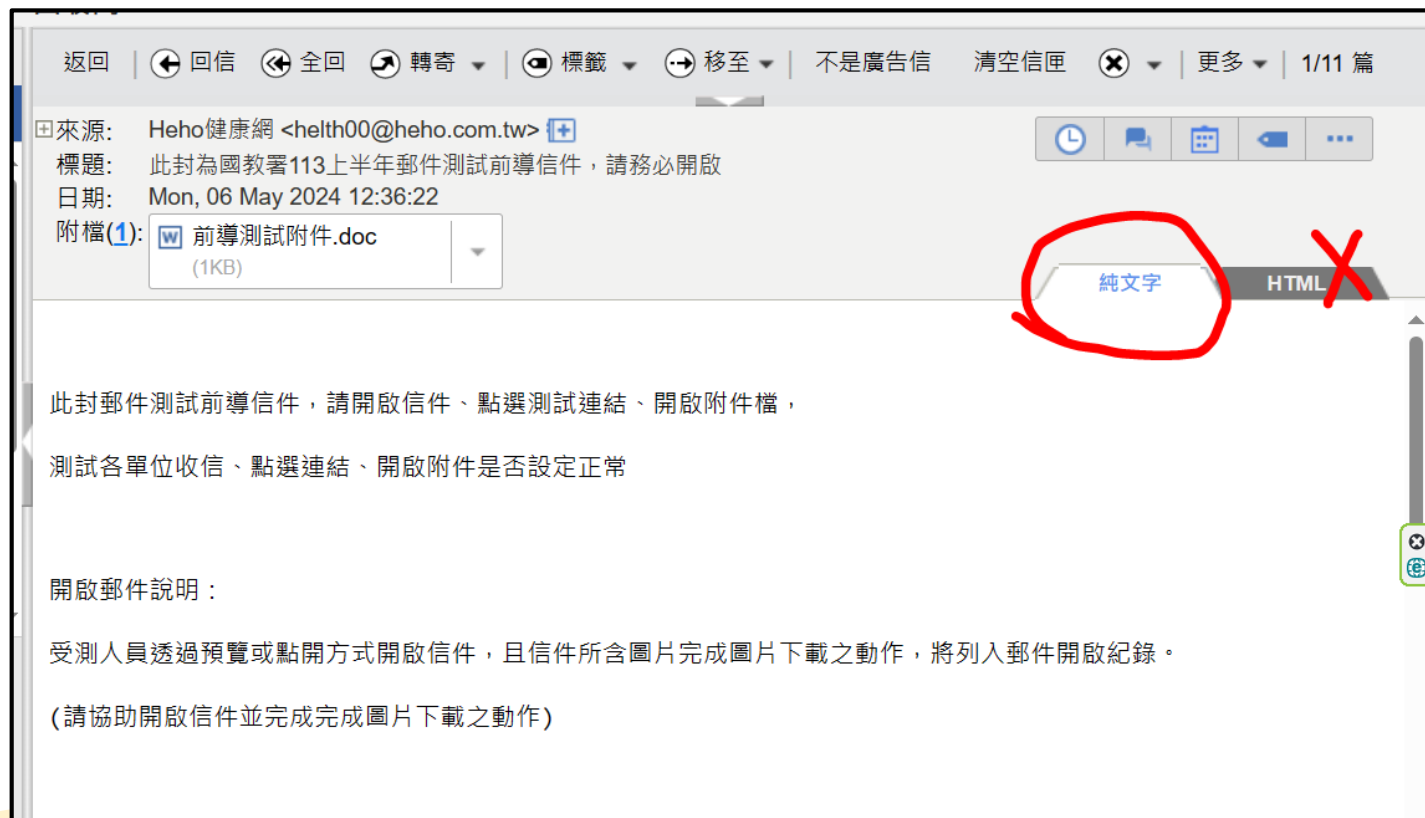
- 三不：不開郵件、不點連結、不下載附檔
- 收到信時，不要直接開啟
 - 先想一下是否應該收到此類型信件。
- 儘量不要使用教育雲端電子郵件收發非教學/學校事務之信件
 - 不要留郵件地址給其他網站...
- 手機收信，勿使用iPhone內建收信App，避免信件開啟誤判
 - 教育雲端電子郵件使用Apple手機收發信件時，請安裝Mail2000 App
- 郵件軟體，設定不【預覽】郵件內容，以純文字檢視
 - 降低風險

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

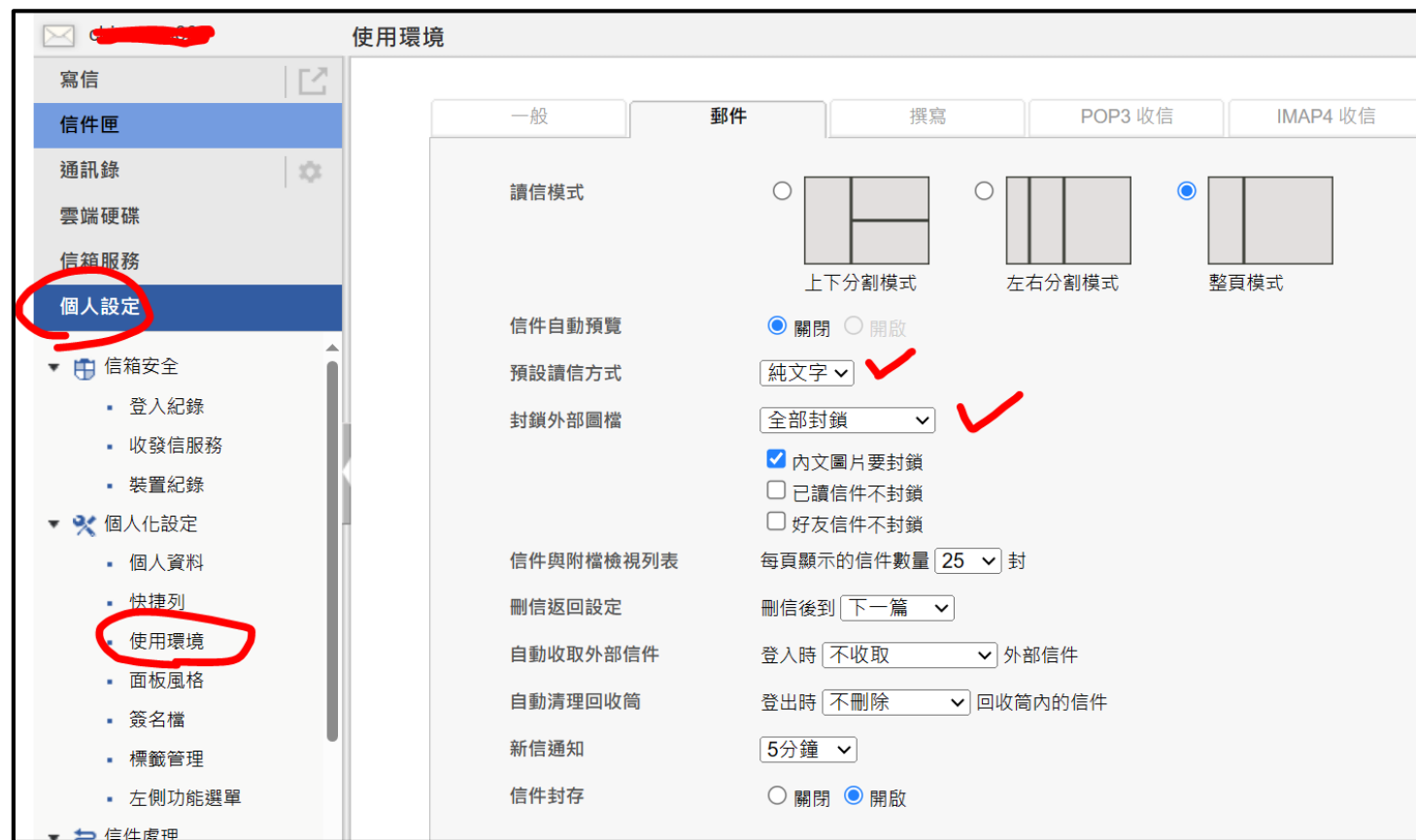


以純文字、不顯示圖片來檢視郵件

- 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

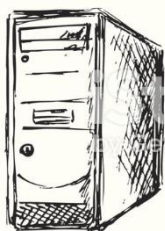
網路連結 - 點下去

Web

你以為會連到官網

其實是釣魚網站

CYVS Web



CVYS Web



嘉義高商
連結點下去



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

111資安研習通知.docx	2022/6/22 下...	Microsoft Wo
111資安研習通知.pdf	2022/6/22 下...	Chrome HTM
111資通安全教育訓練.pptx	2022/6/29 下...	Microsoft Po
96395275623d7fd15c25d.pdf	2022/6/28 下...	Chrome HTM
icon-gbceec635f_1920.png	2022/6/29 上...	PNG 檔案
lock-g670eb4b64_1280.png	2022/6/29 上...	PNG 檔案
password-ga00f553e6_1920.jpg	2022/6/29 上...	JPG 檔案
protect-ga1368a650_1280.png	2022/6/29 上...	PNG 檔案
security-g975c963b0_1920.jpg	2022/6/29 上...	JPG 檔案
security-g21282abf8_1920.jpg	2022/6/29 上...	JPG 檔案
security-gaf7103a6c_1920.jpg	2022/6/29 上...	JPG 檔案
text-gc2f6c13c5_1280.jpg	2022/6/29 下...	JPG 檔案
影片解析.txt	2022/6/28 下...	文字文件

本機磁碟 (C:) > Program Files > Microsoft Office > Office16

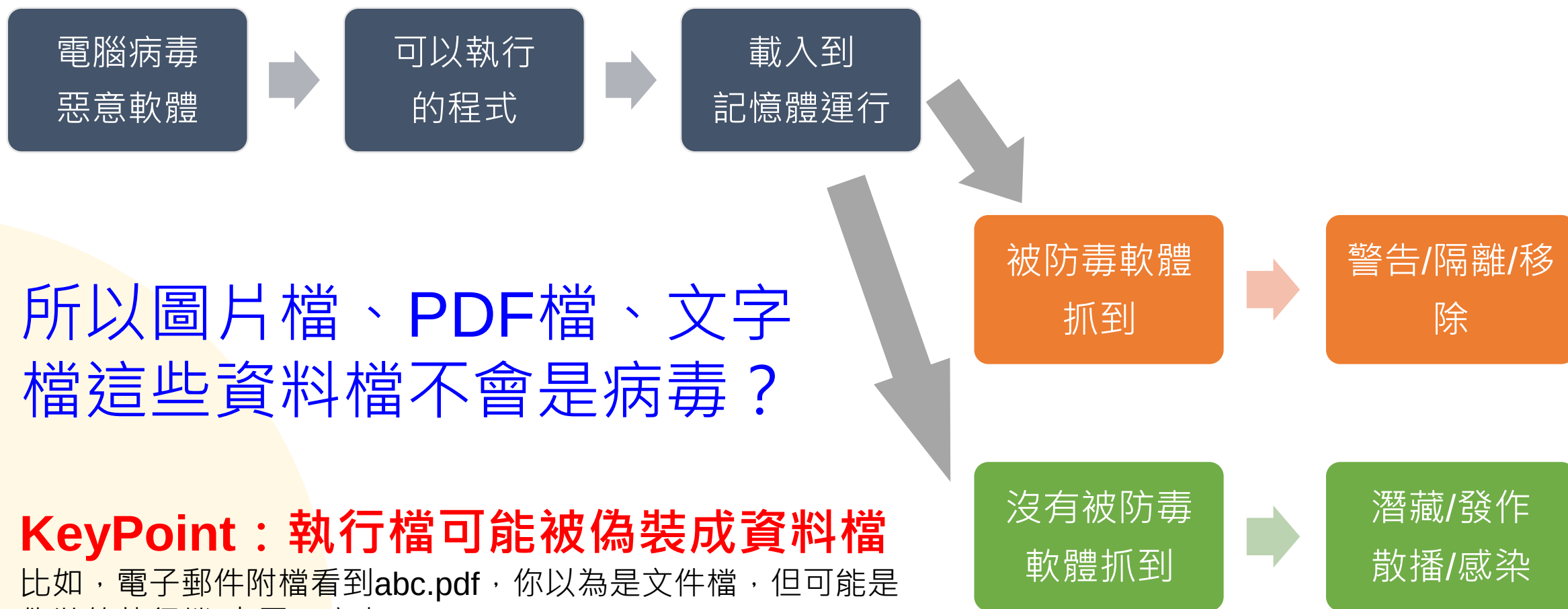
名稱	修改日期	類型	大小
windowsspeakerrecosdk.dll	2015/7/3...	應用	
WINWORD.EXE	2022/4/3...	應用程式	1,898 KB
WINWORD.VisualElementsM	2015/7/3	XML Document	1 KB

> 本機 > 本機磁碟 (C:) > Windows > System32

名稱	修改日期	類型	大小	檔案描述
mspaint.exe	2021/3/2 下...	應用程式	965 KB	小畫家
msra.exe	2021/7/19 上...	應用程式	579 KB	Windows 遠端協助

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

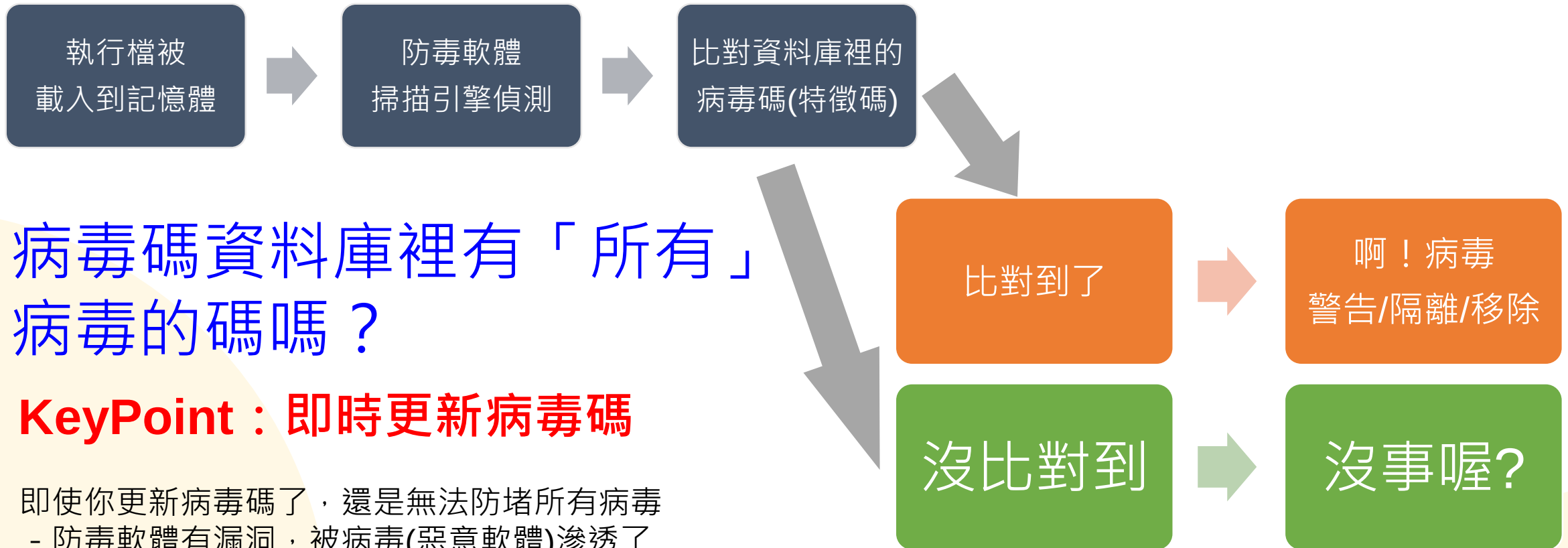


所以圖片檔、PDF檔、文字
檔這些資料檔不會是病毒？

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



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/>



雜湊演算法也是【數位簽章】中重要的一份子

Online Tools

MD5

MD5 online hash function

我是陳建文今年28歲

Input type

Hash ☒ Auto Update

1bce91039df64d68fc23a8b47cc9faa8

Hash	File Hash
CRC-16	CRC-16
CRC-32	CRC-32
MD2	MD2
MD4	MD4
MD5	MD5
SHA1	SHA1
SHA224	SHA224
SHA256	SHA256
SHA384	SHA384
SHA512	SHA512
SHA512/224	SHA512/224
SHA512/256	SHA512/256
SHA3-224	SHA3-224
SHA3-256	SHA3-256
SHA3-384	SHA3-384
SHA3-512	SHA3-512
Keccak-224	Keccak-224
Keccak-256	Keccak-256
Keccak-384	Keccak-384
Keccak-512	Keccak-512

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

名稱 ^

2023_1社交工程演練樣本.pdf
 2023_2社交工程演練樣本.pdf
 2023_社交工程演練教材.pdf
 2024_1社交工程前導測試郵件.pdf
 2024_1社交工程演練教材.pdf
 2024_1社交工程演練樣本.pdf
 2024_2社交工程演練教材.pdf
 2024_2社交工程演練樣本.pdf
 2025_1社交工程演練教材.pdf
 2025_1社交工程演練樣本.pdf
 2025_2社交工程演練樣本.pdf
 2026_1社交工程演練教材.pdf
 2026_1社交工程演練樣本.pdf