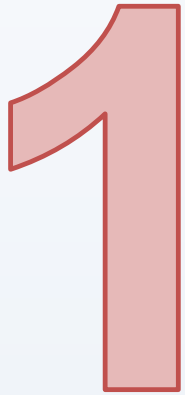
國立南科實中
114年度
資通安全研習

資通安全研習綱要

1. 前言
2. 資通安全相關法規
3. 資通安全概說
4. 資安風險與預防
5. 資安事故通報
6. 資安小叮嚀
7. 社交工程暨教育雲郵件
8. 其他注意事項
   - Google表單安全設定
   - 使用7z壓縮文件並設定開啟密碼
   - 學校公告榮譽榜、Win+L快速螢幕鎖定、PDF密碼保護、PDF滙出成圖片
   - 網路線不可回插

前 言



前言

依據資通安全責任等級分級辦法附表七：資通安全責任等級D級(本校目前級別)之各機關應辦事項內「認知與訓練」要求：「**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。」

數位學習平台

教師適用平台磨課師： https://moocs.moe.edu.tw/moocs/#/home

公務員適用e等公務園：https://elearn.hrd.gov.tw/mooc/index.php

S世代

- X, Y, Z 世代外的 Screen Generation: 滑啊滑
- S世代的年齡層?
- 滑出了些什麼問題 (Jamboard) ?

S世代

- 滑出了些什麼問題？
  - 網路成癮
  - 網路禮貌
  - 資訊安全
  - 網路詐騙
  - 忘了字怎麼寫了
  - 錢花光光

資通安全相關法規

資通安全相關法規

- 資通安全法(107年公告; 108年1月1日實施)
  資通安全法以公務機關及特定非公務機關(基礎關鍵設施)為主
  - 資通安全管理法施行細則
  - 資通安全責任等級分級辦法
  - 資通安全事件通報及應變辦法
  - 特定非公務機關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
  - 公務機關所屬人員資通安全事項獎懲辦法
- 個人資料保護法(112年修訂)：含公務及非公務機關
  - 個人資料保護法施行細則
- 著作權法
- 隱私權
- 肖像權

資通安全相關法規-著作權法

- 著作權法的重點在「什麼是合理的利用?」
  - 「散佈」才是問題的核心

資通安全相關法規-著作權法

- CopyRight <-> CopyLeft
- 合理的利用
  - 畢業影片內崁的歌
    著作權法第55條，非以營利為目的，未對觀眾或聽眾直接或間接收取任何費用，且未對表演人支付報酬者，得於活動中公開口述、公開播送、公開上映或公開演出他人已公開發表之著作。
  - 線上教學使用的教材https://www.lawbank.com.tw/news/NewsContent.aspx?NID=184800.00
- CC授權
- 網路著作權正義使者—林義傑
- 魚餌(引用圖片被告)

個人資料保護法

- 個人資料保護法
  - 民99年5月26日公告，101年實施部份條文，歷經104及112年兩次修訂，目前使用的是112年5月16日修訂版
  - 第27條非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
  - 第47條及48條對非公務機構之罰則
- 個資定義

  個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

個人資料保護法

- 特種個資：病歷、醫療、基因、性生活、健康檢查及犯罪前科
- 第 6 條：在「法律明文規定」、「公務機關履行法定義務」及「經當事人書面同意」等原因下才可蒐集特種個資。

個人資料保護法

- 「什麼是個資」列了20項，但重點是「其他得以直接或間接方式識別該個人之資料」
- 第15條:特定目的
  - 資料蒐集:學生、家長、教職員不必簽同意書, 但志工...
  - 班網貼團體照、公佈教師姓名
- 告訴乃論
  - 無論是故意或不小心都要陪 ，公務人員故意→加重 1/2 刑責
- 51條:家人間、公共場所拍的照片(別忘了還有民法之隱私權)
- 含個資之紙張千萬別回收；善用碎紙機

個人資料保護法

- 資料隱蔽

  依國家發展委員會103年12月31日發資字第1031501471號函

  為強化個資保護，各機關(單位)爾後如需於函文、網站及郵件表單等顯示民眾身分證編號者，請將其後4碼（即第7碼至第10碼）進行遮蓋，並以「*」取代，如另有特殊性用途需遮蓋其他碼或顯示全碼者，則依相關規定辦理。

  例:「劉O炫 A12345**** 」 名字中間及身份證後四碼隱匿

- 本校「網站公告內容審查暨電子表單個資蒐集管理辦法」

  https://hs.nnkieh.tn.edu.tw/modules/tad_book3/page.php?tbsn=13&tbdsn=121

Excel去識別化

=REPLACE(D2,2,1,"O")　**複製已識別化之儲存格-> 以「值」貼上**

	A	B	C	D	E	F
1	年	班	座號	姓名		
2	6	2	1	馬國賢	馬O賢	
3	6	2	2	張克帆	張O帆	
4	6	2	3	高山峰	高O峰	
5	6	2	4	綠茶	綠O	
6	6	2	5	梁赫群	梁O群	
7	6	2	6	王彩樺	王O樺	
8	6	2	7	王瀅	王O	
9	6	2	8	林立雯	林O雯	
10	6	2	9	佐藤麻衣	佐O麻衣	
11	6	2	10	郭彥均	郭O均	
12						

個人資料保護法

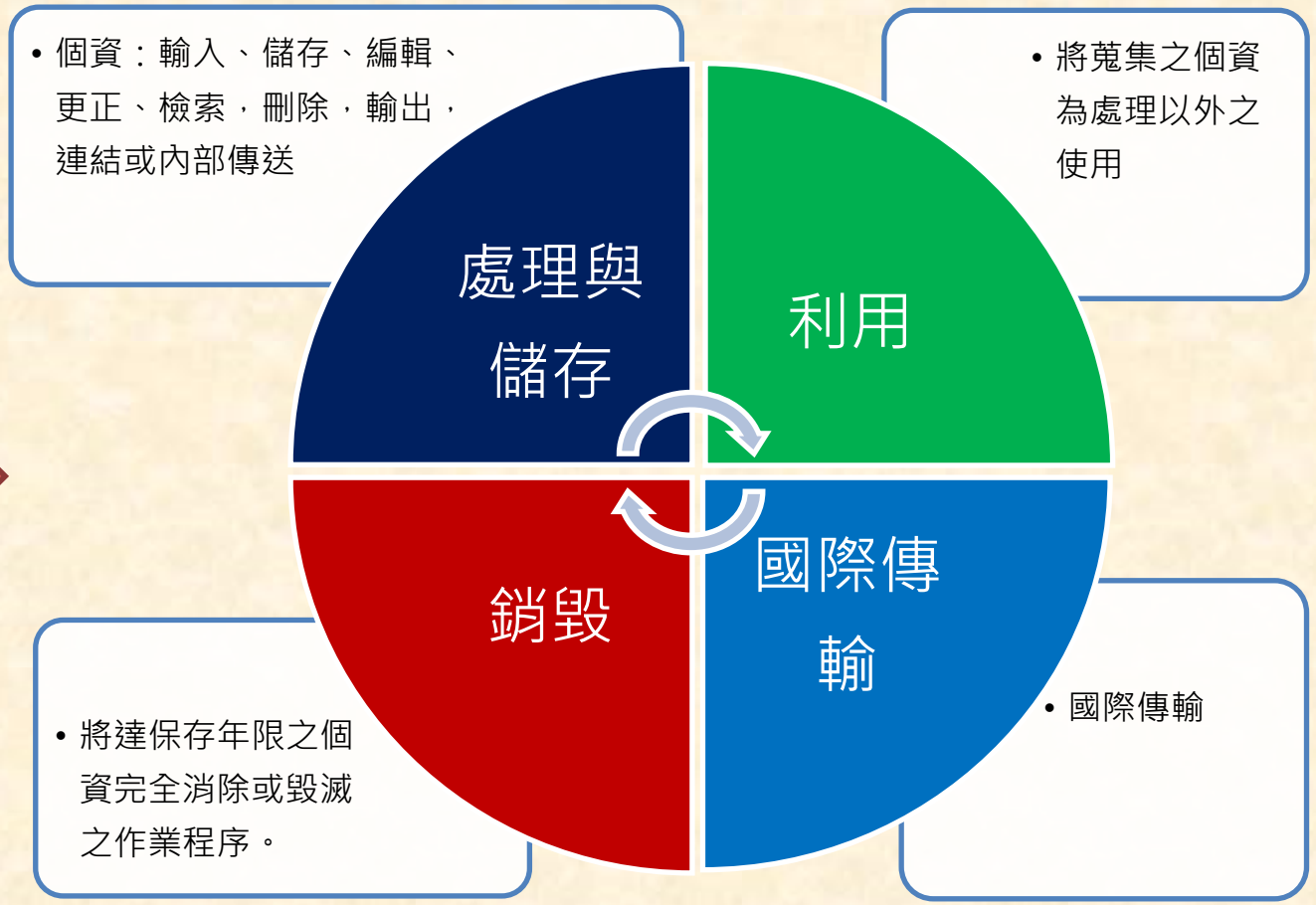
- Google 表單調查事項可否含「個資調查」??
- 依國教署臺教國署秘字第1110089333號公文附件揭露
  - 教育體系資安事件案例1
    國教署於110年3月份接獲外部情資單位通知，2所國立OO高級中學因誤將機敏個資之資料上傳至學校網站，致數百筆學生敏感個資外洩 (通報3級事件)
  - 教育體系資安事件案例2
    國立OO高級中學辦理學生相關業務時，於110年8月份因使用Google表單設定不當，致數百筆學生個資外洩 (通報3級事件)
- 變通做法
  1. 請儘量改用南市教資中心網頁（行政支援網頁）提供的調查系統。
  2. 若非用Google表單不可：表單之敏感個資改以紙本進行。
  3. 真的不行，一定得用Google表單詢問敏感個資，請自負法律責任。在表單設定上，必須學會「限制取得資料」之共用權限設定方式。

個人資料保護如何做

蒐集

以任何方式取得之個人資料

- 符合法定要件
- 履行告知義務
- 書面同意



個人資料保護如何做

- 個人資料保護管理制度建立
  - 個資保護政策及計劃之制定
  - 個資盤點及風險評鑑
- 個人資通訊設備使用：強化資通訊之安全管理
- 教甄、招生等業務取得之個資在活動結束後必須刪除。
  - 個資法11條：個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。
  - 個資法12條：公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

資通安全概說

資安相關影片

- DDoS 攻擊
  https://youtu.be/7kB9-nQJR44
- 破解 WIFI 密碼
  https://youtu.be/tKjVfGEoBZY
- 連 Google 都被駭！你還敢說自己很安全？自己的資安自己顧
  https://youtu.be/C07XolWPNSE
- 帳號被盜、個資外洩，加上假訊息攻擊！面對資訊戰你該怎麼做？
  https://youtu.be/Q58EN6PbPXA
- Targeted Cyber Attack Reality - Don't be a Victim - Trend Micro
  https://youtu.be/0hs8rc2u5ak
- 産業用制御システムが攻撃され、施設の生産は停止- Trend Micro
  https://youtu.be/6hmFmMXinvY
- 掃地機器人https://youtu.be/jhIMveZuYeo

資通安全概說—大綱

- 資通科技(ICT)：
  - 資訊 information
  - 通訊 communication
- 資通安全要素
- 請試著討論一下什麼是「資通安全」
- 組織要做些什麼?
- 個人要做些什麼?

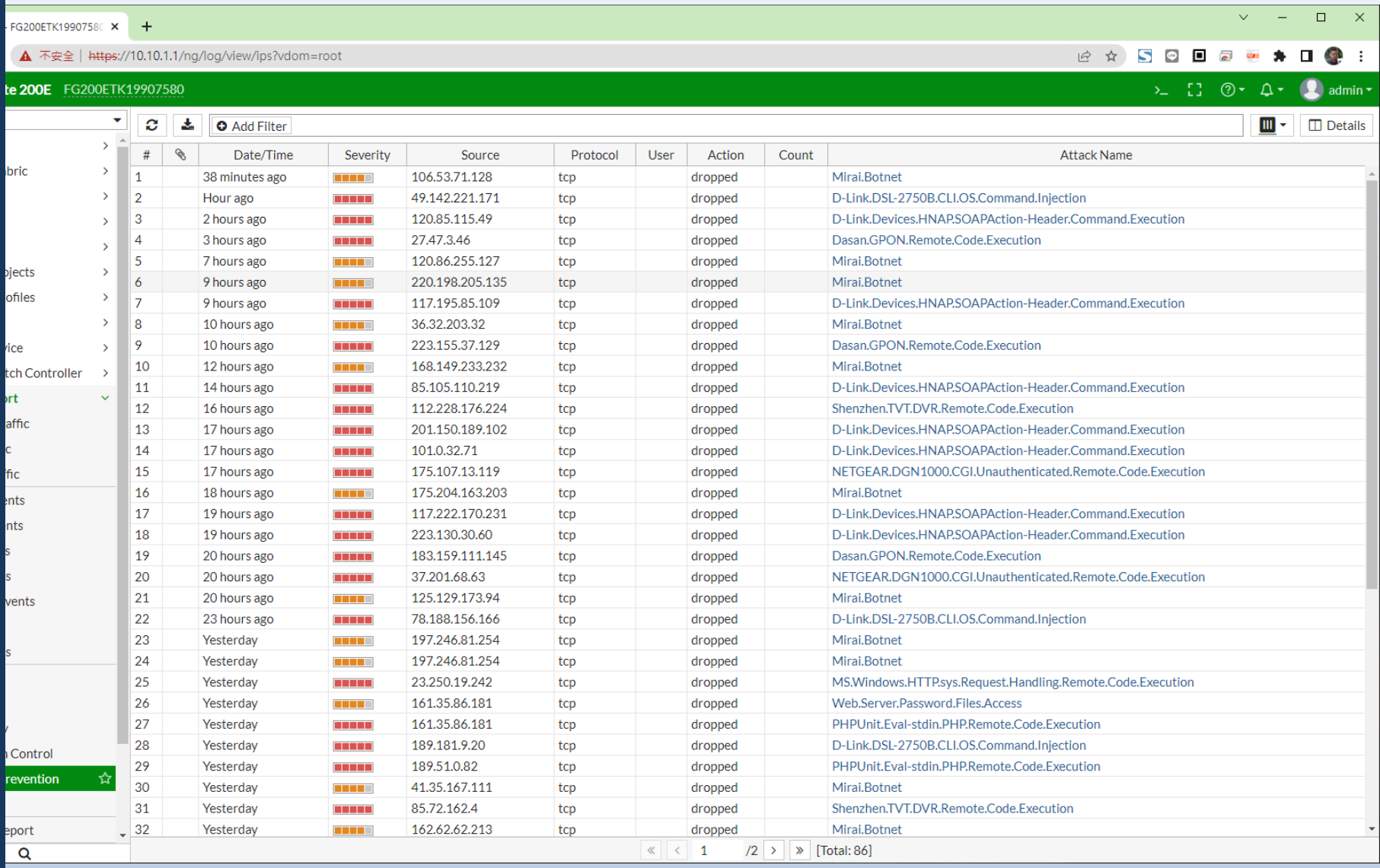
資通安全概說—資安三要素

- 資通安全三要素(資安稽核委員會抽問)
  - 機密性(Confidentiality)不讓資料遭未經授權者存取
  - 可用性(Availability) 在需要時，隨時可透過系統取得資訊
  - 完整性(Integrity) 資訊或系統維持正確性與完整性

資通安全概說-組織該作的事

- 網路出入口封包檢查
- 不當資訊檢查
- 當斷則斷
- 資通安全管理系統(ISMS)
  - 資通系統管理
  - 存取控制(網路安全、資通系統權限、帳號管理)
  - 作業與通訊安全管理(防惡意程式、遠端連線管理、電子郵件安全、實體環境安全、資訊設備使用安全)
  - 資通安全情資評估及因應
  - 資通系統委外管理
  - 資通安全教育訓練
- 本校資安專區裡關於「資通安全維護計畫」、「資安政策」及其他規定請務必要去瀏覽了解。
  https://hs.nnkieh.tn.edu.tw/modules/tad_book3/index.php?op=list_docs&tbsn=13

資通安全概說-組織該作的事



#	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1	38 minutes ago		106.53.71.128	tcp		dropped		Mirai.Botnet
2	Hour ago		49.142.221.171	tcp		dropped		D-Link.DSL-2750B.CLI.OS.Command.Injection
3	2 hours ago		120.85.115.49	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
4	3 hours ago		27.47.3.46	tcp		dropped		Dasan.GPON.Remote.Code.Execution
5	7 hours ago		120.86.255.127	tcp		dropped		Mirai.Botnet
6	9 hours ago		220.198.205.135	tcp		dropped		Mirai.Botnet
7	9 hours ago		117.195.85.109	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
8	10 hours ago		36.32.203.32	tcp		dropped		Mirai.Botnet
9	10 hours ago		223.155.37.129	tcp		dropped		Dasan.GPON.Remote.Code.Execution
10	12 hours ago		168.149.233.232	tcp		dropped		Mirai.Botnet
11	14 hours ago		85.105.110.219	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
12	16 hours ago		112.228.176.224	tcp		dropped		Shenzhen.TVT.DVR.Remote.Code.Execution
13	17 hours ago		201.150.189.102	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
14	17 hours ago		101.0.32.71	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
15	17 hours ago		175.107.13.119	tcp		dropped		NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution
16	18 hours ago		175.204.163.203	tcp		dropped		Mirai.Botnet
17	19 hours ago		117.222.170.231	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
18	19 hours ago		223.130.30.60	tcp		dropped		D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution
19	20 hours ago		183.159.111.145	tcp		dropped		Dasan.GPON.Remote.Code.Execution
20	20 hours ago		37.201.68.63	tcp		dropped		NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution
21	20 hours ago		125.129.173.94	tcp		dropped		Mirai.Botnet
22	23 hours ago		78.188.156.166	tcp		dropped		D-Link.DSL-2750B.CLI.OS.Command.Injection
23	Yesterday		197.246.81.254	tcp		dropped		Mirai.Botnet
24	Yesterday		197.246.81.254	tcp		dropped		Mirai.Botnet
25	Yesterday		23.250.19.242	tcp		dropped		MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution
26	Yesterday		161.35.86.181	tcp		dropped		Web.Server.Password.Files.Access
27	Yesterday		161.35.86.181	tcp		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
28	Yesterday		189.181.9.20	tcp		dropped		D-Link.DSL-2750B.CLI.OS.Command.Injection
29	Yesterday		189.51.0.82	tcp		dropped		PHPUnit.Eval-stdin.PHP.Remote.Code.Execution
30	Yesterday		41.35.167.111	tcp		dropped		Mirai.Botnet
31	Yesterday		85.72.162.4	tcp		dropped		Shenzhen.TVT.DVR.Remote.Code.Execution
32	Yesterday		162.62.62.213	tcp		dropped		Mirai.Botnet

1 /2 [Total: 86]

資通安全概說-組織該作的事

我只是平民老百姓為何會被攻擊

- **在聊聊個人該做些什麼前，要先了解風險之所在!**

- 資安風險演進

  磁碟片/硬碟開機病毒 -> 文件檔案病毒(巨集病毒) -> 網路芳鄰病毒 -> USB 病毒 -> 電子郵件中毒 -> 瀏覽網頁中毒 -> Line/Message…毒訊息

  破壞清洗 -> 拖慢速度 -> 網頁綁架 -> 偷密碼 -> 勒索

- 錢(暗網裡的黑交易)
  - https://nordvpn.com/zh-tw/blog/anwang-shi-shenme/
  - Tor 瀏覽器

電腦故障，還是中毒了~

- 前世今生
  - 以前：慢慢慢直到死亡
  - 現在： 最高品質—靜悄悄
- 密碼不保
  - FB、Line 密碼怎麼換就怎麼被猜中
  - 鍵盤側錄器是原凶
- 綁架
  - 首頁對岸化
  - 文件被加密
    http://www.bleepingcomputer.com/forums/t/563169/after-a-brief-hiatus-malware-developers-release-cryptowall-30/

凡事皆有價

SEPTEMBER 2019

THE ARMOR 2019 BLACK MARKET REPORT

A LOOK INSIDE THE DARK WEB

Extracts from one hacker's price list:

Black Market Service and Goods	Cost
U.S. Visa/Mastercard data (U.S. prices)	$15-$20 dollars (rising to $25-$30 for BIN number and DOB)
US Fullz data (Full ID package)	$30-$40
Generic Ransomware	$225 – $660
Ranion (Ransomware-as-a-service)	$120 per month
MegaCortex	$1000 or 1000 Euros and 10% of ransom
Unhacked Remote Desk Protocol Servers in multiple countries	$20 per RDP server
Amazon gift card with $1000 balance	$100
ATM skimmers	£500 to $1500
DDoS attack	$60 per hour
Money Transfer Services (PayPal, Bank Transfer, Western Union and Skrill)	Average of $800 for a balance of $10,000
Changes to credit history	From $130

暗網外洩個資價值

- 資安研究公司Privacy Affairs分析2021年暗網中個資類型產品於黑市上之價格變化與趨勢

暗網價格指數摘要

- 因虛擬貨幣市場交易活絡，虛擬貨幣帳戶成為最有價值的個資之一
- 隨著取得風險提高、信用卡資訊準確性提高等因素，信用卡與持卡人資訊價格呈現微幅升高
- 因應社群網站資安防護提升與供應管道增加，社群媒體帳號價值呈現下降趨勢
- 另考量隱匿性，黑市交易買賣逐漸摒棄使用比特幣(BTC)，改採門羅幣(XMR)進行支付

Crypto Accounts	Hacked Coinbase verified account	$610
	USA verified LocalBitcoins account	$350
	Crypto.com verified account	$300

Social Media	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Hacked Facebook account	$75	$65	-$10
Hacked Instagram account	$55	$45	-$10
Hacked Twitter account	$49	$35	-$14
Hacked Gmail account	$156	$80	-$76
Instagram followers x 1000	$7	$5	-$2

Product	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Cloned Mastercard with PIN	$15	$25	+$10
Cloned American Express with PIN	$35	$35	$0
Cloned VISA with PIN	$25	$25	$0
Credit card details, account balance up to $1.000	$12	$15	+$3
Credit card details, account balance up to $5.000	$20	$24	+$4

資訊外洩影響：來聊聊詐騙這一回事

- 公教人員個資—值多少錢?
- 在量販店填信用卡申請單送贈品—賺到了嗎?
- 加油站、百貨公司把你的信用卡拿去刷，我們安心在原地等?
- 被盜刷了怎麼辦?
- 網路購物安全嗎?

再由詐騙這一回事—來聊聊手機防廣告

- 手機廣告很討人厭，有沒有法子先知道對方是不是廣告商?
- 付費方案(Andorid, iPhone 適用)
  - Whos call
- Andorid 免費方案
  - Google電話
- iPhone 免費方案
  - 還是 whoscall, 但會有很多廣告…

再由詐騙這一回事—訊息查證

目前是是資訊爆炸的時代，有些訊息一看就很假，有些似真似假。以下幾個網站介紹給大家供訊息查證用。

- 官方的：台灣事實查核中心
  https://tfc-taiwan.org.tw/

- MyGoPen
  https://www.mygopen.com/

- 有使用Line的人, 可以加「Line訊息查證」為好友，查看貼文

- 若與食安或藥物相關訊息，可至衛福部食品藥物消費者專區查看
  https://consumer.fda.gov.tw/

資安相關新聞

- NCC發現小米10T 5G手機內建APP檢查政治敏感詞 有資訊回傳疑慮.
  https://www.cna.com.tw/news/firstnews/202201060387.aspx
- 超過1,200所美國K-12學校的學生資料曝露在暗網中
  https://www.ithome.com.tw/news/146685
- Bosch Rexroth智慧型扳手存在一系列漏洞，可被用於勒索或是RCE攻擊
  https://www.ithome.com.tw/news/160795
- 日本遊戲開發商Ateam Entertainment母公司公告近百萬人個資曝險長達6年，起因是Google Drive配置錯誤(知道連結...)
  https://www.ithome.com.tw/news/160693
- 如何關閉 Google 竊聽功能？
  https://www.techbang.com/posts/118265-how-to-turn-off-google-voyeurism
- 滲透？掃地機器人突播對岸廣播內容　女：嚇歪
  https://news.tvbs.com.tw/life/2742588

資安相關網站

- 漏洞通報平台
  https://zeroday.hitcon.org/
- 國家資通安全會報資安新聞專區
  https://www.nccst.nat.gov.tw/NewsRSS?RSSType=news
- iThome 資安專區
  https://www.ithome.com.tw/security
- 惡意檔案檢測中心
  https://viruscheck.tw/

資通安全風險與預防

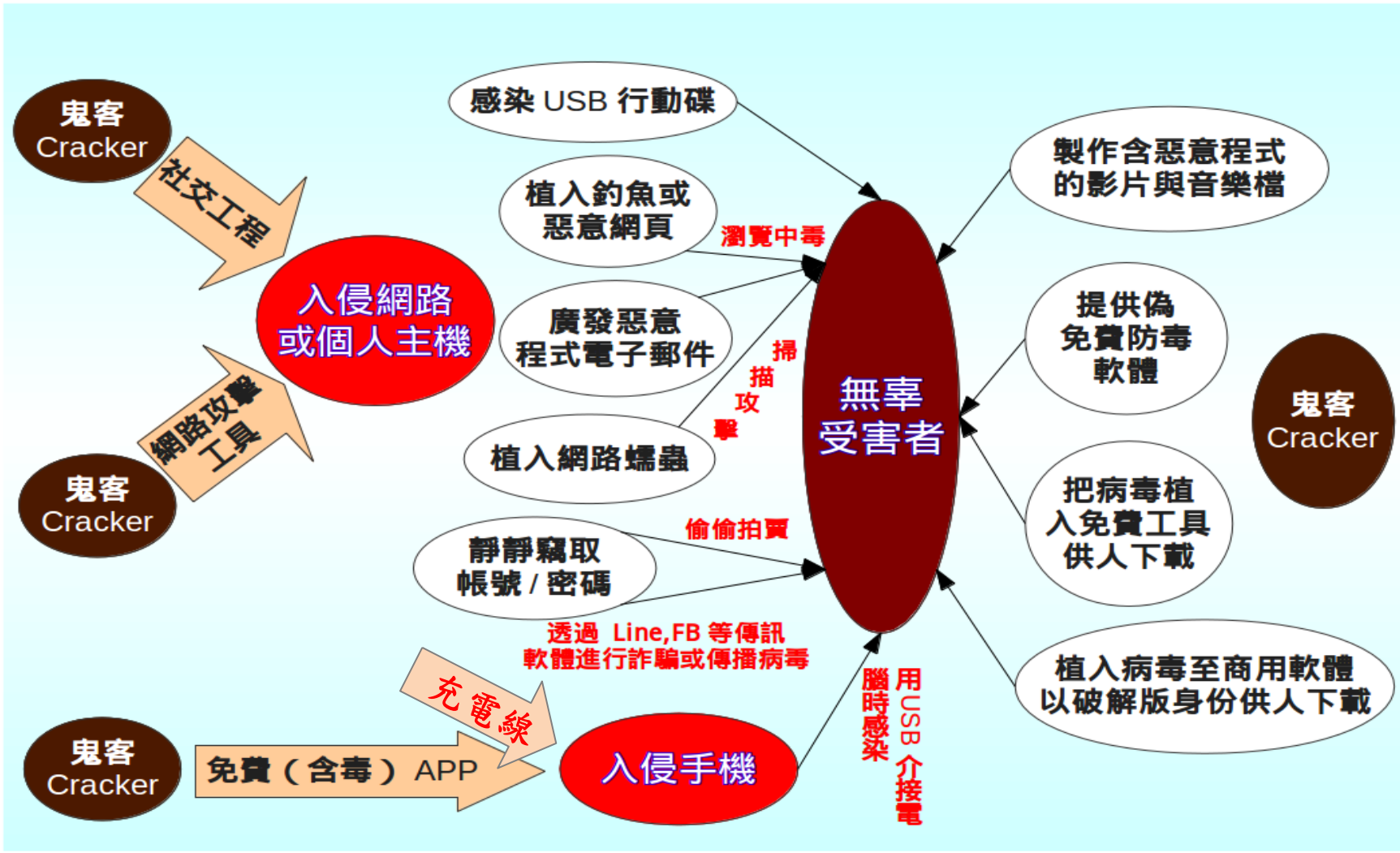
資通安全概說-個人資訊設備風險

- 請討論

請問個人資訊設備的使用，有何風險?

資通安全概說-個人資訊設備風險

- 實體安全：用電、雷擊...

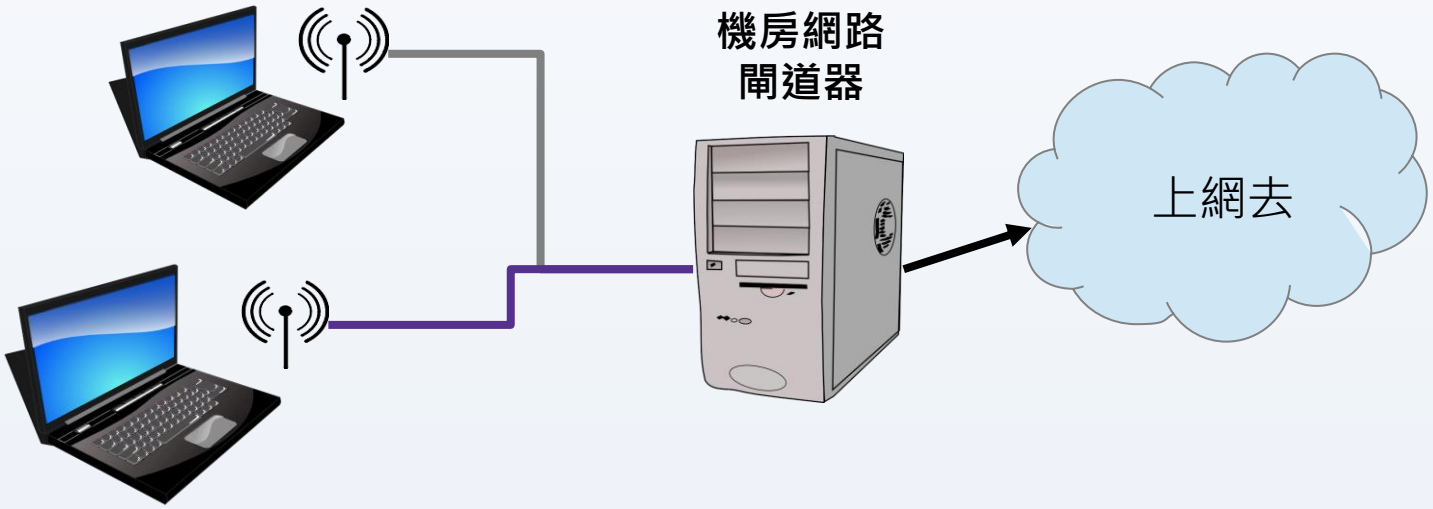


資通安全概說-個人資訊設備風險

- 手機接飯店USB孔充電「跳出傻眼通知」　嚇壞一票網友
  https://www.ftvnews.com.tw/news/detail/2024C15W0017
- 2.8萬存款被盜！專家解釋「用公共WiFi＝裸奔」帳密GG　網友秒懂
  https://www.ettoday.net/news/20180221/1116601.htm

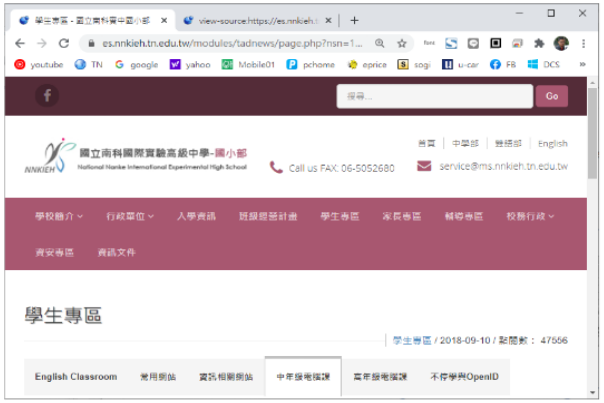
安全的瀏覽-公眾網路的風險

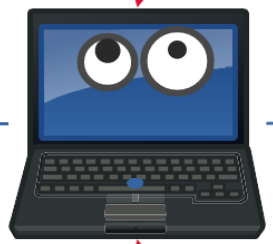
- 公眾網路
  - 咖啡廳/飯店...==>公共 wifi
  - 為了追劇 ==> 公眾 VPN
- 公眾網路架構



安全的瀏覽-什麼是「加密網頁」

- 防止上網資料被偷--瀏覽加密網頁
  - http:// ==> abcd 網路上→ abcd
  - https:// ==> abc 網路上→ e2fc714c4727ee9395f324cd2e7f331f
  - 所以FB, Yahoo, gmail, 銀行...登入時都是 https
- 加密特色
  - 用一數學公式，把某串字變成亂碼
  - 不可逆
- 綁架加密
  - 中毒後檔案被加密，不可逆，所以幾乎無解
  - 除非找得到解藥—加密時用的私鑰

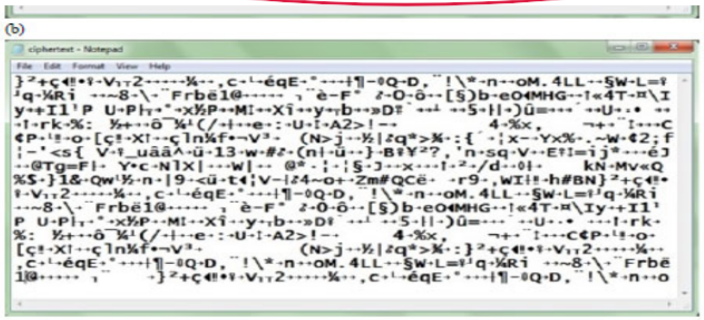




http://example.com

request web page

https://example.com



個人密碼是怎麼被偷的?

- 到系統上強制暴力破解
  - 所以要有圖片認證
- 個人電腦上植入鍵盤側錄病毒
  - 瀏覽含惡意程式的網站
  - 電子郵件含毒
  - USB隨身碟
- 社交工程
  - 千萬不要從提款卡到所有的網路服務，一組密碼通到底。

個人篇: 你該做些什麼?

思考一下: 為使資訊設備能更安全的使用，有那些事是我們該做的?

(Jamboard)

預防勝於治療

- 口訣：更新、防火、防毒、備份
- 有效的防惡意軟體
  - 可以免費，但先查評比，天下沒有永遠的贏家
  - http://www.av-comparatives.org/
  - 整體測試：Real-World Protection Tests
- 其他重點
  - 備份 (最好是分日期多份； 放在同一顆硬碟沒意義)
  - 不要亂下載：只要是電子檔，都可以藏毒
  - 免費的影音資源往往是最貴的
  - 螢幕鎖定（Win+L）、娛樂工作分離、鍵盤側錄器
  - 不要「亂點」; 不要看到QRCode就拍

誰在打我

- 檢查主機網路連線狀況
  - 一般個人電腦 -- tcpview
  - Windows Server 事件記錄器
  - Linux 及 macOS -- netstat
- 怎麼知道怪怪的連線是來自那裡??
  - https://www.abuseipdb.com/
  - https://www.whois365.com/tw/

資安事件通報

5

資安事件通報

- 南科實中通報應變文件 https://cloud.nnkieh.tn.edu.tw/nextcloud/index.php/s/35L3PLoxAMLSp4k
- 通知學校資訊單啟動應變流程
  1. 離線檢查
  2. 有救就救，沒救重灌。資料平時就備份…

資安小叮嚀

資安小叮嚀

- **共用電腦使用完畢，刪除完檔案，記得「清理資源回收桶」**
- 南科實中資安專區
  - https://hs.nnkieh.tn.edu.tw/modules/tad_book3/index.php?op=list_docs&tbsn=13
- 公務電腦必須設置密碼：設定 / 帳戶 / 登入選項
  - 至少8碼; 英數字大小寫並存
  - 暫時離開座位要螢幕鎖定(Win+L)
  - Google、Facebook等平台設定成兩階段認證
- 自帶個人網通設備介接學校網路必須向資訊室申請

  (依規定個人設備不得介接學校網路)

資安小叮嚀

- 實體安全
  - SSD硬碟風險
  - 筆電充電原則
- 備份

  不止只備一份, 要有分時備份的觀念。例如: 三週前、兩週前、每天的。

  用三顆不同的隨碟來備份。以應付勒索病毒。
- 電腦送修
  - 刪除了，就安心了嗎? (陳O希)

資安小叮嚀

- 大陸品牌之資通設備不得介接學校網路。拿大陸品牌手機平板的同仁，希望在未來汰除更換時，改買非大陸品牌。
  大陸品牌: 小米、POCO、OPPO、Vivo、OnePlus、華為、Realme、Sugar、聯想、Motorola(聯想)、TP-Link、海康威視…等
- 當有業務需求到其他同仁的公務電腦前，當同仁要輸入密碼查詢時，請勿一直站在當事人旁邊或後面。會造成當事人極大的心理壓力。

社交工程暨教育雲郵件

社交工程攻擊

- 先看個影片吧!
  - 網路釣魚
    https://www.youtube.com/watch?v=WNVTGTrWcvw
  - Trend Micro宣導影片：利用社交工程攻擊的入侵過程
    https://youtu.be/0hs8rc2u5ak
- 社交工程攻擊
  - 利用人性弱點，騙取機敏資料的過程。
  - 古代：打電話偽裝成長官
  - 現代：使用簡訊、Line、Message及e-mail等方式，以「假到很真」的訊息騙取我們點含惡意程式連結盜取機敏性資料。
- 社交工程攻擊信件特色
  - 寄件者很真實，因為寄件者郵件是可以偽造
  - 大多會要求點連結、檢視附件
  - 與當下的新聞實事很貼切，但公告的人不是學校相關單位

社交工程攻擊案例

偽冒肺炎疫情通知，開啟電郵的附件檔案後，會執行惡意程式!!

取自:電子郵件安全與社交工程防護研習講義(劉得民, 2022, P.13)

社交工程攻擊案例


Guest 5755
上午10:07
*7P Media AI部門會自動通知您
我們收到 1 份報告。 您的帳號違
反了 Facebook 的政策和社群標準
如果您認為我們犯了錯誤，您可
以對暫停提出申訴
申訴連結：{{ https://
mt-max-suppott.pages.mus.br/
sp-mt-taiwan-886 }}
依照螢幕上的指示提交申訴
請注意，在某些情況下，我們可
能不會在停用帳戶之前發送警
告。 我們也無法恢復因嚴重違規
而被暫停的帳戶。 詳細了解我們
如何偵測嚴重違反 Facebook 社群
標準政策的行為。
臉書團隊！


Invitato 7725
下午8:26
我們已通知您您的個人資料有問
題。 但還沒收到你的回覆。 請依
照連結中的說明進行：
https://shorter.me/jsMVg
取得專家協助。 如果我們沒有收
到您的任何回復，我們將被迫無
限期暫停您的個人資料。
專家團隊！

社交工程攻擊現代式 -- AI時代詐騙

- Deep Fake ：深度偽造
  - 就是換臉、換聲音
    你接到親人的電話，不一定是真的那個人。小心被騙．．．
    https://www.typd.gov.tw/index.php?catid=551&cid=25&id=183&action=view&pg=3#gsc.tab=0
  - 免費工具介紹
    https://tw.cyberlink.com/blog/photo-editing-tips/3039/deepfake-tools
  - 面貌聲音都能偽造 陸「AI半臉」詐騙新手段｜TVBS新聞
    https://www.youtube.com/watch?v=oI_WaB_5654
  - 老師在說，你都沒有在聽！深偽名人影音
    https://www.youtube.com/watch?v=s0-h6BUyKpQ
- AI助攻Email詐騙2025年將會大爆發 如何避免成為受害者？
  https://www.technice.com.tw/techmanage/infosecurity/158253/

社交工程攻擊預防

- 訊號內文的合理性
  - 郵件標題之合理性?
  - 親友/朋友會討論的話題嗎?
  - 話題夠誇張，令人不可思義!
- 訊號內文要我們所點的超連結的網址與所述機構網址一致嗎?
- 短網址值得信任嗎?
  - 從短網址看不出原網址
  - 點了就中招了...
- 郵件寄件者合理嗎?
  - 是該機構寄出的嗎?
- 破解; 免費; 大減價; 通常最費錢。

社交工程演練

- 教育部國民及學前教育署對國立學校教職員工的教育雲郵件演練
  - 從各校挑出35名人員
  - 歷程約一至兩個月，寄四到五封信
- 演練目標
  - 社交工程郵件開啟率：各次演練作業，各演練對象開啟率應低於10%。點了郵件標題，看到內容就中招。
  - 社交工程郵件連結點閱率：各次演練作業，各演練對象點選率應低於６％（含）。點了郵件內容所附之超連結。
  - 社交工程郵件附件開啟率：各次演練作業，各演練對象附件開啟率應低於2%(含)。開了郵件附件。

社交工程演練

113年5月份國教署社交工程演練信件

信件編號	信件主旨	寄件者
01-協作邀請	有人與你共用了試算表：「2024 人事異動 ver2.3」	Google Drive drive-share@google.com
02-終身學習	公務人員每人每年必須完成之課程及其時數	e 等公務園+學習平臺 e.learning@hrd.gov.tw
03-LINE 神器	LINE 偷吃抓包密技：教你查出對方所有通話記錄和隱藏對話	網路溫度計 service@dailyview.tw
04-韓國旅遊	【2024 韓國景點】15 個首爾旅行必去、IG 打卡點總整理！	Klook supporttravel@klook. com

社交工程演練

113年12月份國教署社交工程演練信件

信件編號	信件主旨	寄件者
01-好市多	好市多線上購物 訂單收到通知	Costco Taiwan costcotp@email.costco.com.tw
02-行李理賠	行李託運前別忘做一個小動作！ 旅遊保險專家：重要理賠關鍵	ETtoday 新聞雲 appservices@ettoday.net
03-國外出差	國外出差注意事項	hr2024 hr2024@mail.k12ea.gov.tw
04-加薪通知	十二月份加薪通知	人力資源部 hr@mail.k12ea.gov.tw

社交工程演練預防

- 以純文字方式開啟郵件
  - 直接以網頁型式開啟郵件內容，會偷跑一些眼睛看不到的東西，例Javascript。
  - 有些郵件內崁圖片/影片/音樂內含惡意碼，在開信的一瞬間讓讀信軟體當掉，病毒也就被放了出來。
- 手機/平板可用Mail2000 APP收發教育雲信件
  - 把教育雲的信轉到其他平台(尤其是Apple)，會有「轉信即已閱讀」的扣分可能性。
  - 要即時掌握訊息，可安裝Mail2000 APP。

社交工程演練預防：教育雲

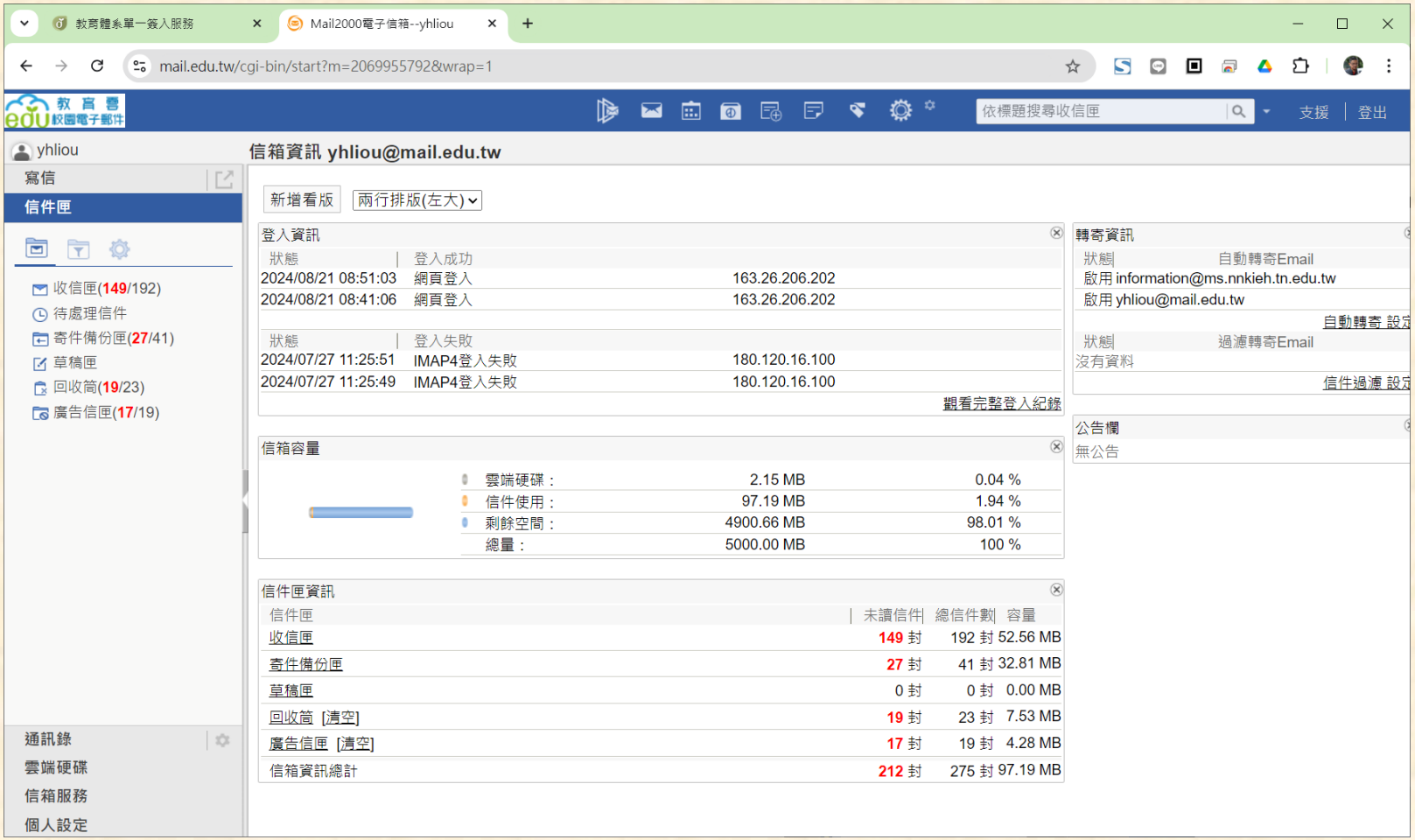
https://mail.edu.tw

社交工程演練預防：教育雲

https://mail.edu.tw

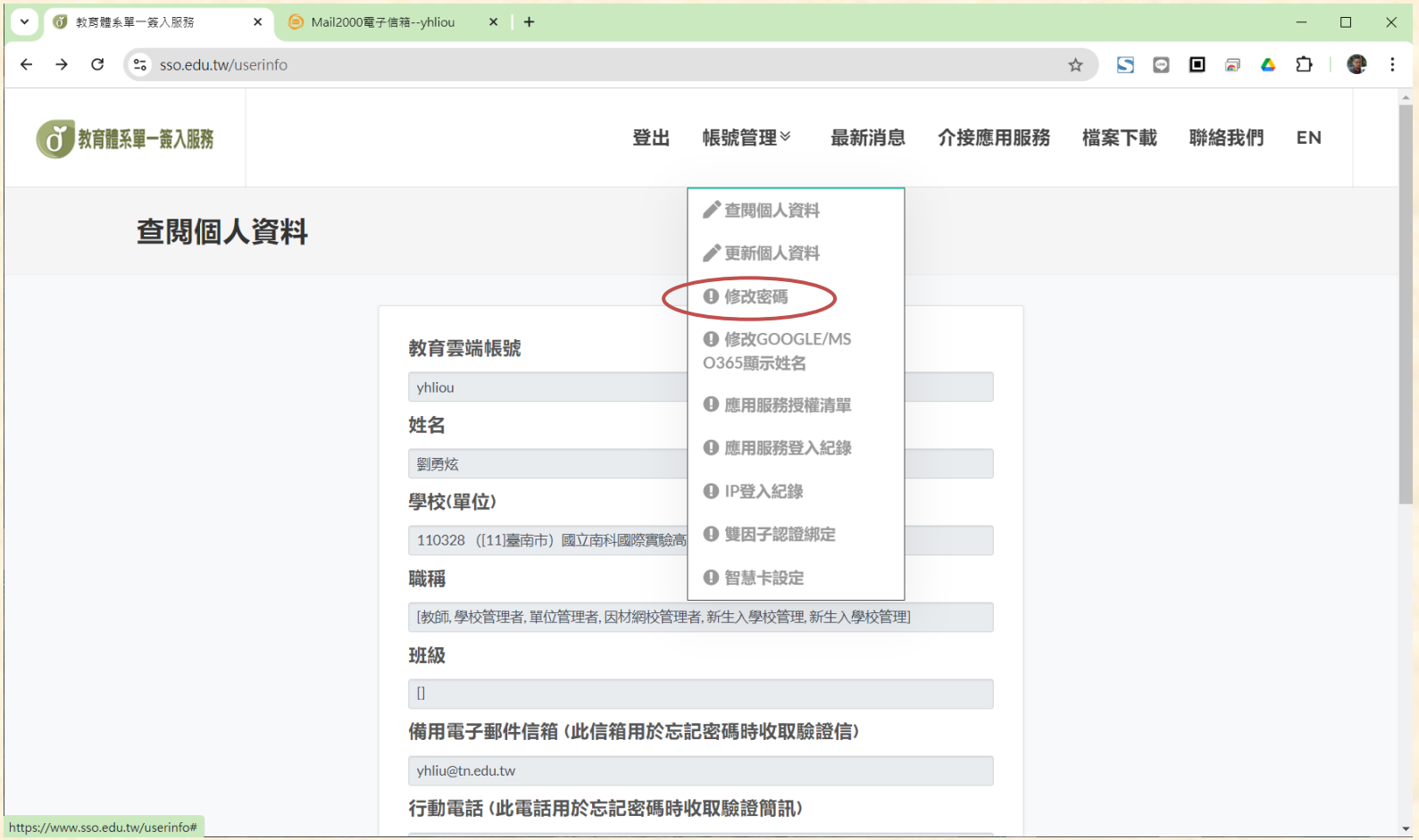
社交工程演練預防：教育雲

https://mail.edu.tw

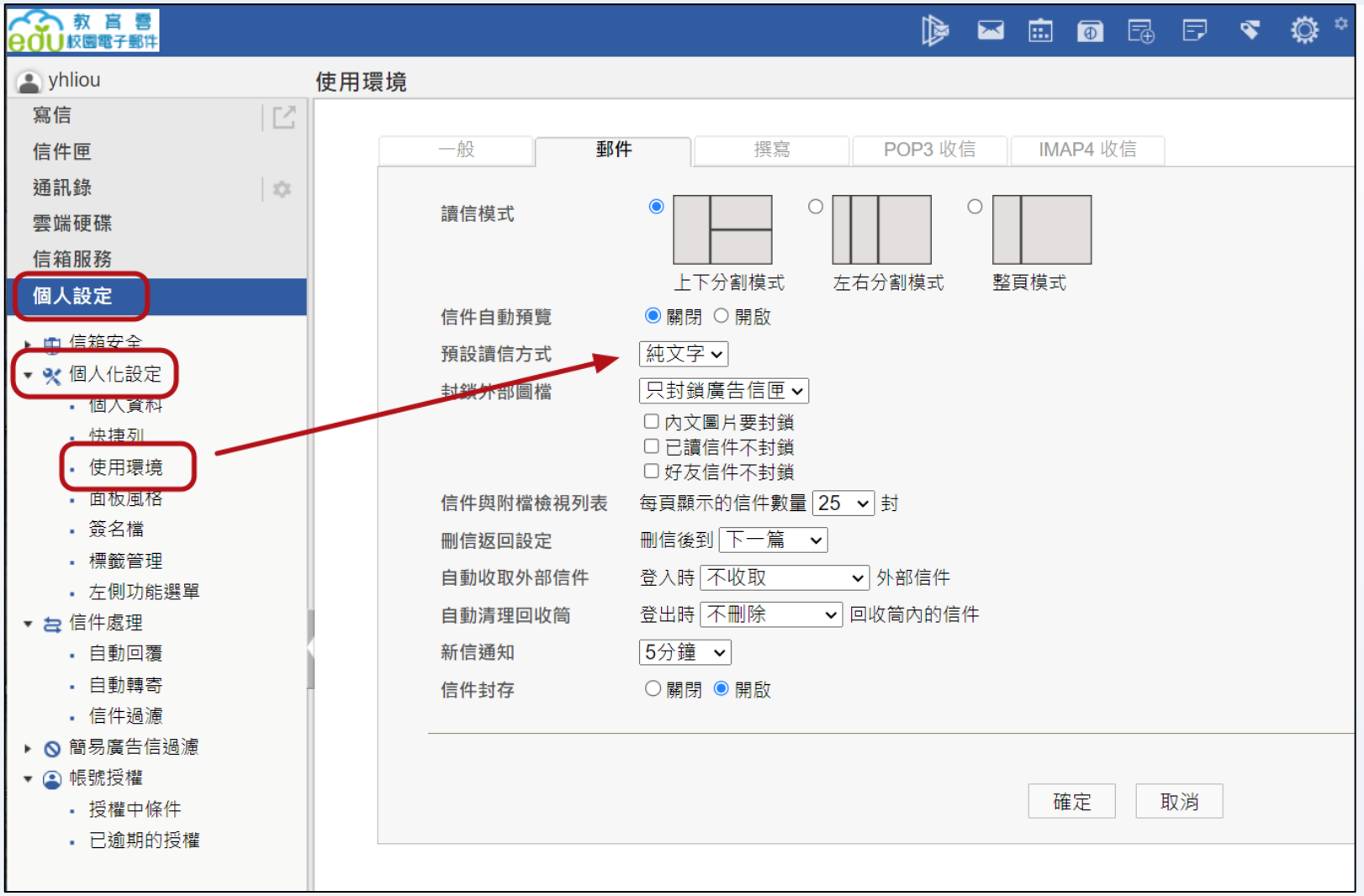


社交工程演練預防：教育雲修改密碼

https://www.sso.edu.tw/userinfo



社交工程演練預防– 以純文字方式開啟郵件



社交工程演練預防—取消勾選自動轉寄

社交工程演練預防

@Mail2000 APP

其他注意事項

學校使用資通系統或服務蒐集及使用個人資料注意事項

一、教育部為保護教職員、學生、家長之權益，特訂定學校使用資通系統或服務蒐集及使用個人資料注意事項（以下簡稱本注意事項）。

二、各級學校為行政目的使用資通系統或服務蒐集教職員、學生、家長之個人資料者，應遵循個人資料保護法相關規定並參酌本注意事項辦理。但各直轄市、縣（市）政府另有規定者，其所轄學校從其規定。

三、學校為行政目的使用資通系統或雲端資通服務（如 Google 表單、Microsoft Forms 等問卷調查服務）涉及蒐集個人資料者，應注意下列事項：

（一）資料蒐集最小化：僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，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。

（二）存取控制：應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。

（三）使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容（如 Google 表單不應勾選「顯示摘要圖表和其他作答內容」），避免使用者能瀏覽其他使用者資料，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。

學校使用資通系統或服務蒐集及使用個人資料注意事項

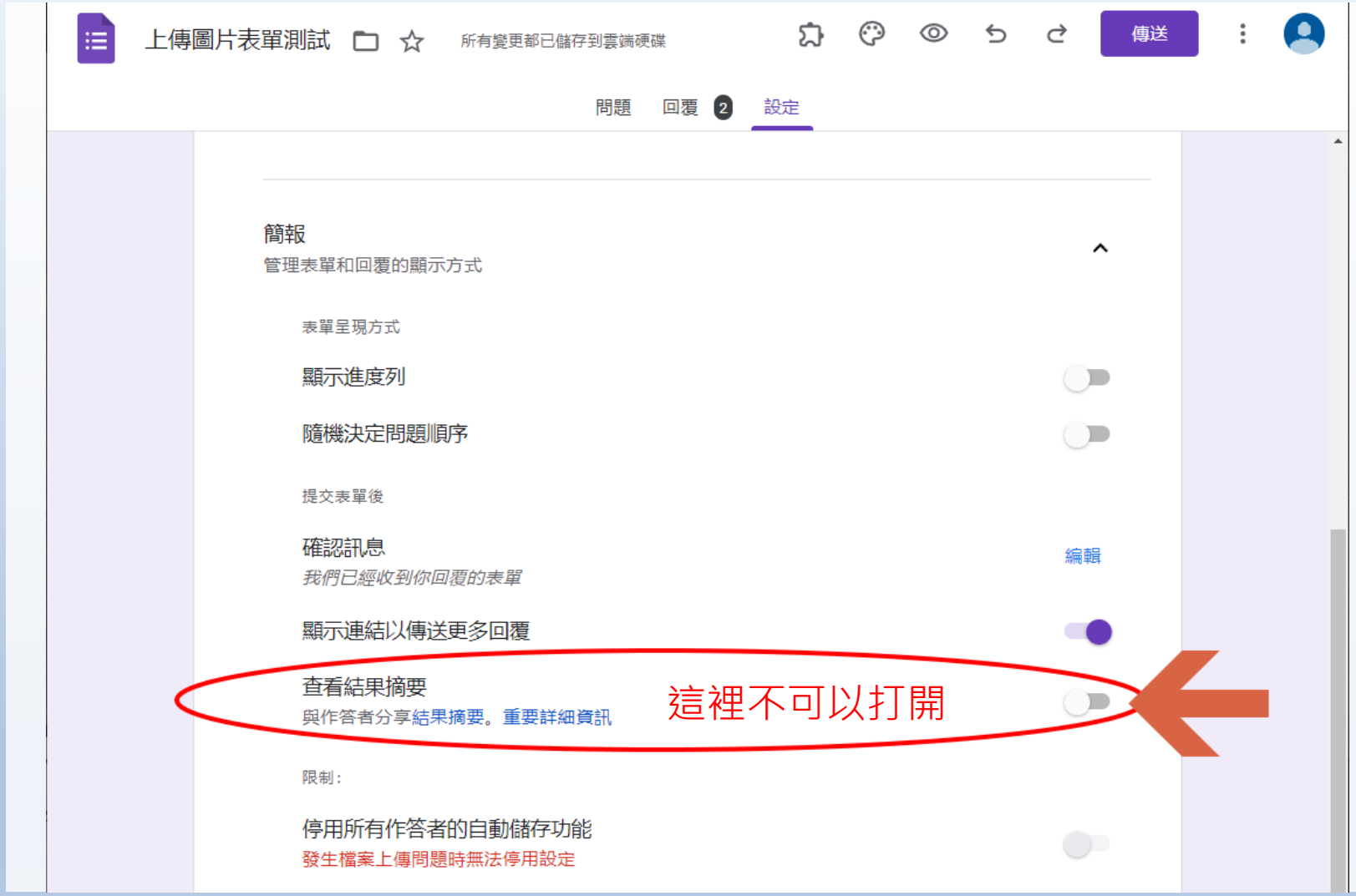
（四）傳輸之機密性：網路傳輸應採用網站安全傳輸通訊協定（HTTPS）加密傳輸，並使用 TLS 1.2 以上版本傳輸。

（五）資料儲存安全：如涉及蒐集個人資料保護法第 6 條之個人資料或其他敏感個人資料，應以加密方式儲存。

（六）應訂定個人資料保存期限，並於期限或業務終止後將蒐集之個人資料予以刪除或銷毀，避免個人資料外洩。

四、各校或其主管機關得依本注意事項，訂定各校相關作業流程規定。

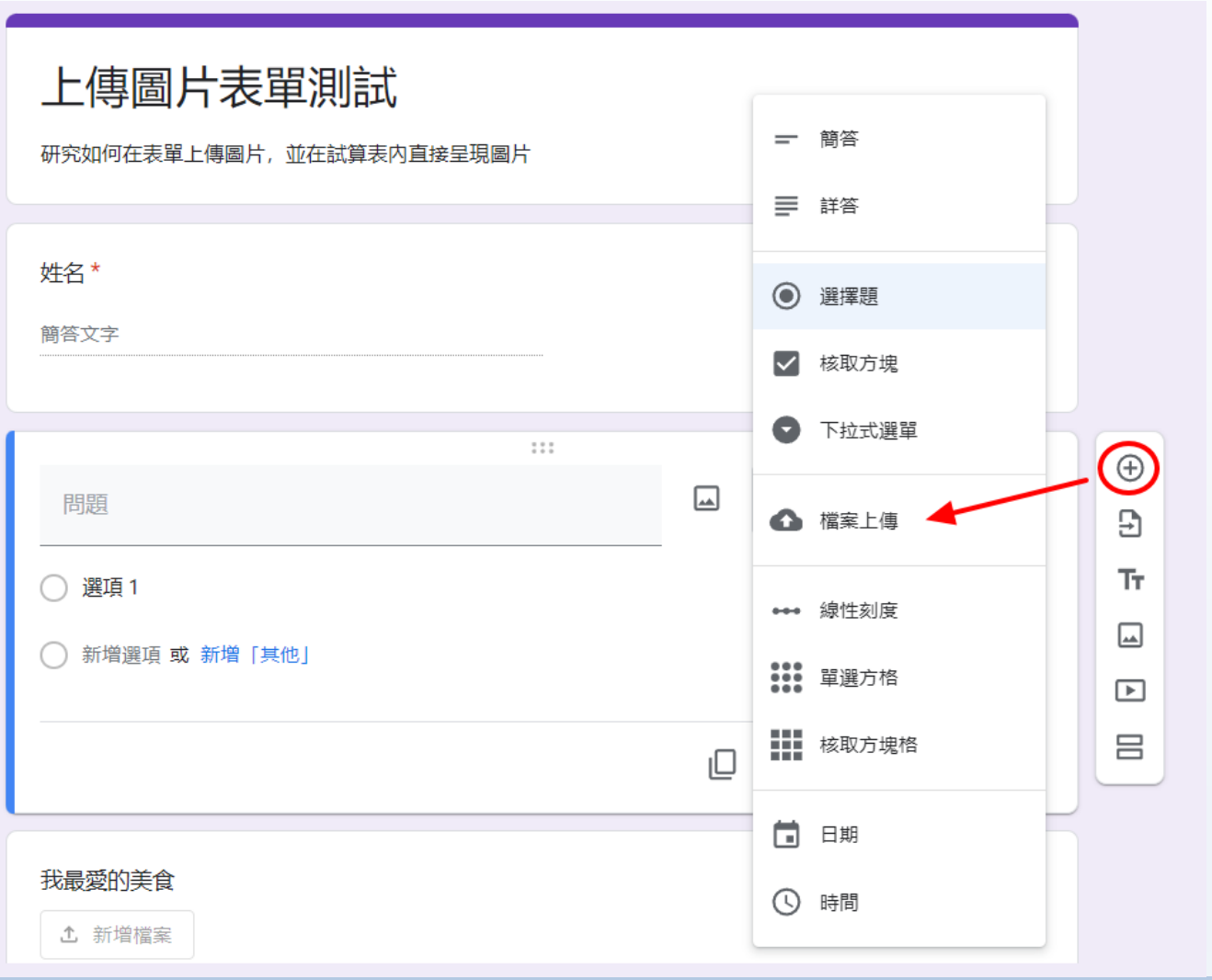
其他：Google表單安全設定



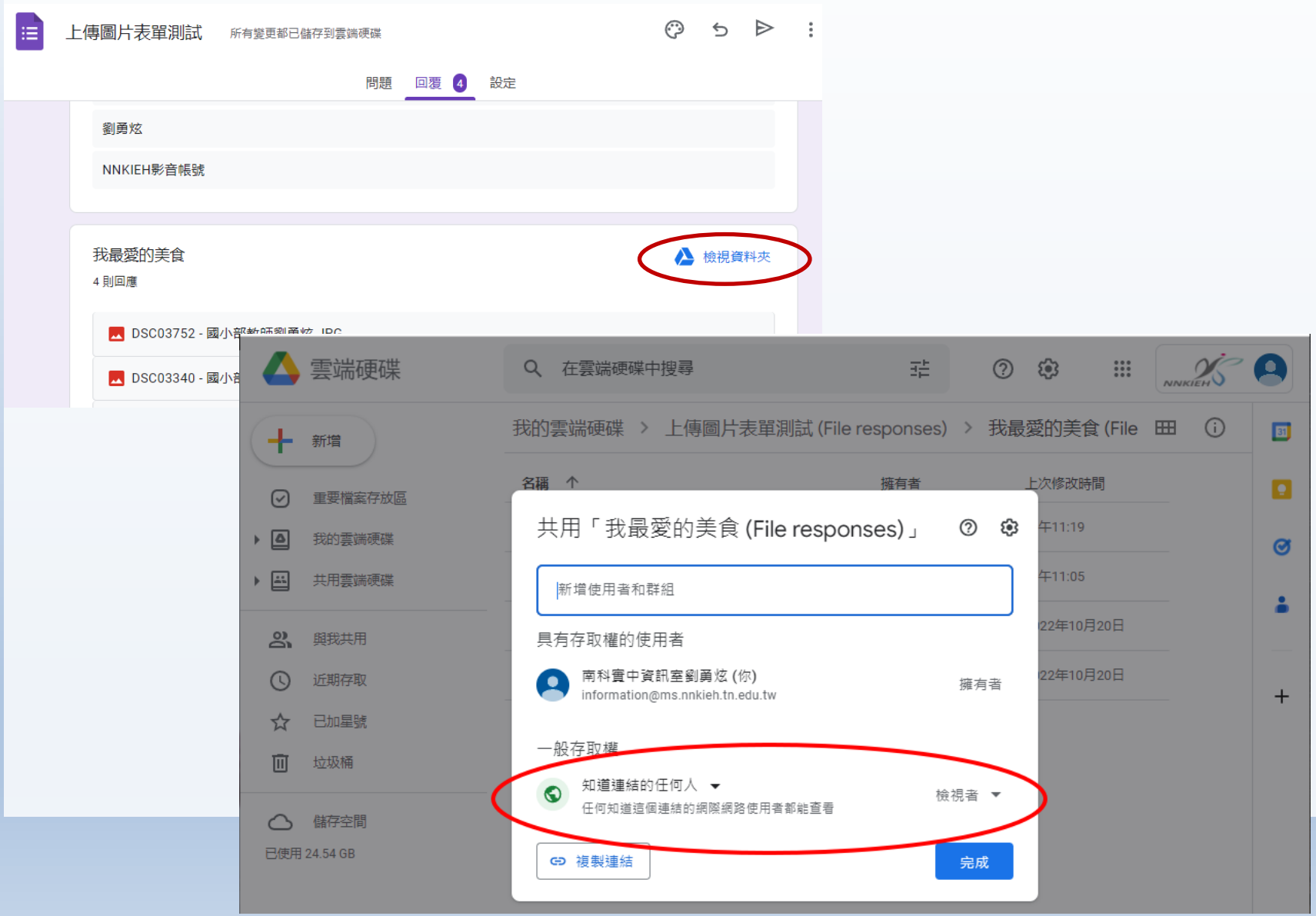
其他： Google表單安全設定

打開「查看結果摘要」後幾乎等於公開其他人的填答內容。

其他： Google表單—在結果試算表中秀圖片
Step1: 設計可上傳檔案的欄位



其他： Google表單—在結果試算表中秀圖片
Step2: 資料夾「知道連結的共用設定」

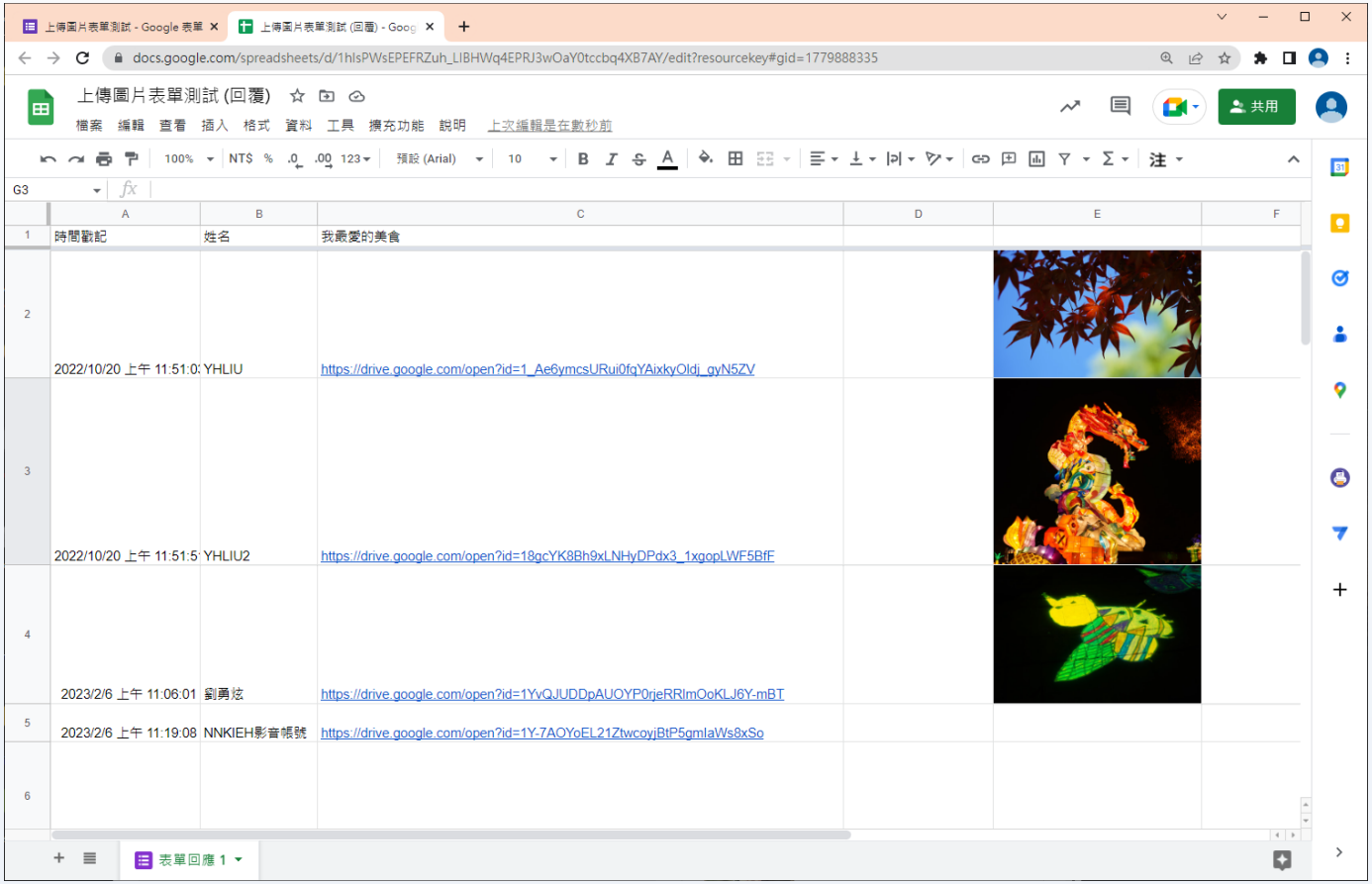


其他： Google表單—在結果試算表中秀圖片
Step3: 在試算表中查看

其他： Google表單—在結果試算表中秀圖片

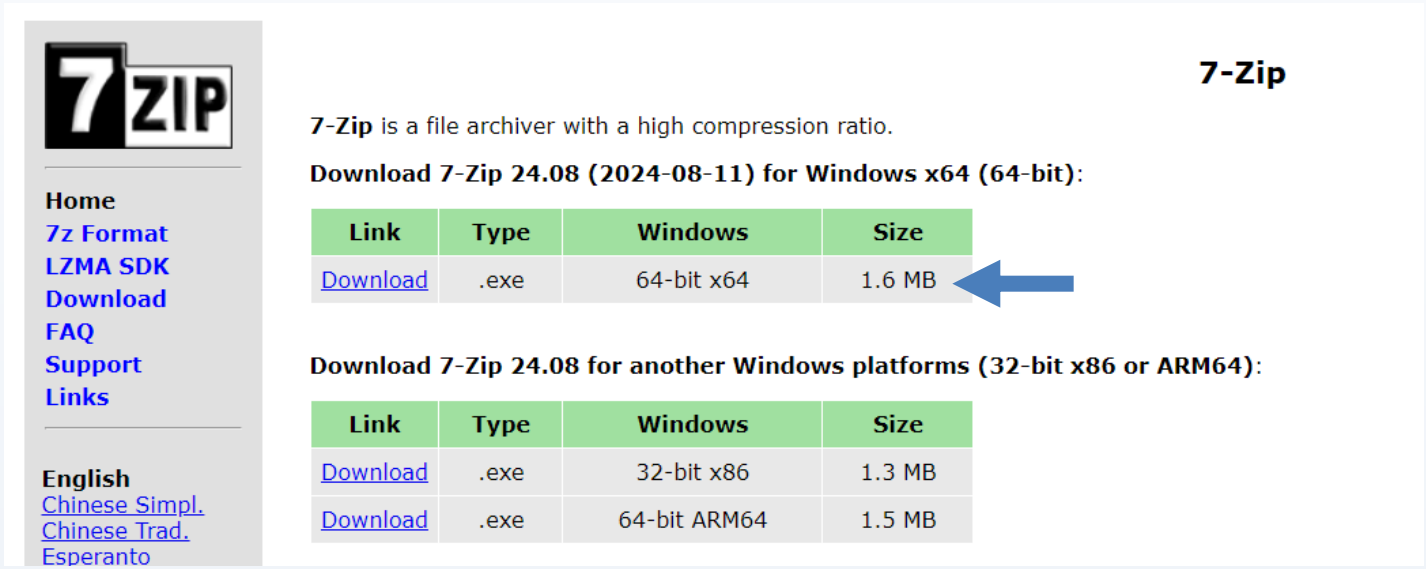
Step4: 在試算表中，在儲存格加上可顯示圖片的公式

```
=image("https://drive.google.com/uc?export=view&id=" & right(C2,33),2)
```



其他：使用7z壓縮文件並設密碼

7z下載
https://www.7-zip.org/



7-Zip

7-Zip is a file archiver with a high compression ratio.

Download 7-Zip 24.08 (2024-08-11) for Windows x64 (64-bit):

Link	Type	Windows	Size
Download	.exe	64-bit x64	1.6 MB

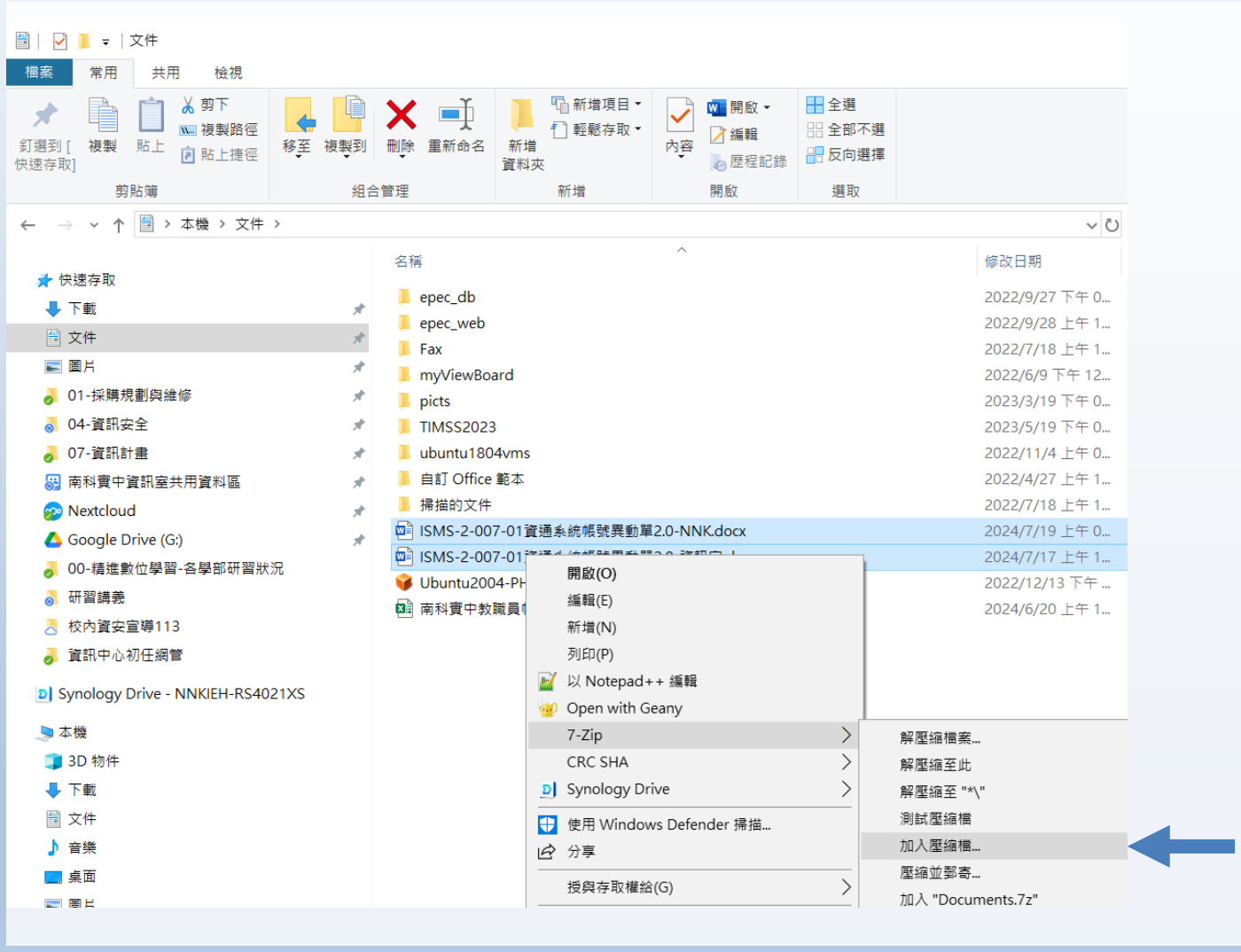
Download 7-Zip 24.08 for another Windows platforms (32-bit x86 or ARM64):

Link	Type	Windows	Size
Download	.exe	32-bit x86	1.3 MB
Download	.exe	64-bit ARM64	1.5 MB

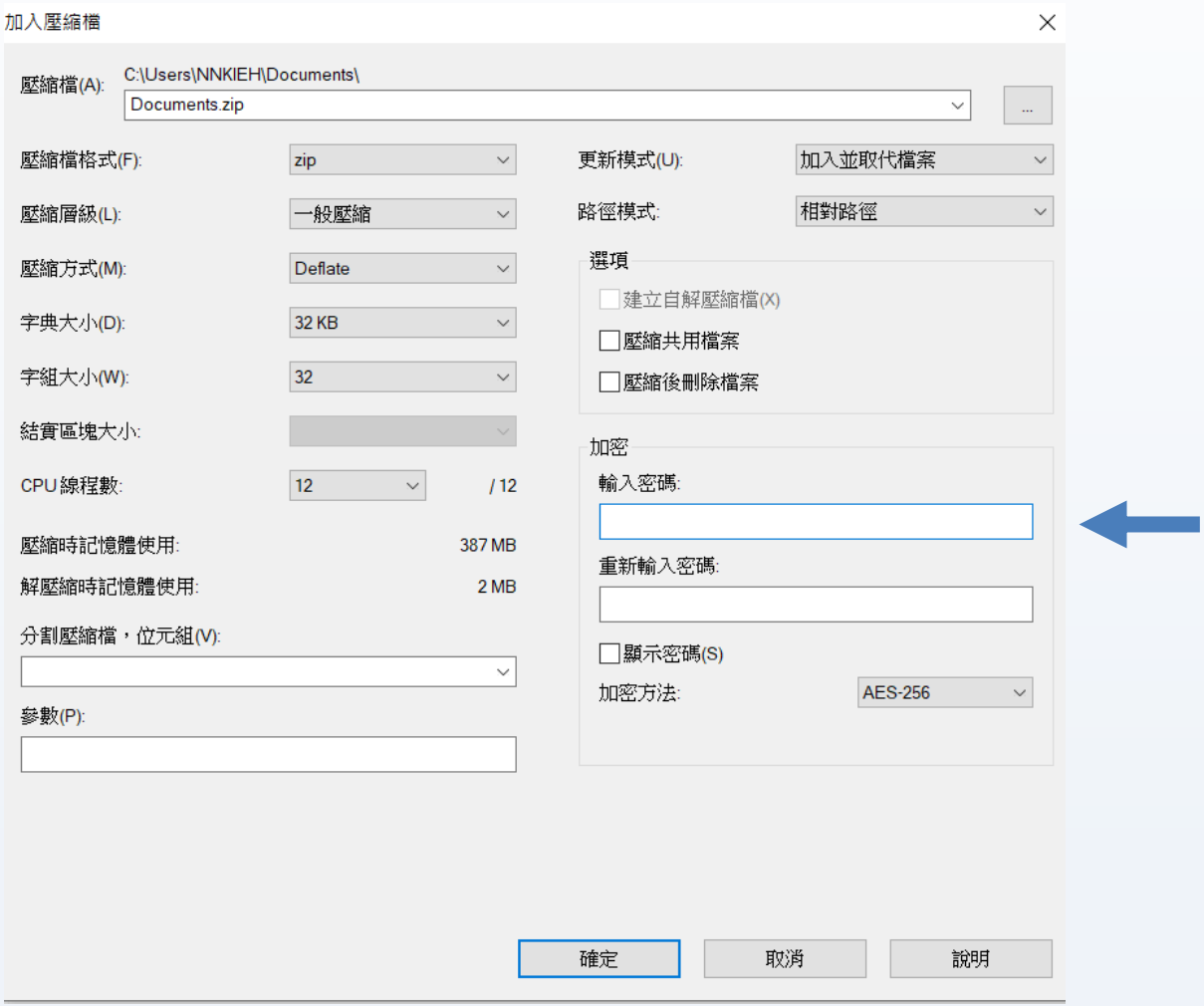
Home
7z Format
LZMA SDK
Download
FAQ
Support
Links

English
Chinese Simpl.
Chinese Trad.
Esperanto

其他：使用7z壓縮文件並設密碼



其他：使用7z壓縮文件並設密碼

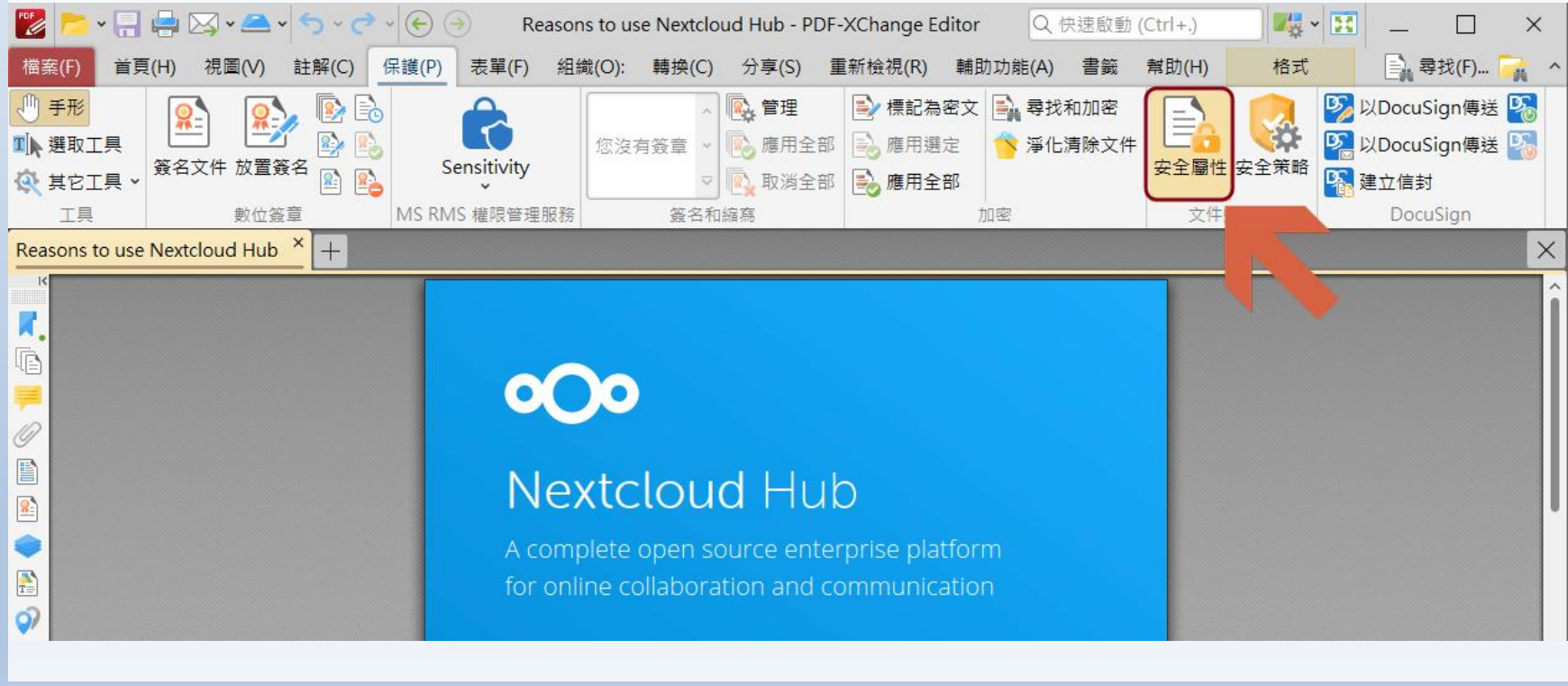


其他：其他實務操作技巧

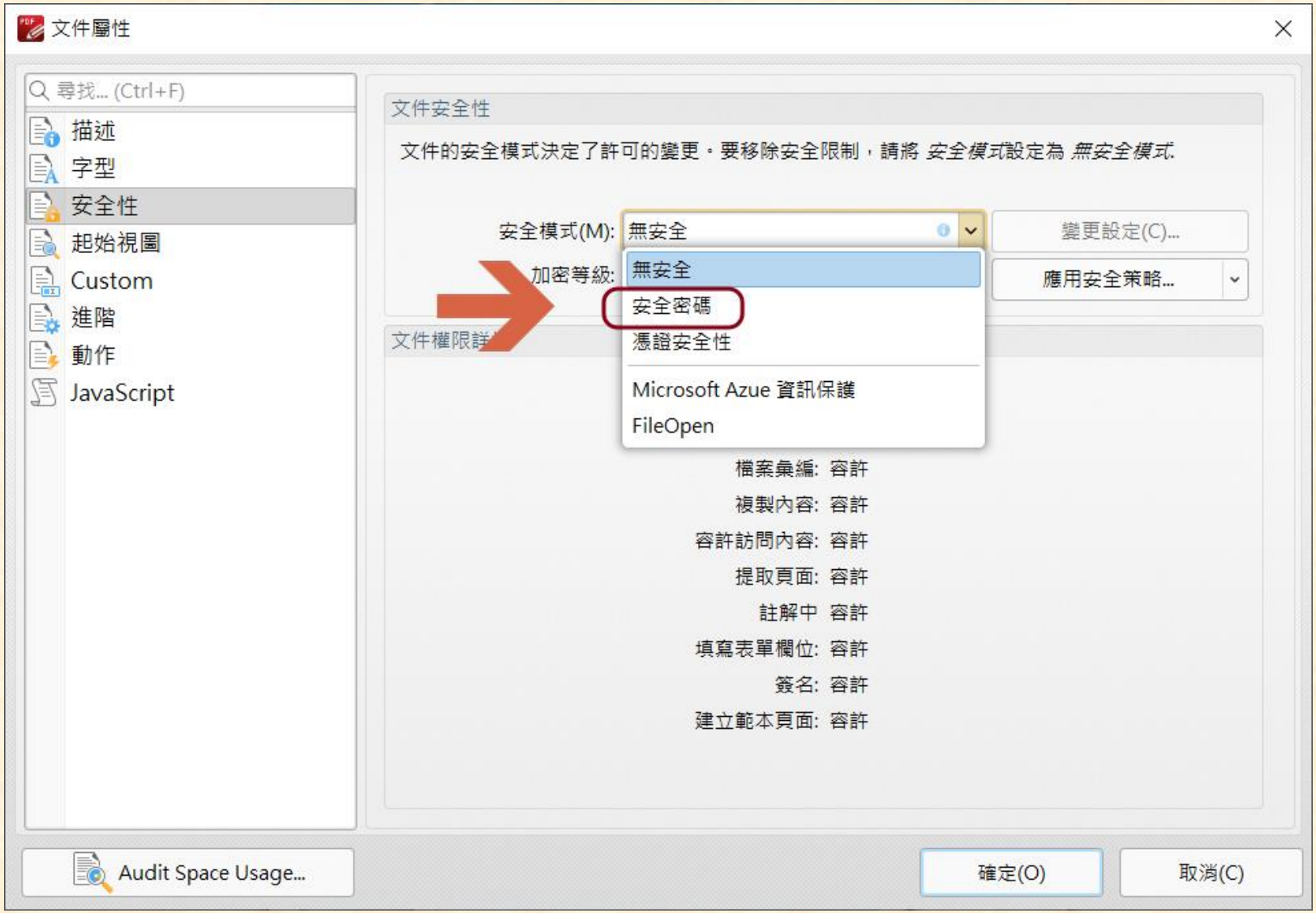
- 快速縮圖
  - 免費軟體：FastStone Image
  - 工具/批次轉換
- 學校公告: 可到「進階設定」裡填入「結束日期」
- 學校公告與榮譽榜：每年暑假安排一個時間把兩年以上的公告刪除
- 學校公告要注意把個資去識別化
  https://hs.nnkieh.tn.edu.tw/modules/tad_book3/page.php?tbsn=13&tbdsn=121
- 用 Word 開啟 PDF：使用檔案總管，對 PDF 檔案/右鍵/開啟檔案/以 word 開啟
- 學校公告用的文件，如果「沒有編輯資料需求」，請使用 PDF 文件格式來進行公告。
- 如果有編輯需求，只能使用開放文件格式(ODF)，如ODT, ODC等
- **Google Android手機其實會「偷聽我們的語音對話」**
  https://www.techbang.com/posts/118265-how-to-turn-off-google-voyeurism

PDF文件加密碼保護

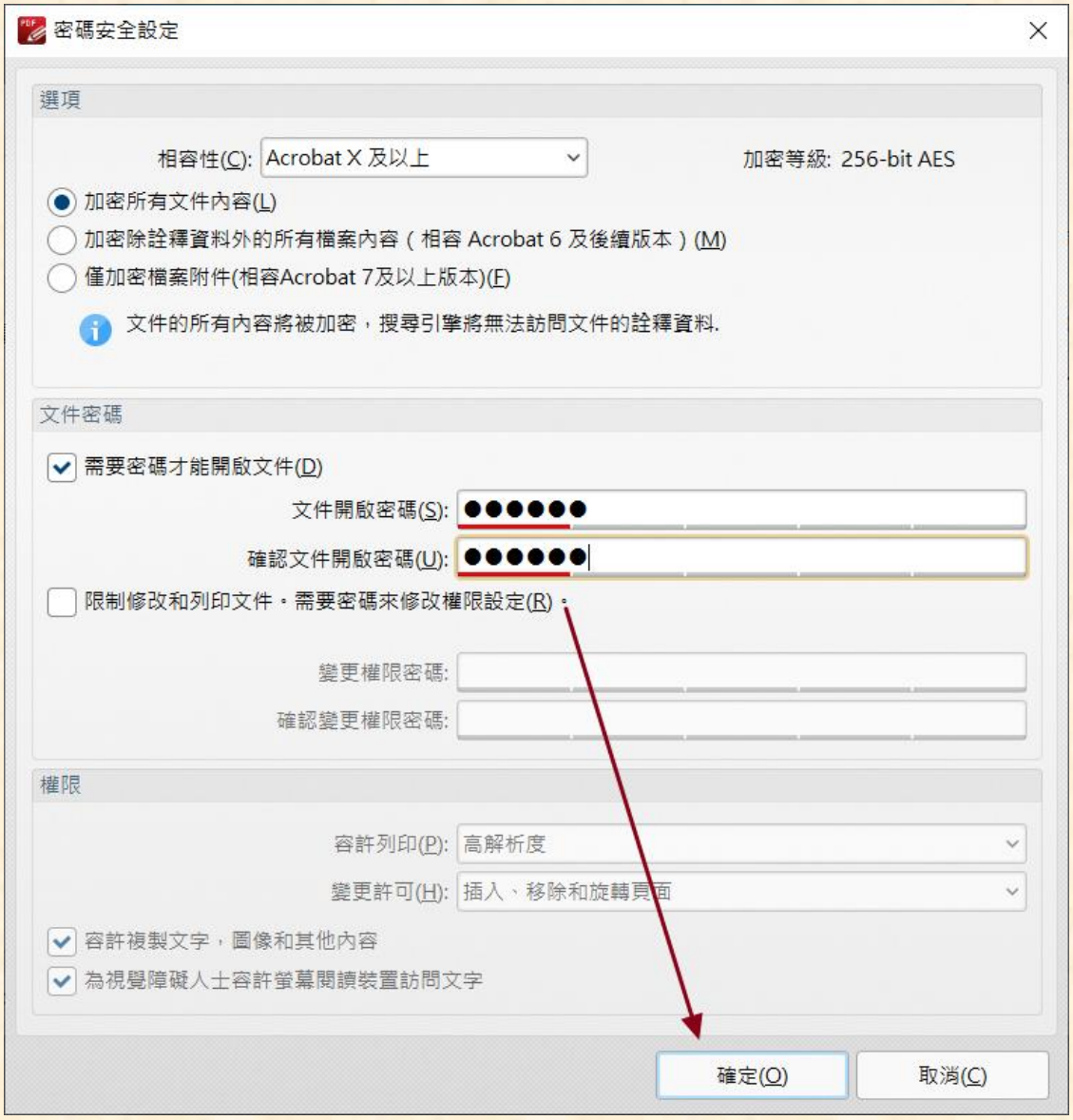
- 可用工具： PDF-Xchange Editor
  70%功能免費; 可先免費下載安裝使用; 如果有需要再付費升級
  https://www.pdf-xchange.com/product/pdf-xchange-editor
  安裝時請注意，**要勾選「Free」**選項
- 開啟需設密碼的PDF文件後：安全屬性



PDF文件加密碼保護

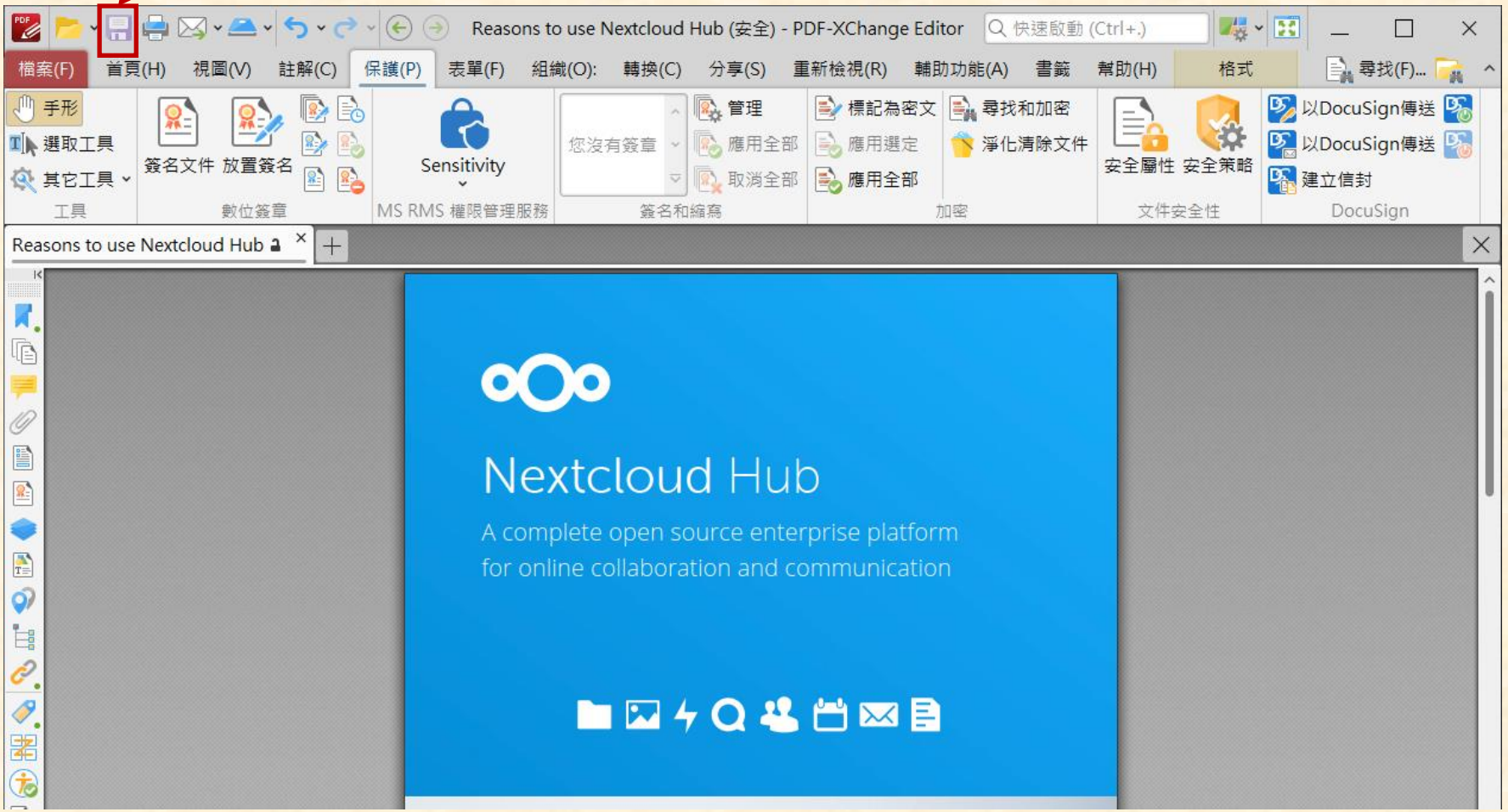

文件屬性
尋找... (Ctrl+F)
描述
字型
安全性
起始視圖
Custom
進階
動作
JavaScript
文件安全性
文件的安全模式決定了許可的變更。要移除安全限制，請將 安全模式設定為 無安全模式.
安全模式(M): 無安全
變更設定(C)...
加密等級: 無安全
安全密碼
憑證安全性
Microsoft Azue 資訊保護
FileOpen
應用安全策略...
文件權限詳
檔案彙編: 容許
複製內容: 容許
容許訪問內容: 容許
提取頁面: 容許
註解中 容許
填寫表單欄位: 容許
簽名: 容許
建立範本頁面: 容許
Audit Space Usage...
確定(O)
取消(C)

PDF文件加密碼保護

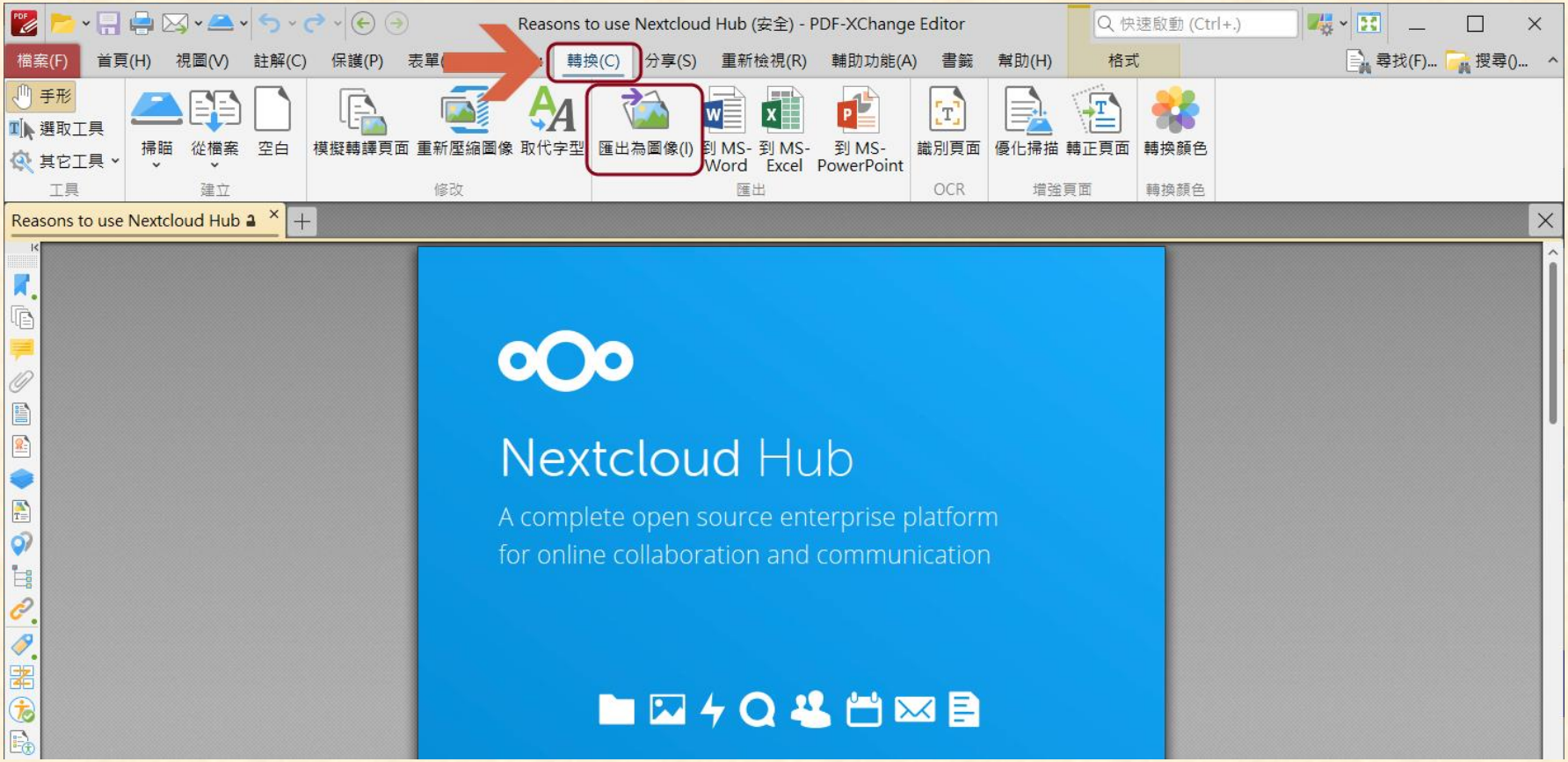

密碼安全設定
選項
相容性(C): Acrobat X 及以上
加密等級: 256-bit AES
加密所有文件內容(L)
加密除詮釋資料外的所有檔案內容（相容 Acrobat 6 及後續版本）(M)
僅加密檔案附件(相容Acrobat 7及以上版本)(F)
文件的所有內容將被加密，搜尋引擎將無法訪問文件的詮釋資料.
文件密碼
需要密碼才能開啟文件(D)
文件開啟密碼(S):
確認文件開啟密碼(U):
限制修改和列印文件，需要密碼來修改權限設定(R)：
變更權限密碼:
確認變更權限密碼:
權限
容許列印(P): 高解析度
變更許可(H): 插入、移除和旋轉頁面
容許複製文字，圖像和其他內容
為視覺障礙人士容許螢幕閱讀裝置訪問文字
確定(O)
取消(C)

PDF文件加密碼保護

設好密碼記得要「儲存」

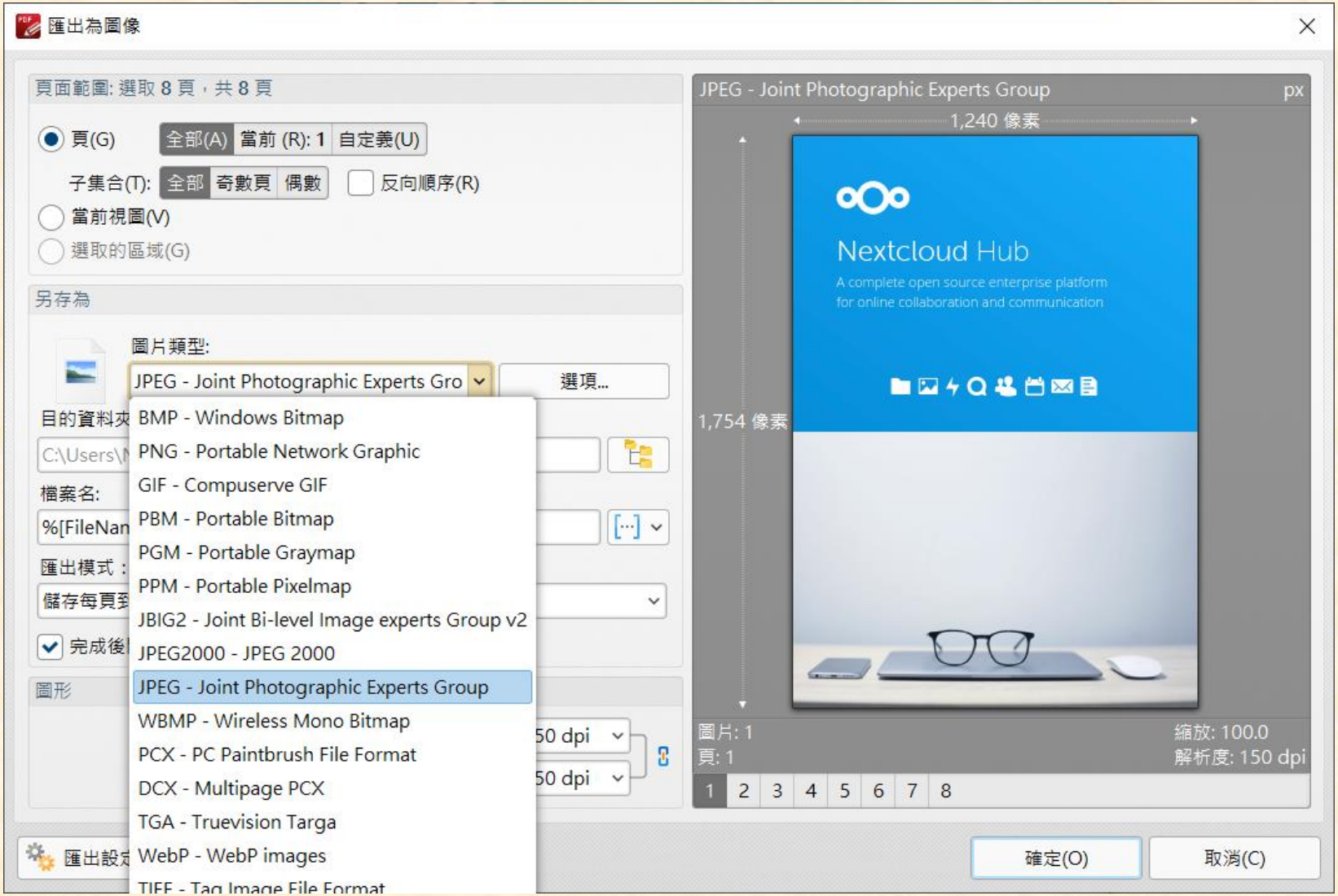


PDF-Xchange匯出成圖片（免費）



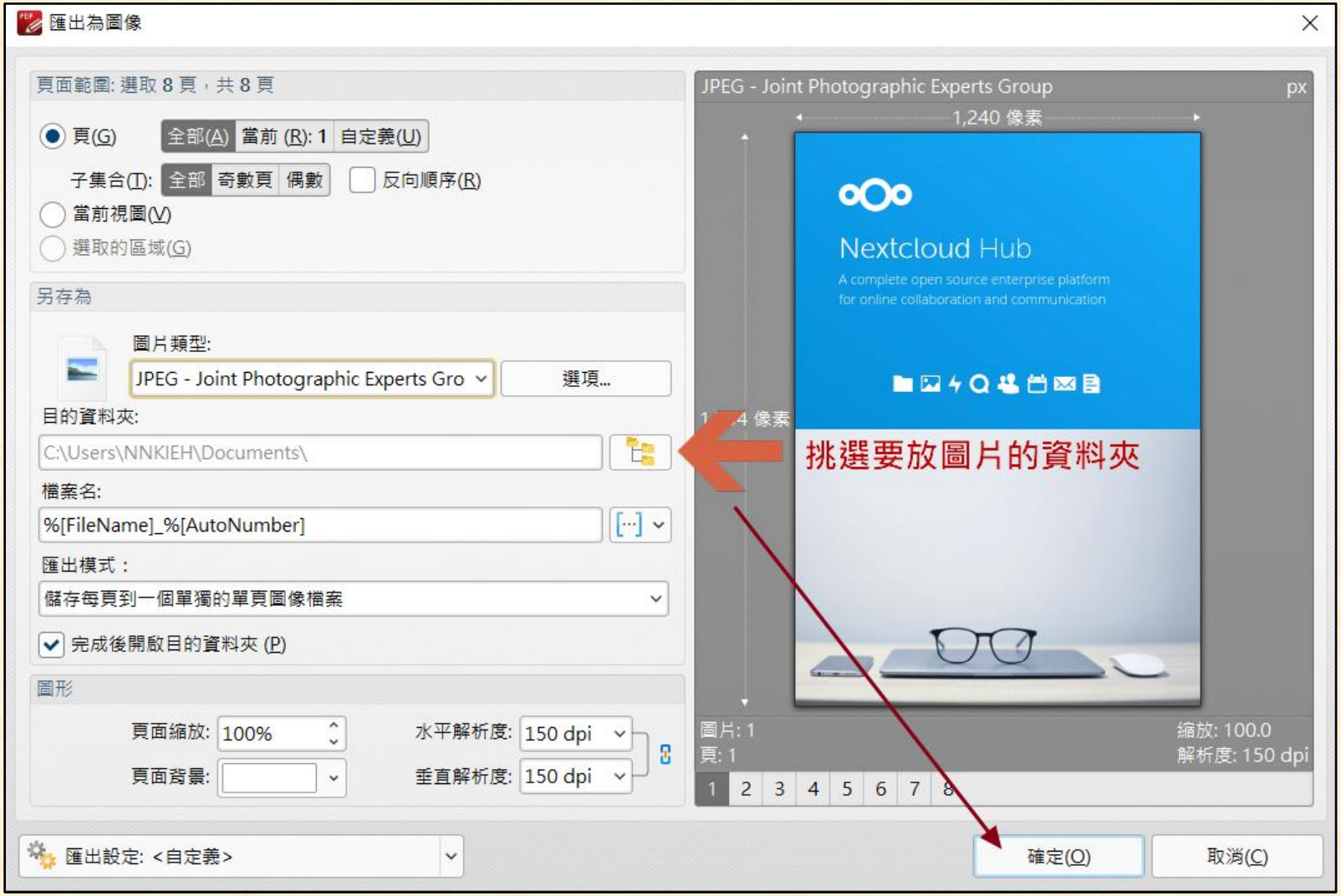
PDF-Xchange滙出成圖片（免費）

選取所需圖檔格式



PDF-Xchange滙出成圖片（免費）

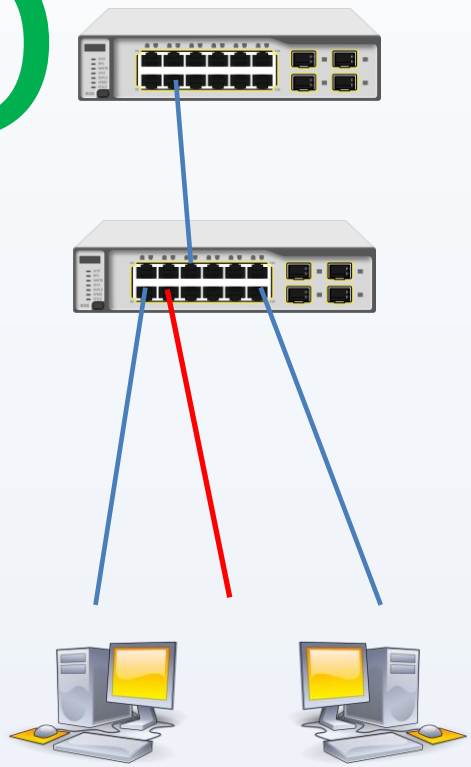
選取存放圖片的資料夾位置



網路線不可以回插

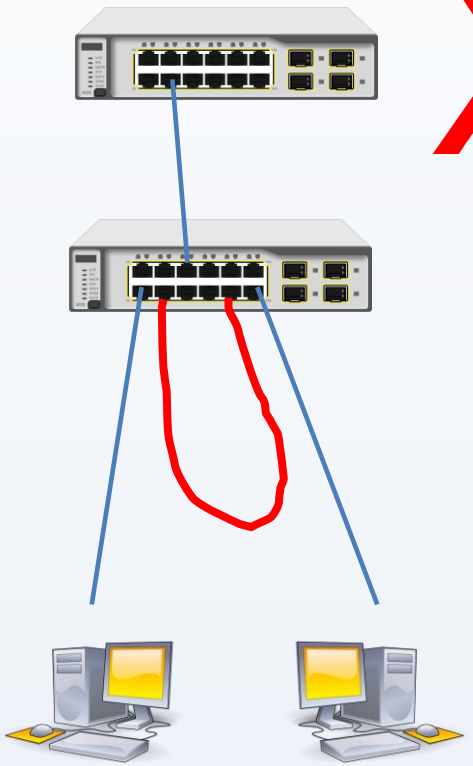
正常：樹狀網路

O



多餘的線不可回插

X



好用工具介紹

- 是真免費還是免費的永遠最貴: 破解 or 自由
- 免費防毒工具推薦
  - Windows 10 內建的 defender 好用嗎?
    https://www.av-test.org/en/antivirus/business-windows-client/windows-10/december-2021/
    https://www.av-comparatives.org/test-results/
- 學校雲端磁碟Google Drive (學校郵件帳號)
  - 優點：無限量；不占硬碟空間；手機平板也看得到
  - 缺點：要網路；美國政府因特定目的可瀏覽
- 真正刪除資料 – eraser
  - https://www.foolegg.com/how-to-completely-delete-files-or-folder-with-eraser/

IOT上的資安

- IOT是什麼：我們與電腦的距離．．．
  - 只要「可以用APP遠端控制的」都有危險
  - 自動車: 你在開還是駭客在開?
    https://newtalk.tw/news/view/2022-01-13/695922
- 什麼？ 我家的監控系統被公開了
  http://www.insecam.org/en/bycountry/TW/?page=1
  Why??
- IOT產品資安認證
  https://www.taics.org.tw/Validation00.aspx
- Shodan 網路設備對外開埠查詢
  https://www.shodan.io/