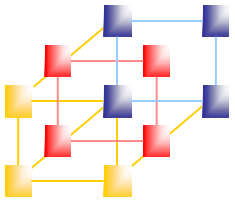
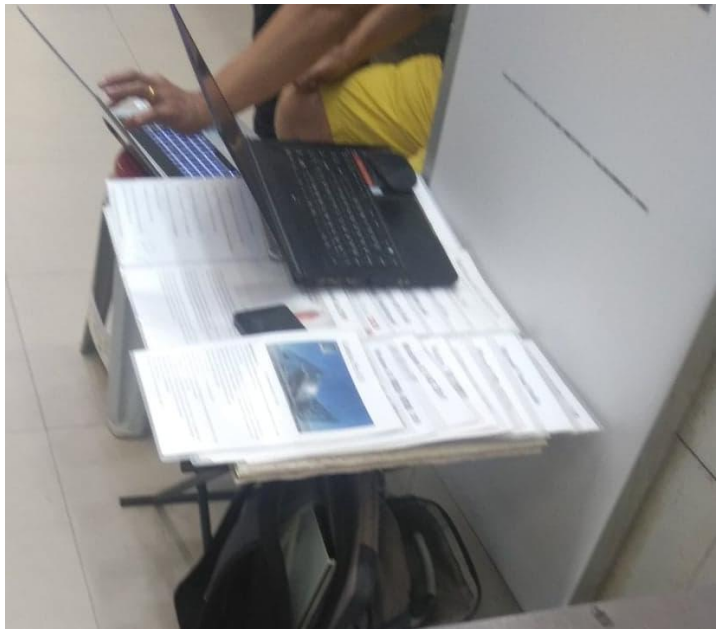


Unit 1
Network Security Concept

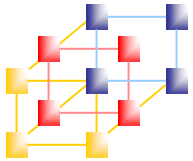
有關這份投影片會出現的東西

大補帖是什麼
好吃的泡麵、窮人的工具庫

- 多數都來自隔壁TJ老師
- 會加底線與**粗體**
- 會有很多補充資料
  - 會有額外標示
  - 會考嗎？
    - 只要上課有講的...
    - 別擔心，不會很難
- 投影片幾乎是英文
  - 英文很爛怎麼辦？我也很爛！
  - 給你釣竿，Google英文很好



大補帖的垂暮
剩2攤
居然還在賣Office2010



Quiz 1

- 簡單敘述印象裡的資訊安全？

Taiwan No. 1

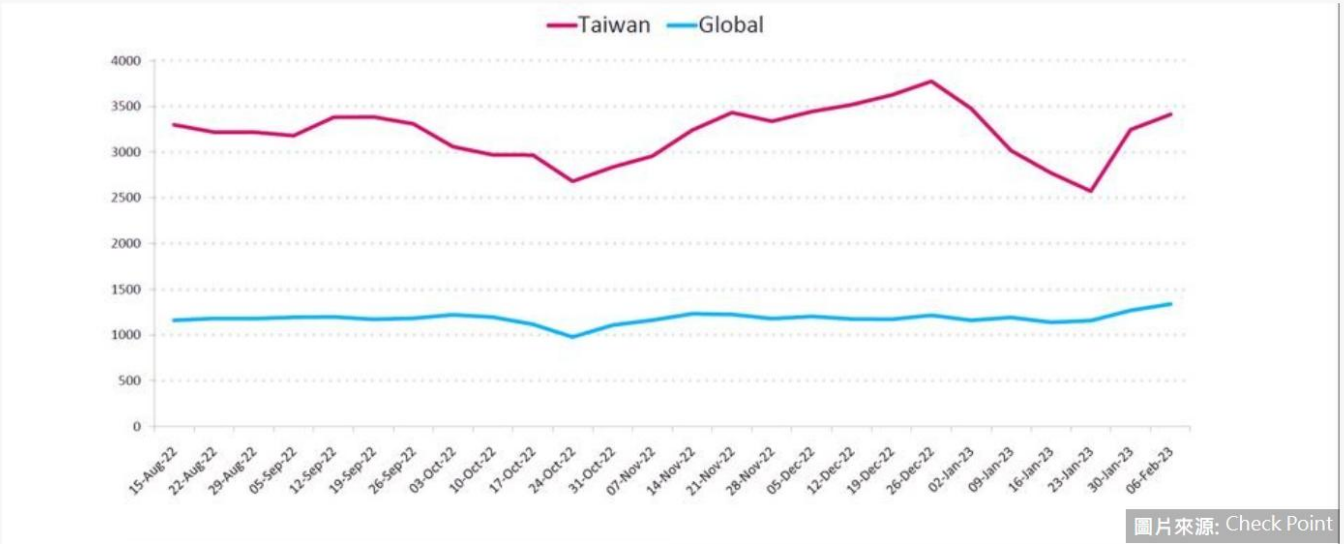
新聞

臺灣面臨網攻次數是全球平均的兩倍！2022年臺灣每週每個組織面臨3千次攻擊

2022全球網路攻擊次數比起2021年增長38%，醫療照護名列全球三大攻擊目標產業，竊密軟體躍居惡意軟體之首

文/ 李宗翰 | 2023-03-22 發表

讚 51 分享



圖片來源: Check Point

https://www.ithome.com.tw/news/156040

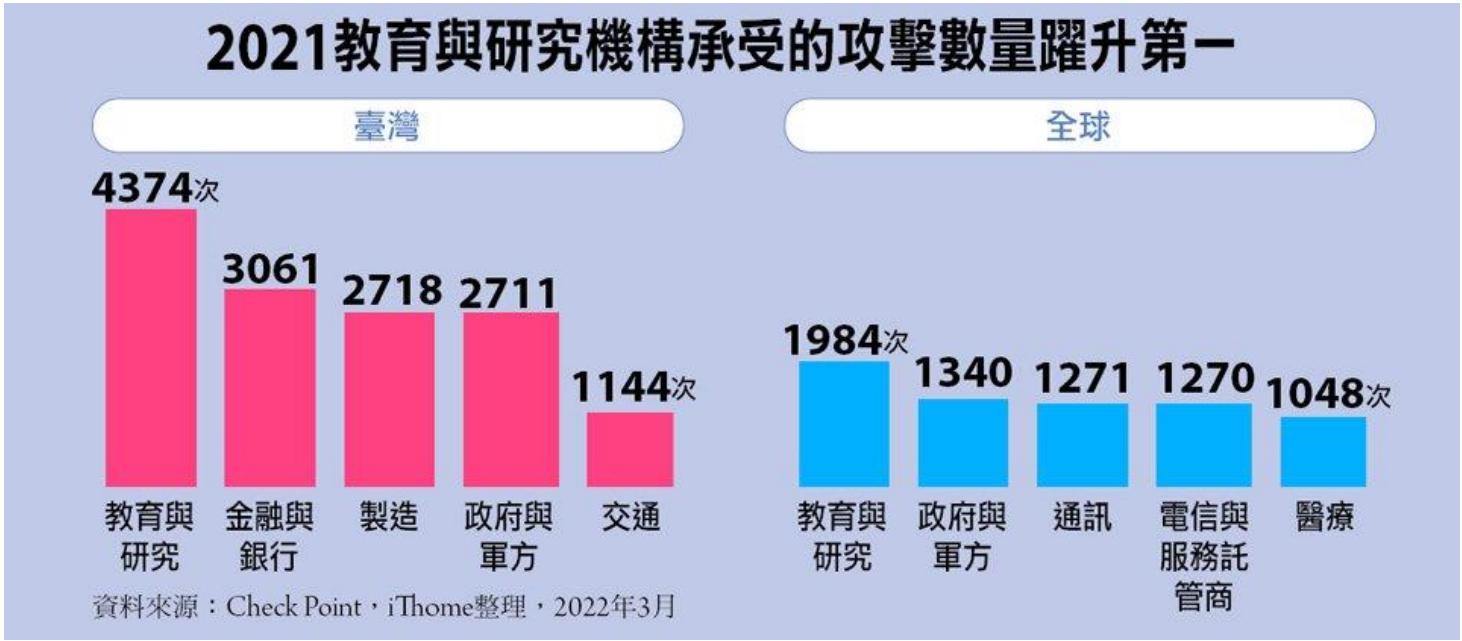
資安事件知多少

Source: https://technews.tw/2020/05/23/3-keys-figures-expose-taiwan-cybersecurity-crisis/

資安事件知多少

2021年學校與研究單位成攻擊最頻繁目標，臺灣每週遭攻擊次數是全球平均3倍

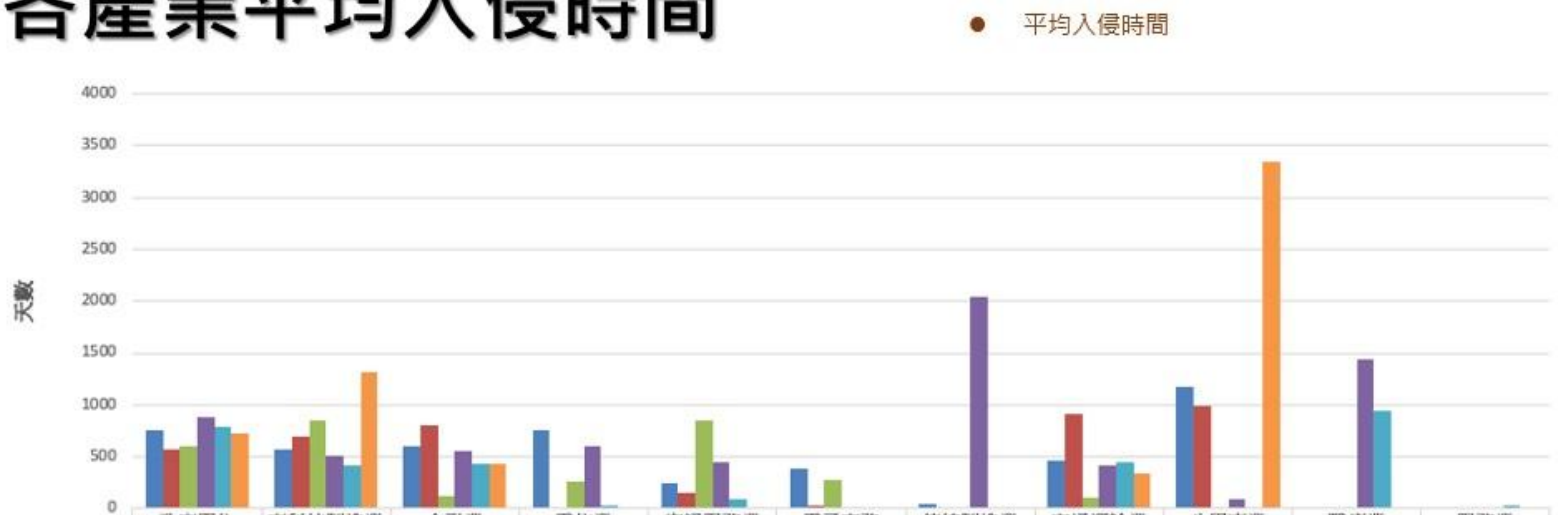
2021年企業與組織遭受攻擊趨勢大公開，資安業者Check Point指出全球產業中，全球教育與研究機構遭受攻擊數量最多，臺灣亦有同樣的狀況，另要注意鎖定全球軟體供應商的攻擊趨勢，在全球增幅達146%居冠



Source: https://www.ithome.com.tw/news/149919

網路攻擊潛伏期

各產業平均入侵時間



	政府單位	高科技製造業	金融業	電信業	資訊服務業	電子商務	傳統製造業	交通運輸業	公用事業	醫療業	服務業
2012~2014	759	567	603	761	242	386	52	458	1171		
2015	567	695	809		157	27		910	986		
2016	607	848	126	266	844	280		111			
2017	886	517	561	599	448		2048	418	98	1445	
2018	791	417	434	29	100			445.7		940	34
2019	735	1310	441					343	3339	2	5

- 入侵時間是統計駭客從入侵開始至事件調查發現的平均時間間隔

整個攻擊趨勢，也從早期以破壞為主，至現在多以勒索為目標，部分產業駭客攻擊的「潛伏期」達三、四年甚至十多年。此外他說，因地緣、政治之故，背後有國家單位資助的國家級駭客，其攻擊數量亦不斷增加。除政府、金融、高科技產業外，傳統產業、醫療、中小企業，如今都成駭客可能下手的目標。

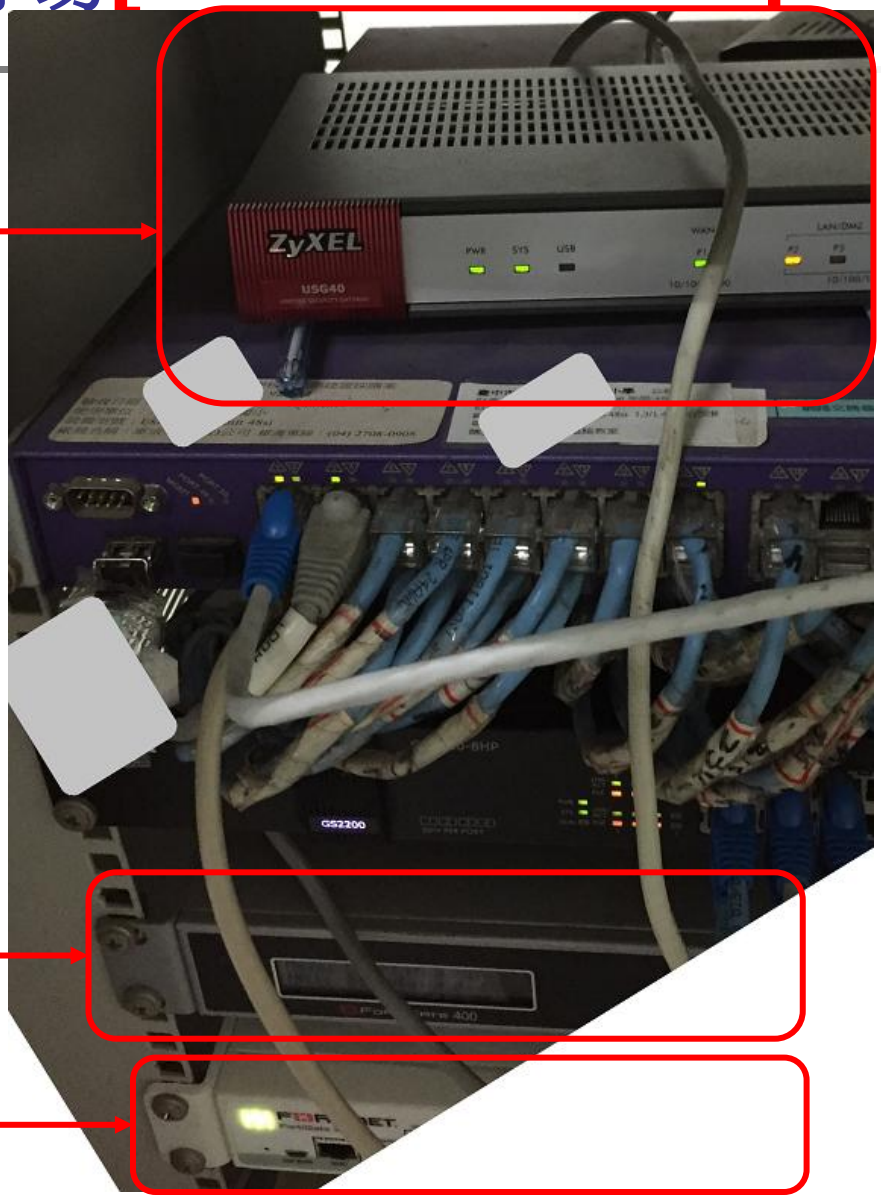
課程的開場[TOP SECRET]

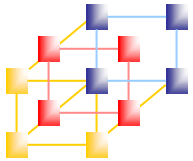
一台ZyWall下面墊原子筆散熱

還有一台Fortinet沒拍到...

一台Fortinet沒接電

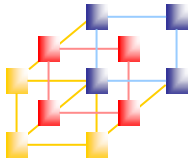
一台Fortinet有接電沒接線





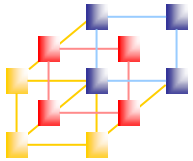
買設備是萬靈丹？！

- 防火牆
- 入侵偵測/防禦系統
- 應用程式防火牆
- 零信任
- EDR/MDR
- …
  - 我們來看看現實的案例…



我家的萬里長城？！

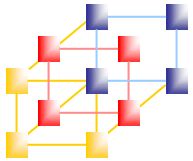
應該長醬→



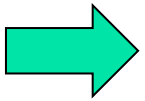
我家的萬里長城？！

沒多久…

變醬→



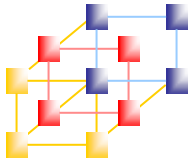
好，花錢築牆！！



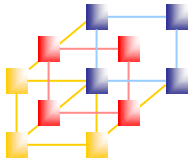
現實中的駭客攻擊？！

又過不了多久

變醬→



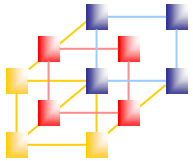
最後只好醬：



後來變成醬：

社會科學的小小結論

- 社會科學的特色就是沒辦法重來
- 生命會自己找到出路 -- Jurassic Park
- 水桶理論是真的
- 尋找弱點的能力是與生俱來的！
- 您還相信萬里長城有效嗎？



一個TANet的中獎案例

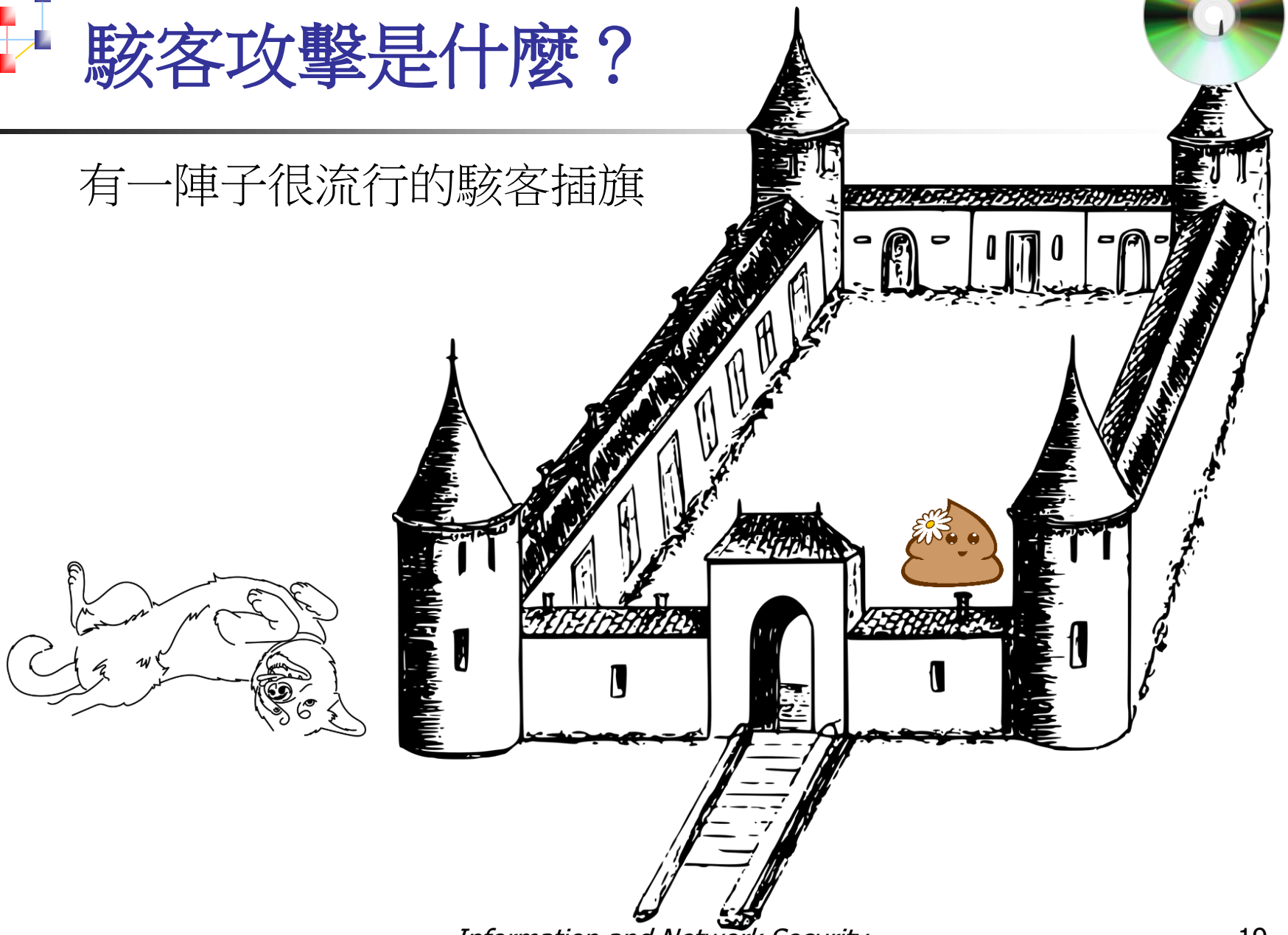
- 見樹不見林是什麼狀況？！
- [TOP SECRET]

發生了什麼事？

大部分的攻擊都是迂迴繞過預防機制所產生的結果

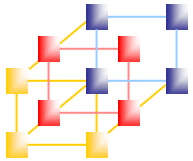
駭客攻擊是什麼？

有一陣子很流行的駭客插旗



駭客攻擊是什麼？

(Netflix沒有了 QQ)



什麼是安全？

- 感覺安全 與 真正安全
  - 防毒軟體 很吵 v.s. 很安靜
  - 資安事件通報單 一天好幾張 v.s. 很久不見
  - 大家提心吊膽 v.s. 高枕無憂
  - 花錢買大牌子 v.s. 有就好

單位的資訊化，誰比較安全？

or

資料來源: http://pic.bbs.hexun.com/2011-12-05/135992143_1.html / Wikipedia

真的比較安全？

資料來源: http://pic.bbs.hexun.com/2011-12-05/135992143_1.html

發生什麼問題？

Source: https://www.reddit.com

發生什麼問題？

2.5萬筆學習歷程檔案遺失 81校7千人受災

2021-09-26 01:06 聯合報 / 記者趙宥寧、江良誠／連線報導

(udn.com)

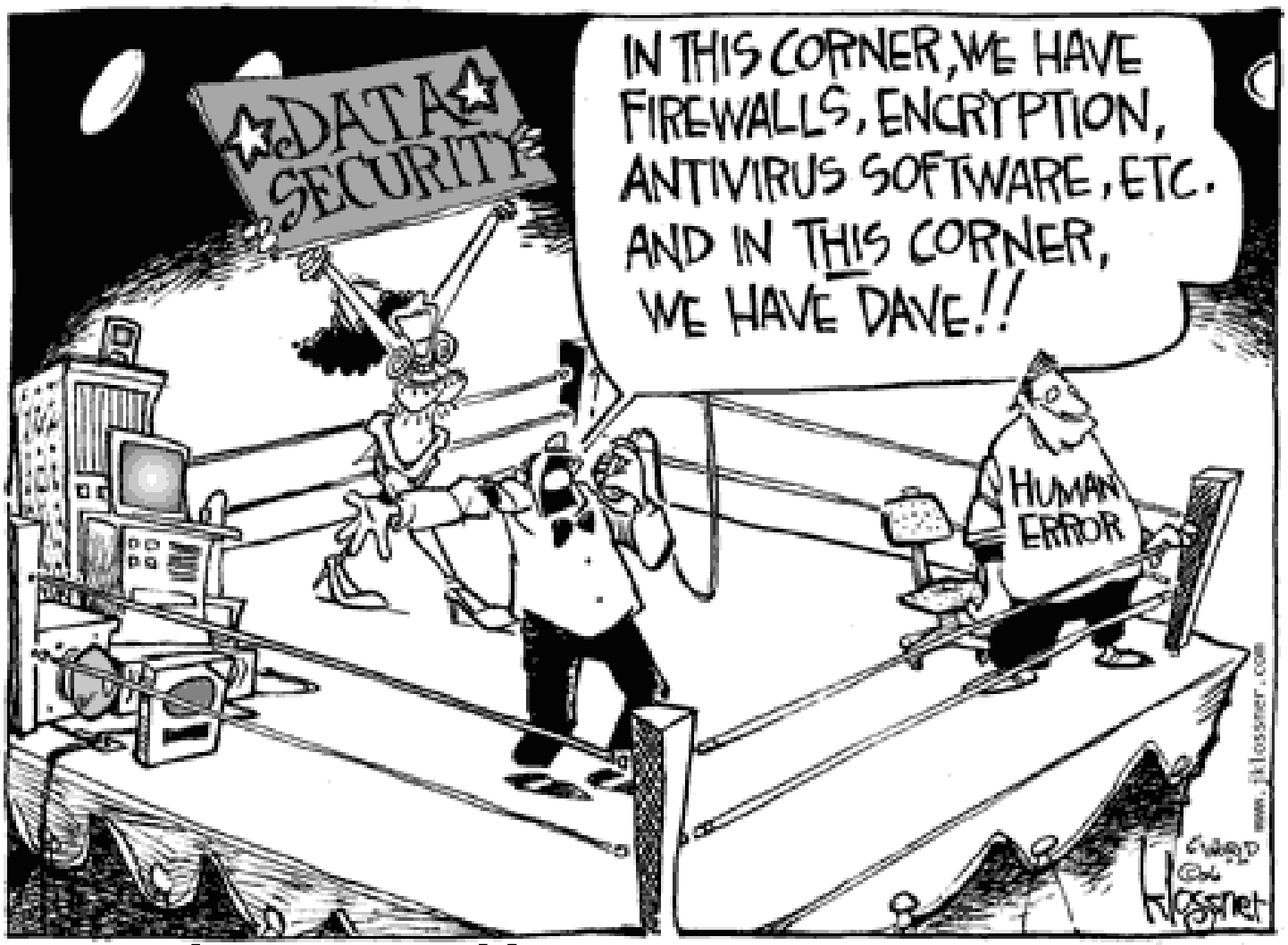
發生什麼問題？

南韓境內只要是採用KT電信公司網路服務的用戶，全都受影響。（示意圖 / shutterstock達志影像）

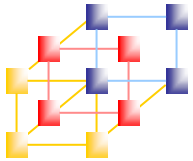
事故發生後，KT電信公司表示，網路服務因受到大規模DDoS攻擊中斷，已立即召開危機管理委員會因應，將盡快恢復正常服務。但根據官方最新公告指出，事發之初由於流量超過負荷，因此將斷網原因推測為受到DDoS攻擊，但經過內部嚴謹調查後，發現實際上導致斷網的原因是「網路路徑設置錯誤」，將與政府進一步調查該起事件，並向用戶致上歉意。

(Source:TVBS)

發生什麼問題？



Source: http://www.jklossner.com/



為何資安事件似乎越來越多？

Past

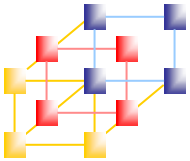
- 家醜不外揚
- 被黑了很丟臉

→ 低調找資安公司處理處理就好

Now

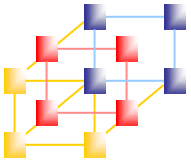
- 資安即國安
- 資安防護一起來
- 大公司都被黑過

→ 證交所重大訊息處理程序修訂，上市公司發生重大資安事件應揭露於重訊



Outline

- OSI security architecture
- Security attacks
- Security services
- Security mechanisms
- Network security model

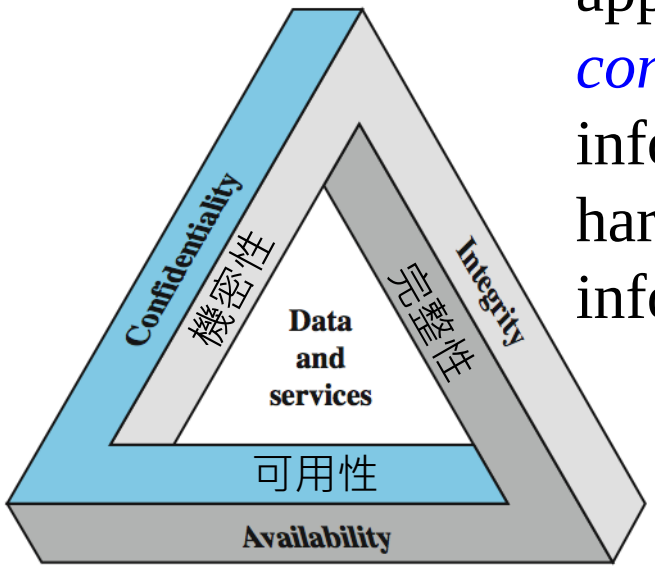


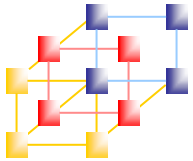
Definition (1/2)

- Computer/system security
  - Generic name for the collection of tools designed to protect data and to thwart hackers 系統安全
- Network security
  - Protect data during their transmission
- Internet security 傳輸安全
  - Protect data during their transmission over a collection of interconnected networks

Definition (2/2)

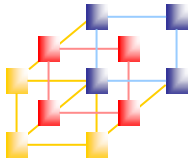
- A definition of computer security – The NIST Computer Security Handbook
  - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the *confidentiality*, *integrity* and *availability* of information system resources (includes hardware, software, firmware, information/data, and telecommunications).





NIST

- NIST: National Institute of Standards and Technology (*what is?*)
- SP 800 (*what is?*)
  - SP 800-53



C.I.A.

- Confidentiality（機密性）
  - Cover both data confidentiality and privacy
    - Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

資訊安全 v.s. 隱私保護-一樣嗎?

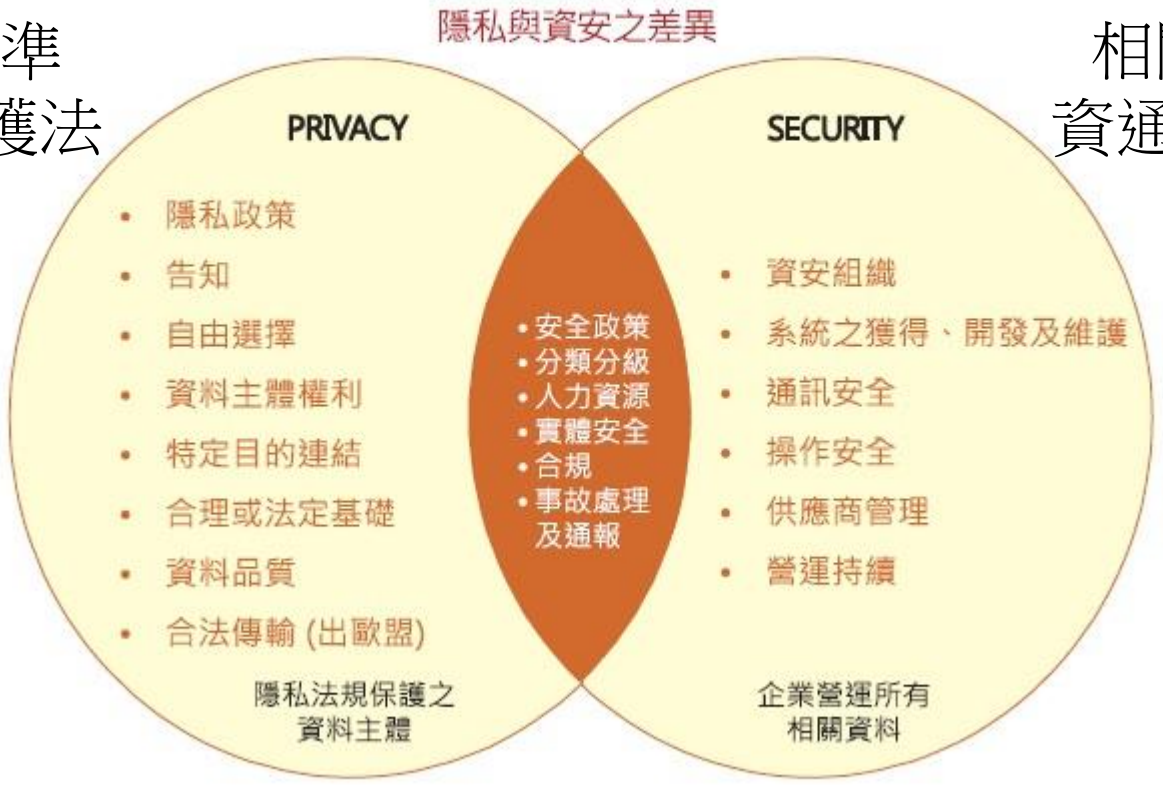
- Integrity（完整性）
  - Covers both data and system integrity
    - Guard against improper information modification or destruction, and includes ensuring information non-repudiation(不可否認) and authenticity（真實性）
- Availability（可用性）
  - Ensure timely and reliable access to and use of information

資訊安全 v.s. 隱私保護

大補帖

隱私不等於資安

相關規範/標準
個人資料保護法
GDPR
PIMS
ISO27701
BS10012
…



圖片來源／PwC Taiwan 資誠

相關規範/標準
資通安全管理法
ISMS
ISO27001
…

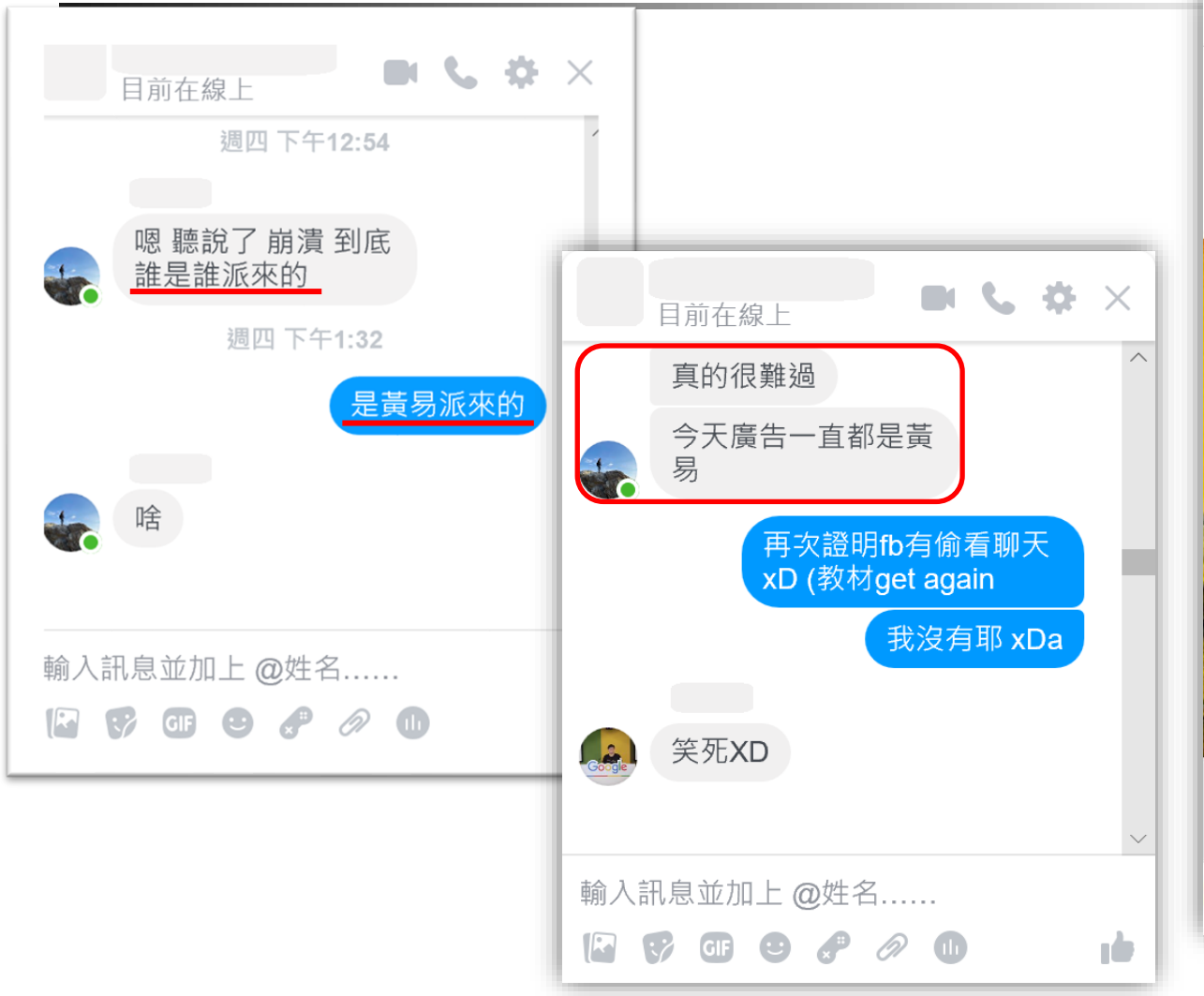
線上聊天有祕密嗎？

- FB
- Line
- Dcard
- IG
- What’s APP

FB - 犀牛盾的故事


搜尋
ASimon Chang
首頁
建立
ASimon Chang
動態消息
Messenger
Watch
Marketplace
捷徑
探索
社團
粉絲專頁
Oculus
活動
遊戲
查看更多.....
284
本週有9個新讚數
最新貼文
"【Code Injection—XM
3月29日下午12:01
15
加強推廣貼文
建立推廣活動
犀牛盾 RhinoShield
贊助
我們與超多具風格特色的品牌及設計師合作，
手機殼將不只是保護手機的套件，
而是展現自我風格的配件，
粉絲們千萬別錯過，快來尋寶、支持你喜歡的設計師吧！
DESIGNERS
RHINOSHIELD
設計師聯名專區
RHINOSHIELD.TW
犀牛盾 X 聯名設計師
你可以在這裡找到Hello...
來去逛逛
330
38則留言 11次分享
讚
回應
分享
Marketplace 熱門精選
NT$20
NT$528
NT$1,500
NT$418
可超貸
到 Marketplace 搜尋更多商品
仍在 Marketplace 販售
NT$75,000
NT$69,999
你的粉絲專頁
三甲科技 AAA Secu...
聯絡人
製造業
博弈製造業
不是啦 XD
他們主要是做手機週邊
最有名的應該是 犀牛盾手機殼
喔喔
輸入訊息.....
搜尋

FB - 你誰派來瘩？


目前在線上
週四 下午12:54
嗯 聽說了 崩潰 到底 誰是誰派來的
週四 下午1:32
是黃易派來的
啥
輸入訊息並加上 @姓名.....
目前在線上
真的很難過
今天廣告一直都是黃易
再次證明fb有偷看聊天 xD (教材get again
我沒有耶 xDa
笑死XD
輸入訊息並加上 @姓名.....


說黃易群俠傳 M 讚。
黃易群俠傳 M
贊助 ·
穿越古今未來
2020奇幻武俠史詩大作
現在、立刻、馬上就去…… 繼續閱讀
你是誰派來的?
黃易群俠傳M
武俠 MMORPG 手遊
雙平台•預下載開放
GET IT ON Google Play
Pre-order on the App Store
HEM.GAMEFLIER.COM
我黃易派來的！
雙平台預約即刻開約，好禮等……
搶先預約
69
5則留言 1次分享

真實的釣魚案例

- 某次買完eBay後的優閒早晨
- 看到一封神奇信件

Chunghwa Post | 中華郵政	Last Reminder: Your package could not be delivered on 18.12.2020
昨天	
Chunghwa Post	Fwd: Tr: RE: Last Reminder: Your package could not be delivered on
今天	
Chunghwa Post	Chunghwa Post informs you that your shipment N° TW00275029 is

真實的釣魚案例

2020/12/18 (週五) 上午 09:11

Chunghwa Post | 中華郵政 <stampmall@mail.post.gov.tw>

Last Reminder: Your package could not be delivered on 18.12.2020

收件者 asimon@asimon.idv.tw

這封郵件以高重要性傳送。

中華郵政全球資訊網
Chunghwa Post Co., Ltd.

Hello asimon@asimon.idv.tw

Last Reminder: This Email informs you that your shipment is still pending.

Your package could not be delivered on **18.12.2020** because no customs duty was paid (**369** 新台幣 **NT Dollars**)

Merchant 商人 **: Chunghwa Post**
Order Number 訂單編號 **: 00275029**
Purchase Amount 訂單金額 **: 369** 新台幣 **NT Dollars**
Delivery scheduled between 預定的交貨時間 **: 19.12.2020 - 22.12.2020**

- To confirm the shipment of your package Click here .

You will receive an email or SMS when you arrive in your home address. You will have 8 days, from the date of availability,

- For more services, find the follow-up of your shipment by **Clicking here** .

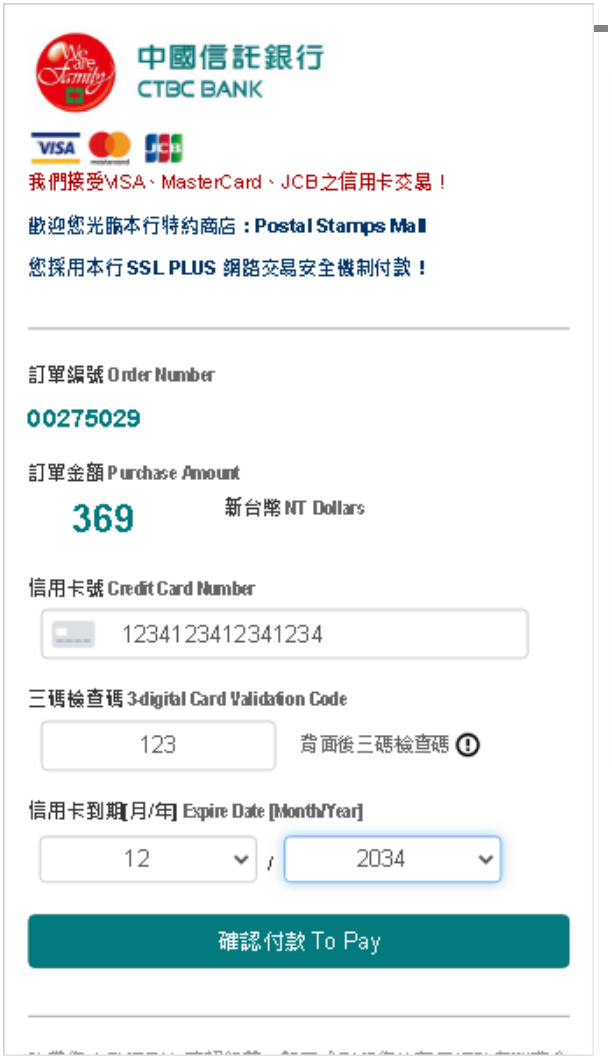
Thank you for your trust,

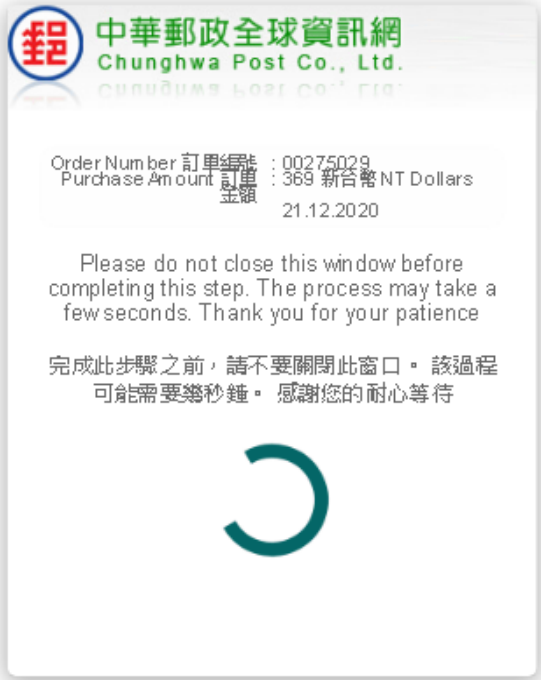
Sincerely,
Your **Chunghwa Post** customer service.

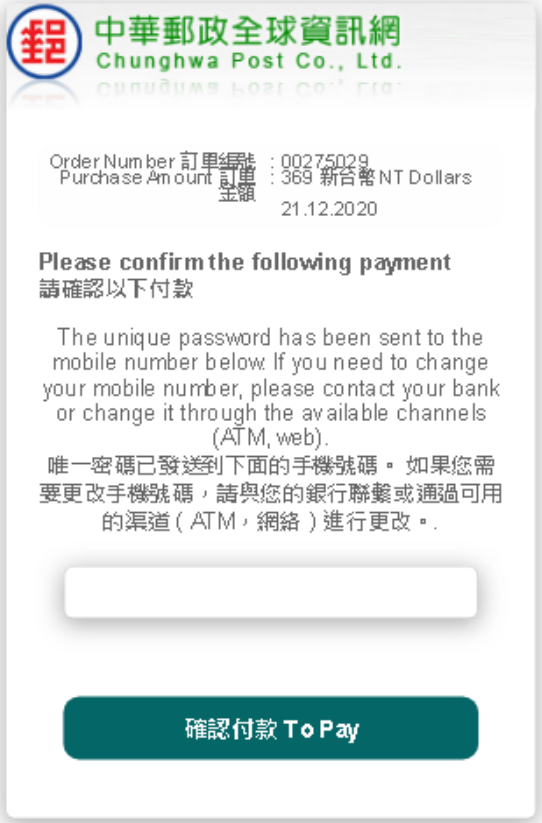
Compensation
Chunghwa Post Co., Ltd. (hereinafter the "Company") is committed in respecting all users' personal privacy,
being in accord with the Personal Information Protection Act of Republic of China and Company's personal information protection policy.
The Company hereby declaring the following statements in regards with the collection, processing,

真實的釣魚案例


大補帖


中國信託銀行
CTBC BANK
我們接受VISA、MasterCard、JCB之信用卡交易！
歡迎您光臨本行特約商店：Postal Stamps Mall
您採用本行SSL PLUS 網路交易安全機制付款！
訂單編號 Order Number
00275029
訂單金額 Purchase Amount
369
新台幣 NT Dollars
信用卡號 Credit Card Number
1234123412341234
三碼檢查碼 3-digital Card Validation Code
123
背面後三碼檢查碼
信用卡到期[月/年] Expire Date [Month/Year]
12
2034
確認付款 To Pay


中華郵政全球資訊網
Chunghwa Post Co., Ltd.
Order Number 訂單編號 : 00275029
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars
21.12.2020
Please do not close this window before completing this step. The process may take a few seconds. Thank you for your patience
完成此步驟之前，請不要關閉此窗口。該過程可能需要幾秒鐘。感謝您的耐心等待


中華郵政全球資訊網
Chunghwa Post Co., Ltd.
Order Number 訂單編號 : 00275029
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars
21.12.2020
Please confirm the following payment
請確認以下付款
The unique password has been sent to the mobile number below. If you need to change your mobile number, please contact your bank or change it through the available channels (ATM, web).
唯一密碼已發送到下面的手機號碼。如果您需要更改手機號碼，請與您的銀行聯繫或通過可用的渠道（ATM，網絡）進行更改。
確認付款 To Pay

真實的釣魚案例

大補帖


中華郵政全球資訊網
Chunghwa Post Co., Ltd.
Order Number 訂單編號 : 00275029
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars
21.12.2020
Please confirm the following payment
請確認以下付款
The unique password has been sent to the mobile number below. If you need to change your mobile number, please contact your bank or change it through the available channels (ATM, web).
唯一密碼已發送到下面的手機號碼。如果您需要更改手機號碼，請與您的銀行聯繫或通過可用的渠道（ATM，網絡）進行更改。
12345
確認付款 To Pay
中華郵政全球資訊網
Chunghwa Post Co., Ltd.
Order Number 訂單編號 : 00275029
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars
21.12.2020
Please do not close this window before completing this step. The process may take a few seconds. Thank you for your patience
完成此步驟之前，請不要關閉此窗口。該過程可能需要幾秒鐘。感謝您的耐心等待
中華郵政全球資訊網
Chunghwa Post Co., Ltd.
Order Number 訂單編號 : 00275029
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars
21.12.2020
Please confirm the following payment
請確認以下付款
The unique password has been sent to the mobile number below. If you need to change your mobile number, please contact your bank or change it through the available channels (ATM, web).
唯一密碼已發送到下面的手機號碼。如果您需要更改手機號碼，請與您的銀行聯繫或通過可用的渠道（ATM，網絡）進行更改。
SMS is wrong or expired! After (3) errors when entering the code received via SMS, the current transaction is canceled and the credit card is blocked.
短信錯誤或已過期！輸入通過SMS接收到的代碼後出現（3）錯誤後，當前交易被取消，信用卡被凍結。
確認付款 To Pay

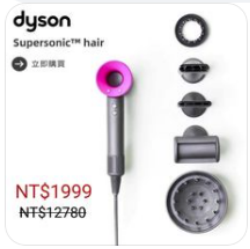
真實的釣魚案例


新光三越 台北信義店
贊助
大家好，我是新光三越百貨dyson專賣店的櫃姐。
由於403花蓮大地震我們臺北信義店各大奢侈品牌店玻璃被震碎，導致我們無法正常開業。現修業整頓，由於庫存積壓，為此，我們將低價出售店內庫存Dyson吹風機，以回饋粉絲們歷年的支持
原價NT$12780，現僅售NT$1999！限時限量大促，數量有限趕快行動！！
dyson
Supersonic™ hair
立即購買
NT$1999
NT$12780
KSAZZ.FUN
三年保修，一年內無理由包退換！
瞭解詳情
887
286則留言 339次分享

真實的釣魚案例

新光三越 台北信義店的貼文

作者
新光三越 台北信義店
大家好，我是新光三越百貨dyson專賣店的櫃姐。
由於403花蓮大地震💥我們臺北信義店各大奢侈品牌店玻璃被震碎，導致我們無法正常開業。現修業整頓，由於庫存積壓，為此，我們將低價出售店內庫存Dyson吹風機，以回饋粉絲們歷年的支持🙏
🛒：https://ksaxr.fun/m0soqeqh2o00
🤩原價NT$12780，現僅售NT$1999！💝限時限量大促，數量有限趕快行動！



6小時 讚 回覆 27

陳清華
戴森的吹風機是第一次購買真的不錯，質感做工都很棒

5小時 讚 回覆 12

新光三越 台北信義店已回覆 · 1則回覆 5小時

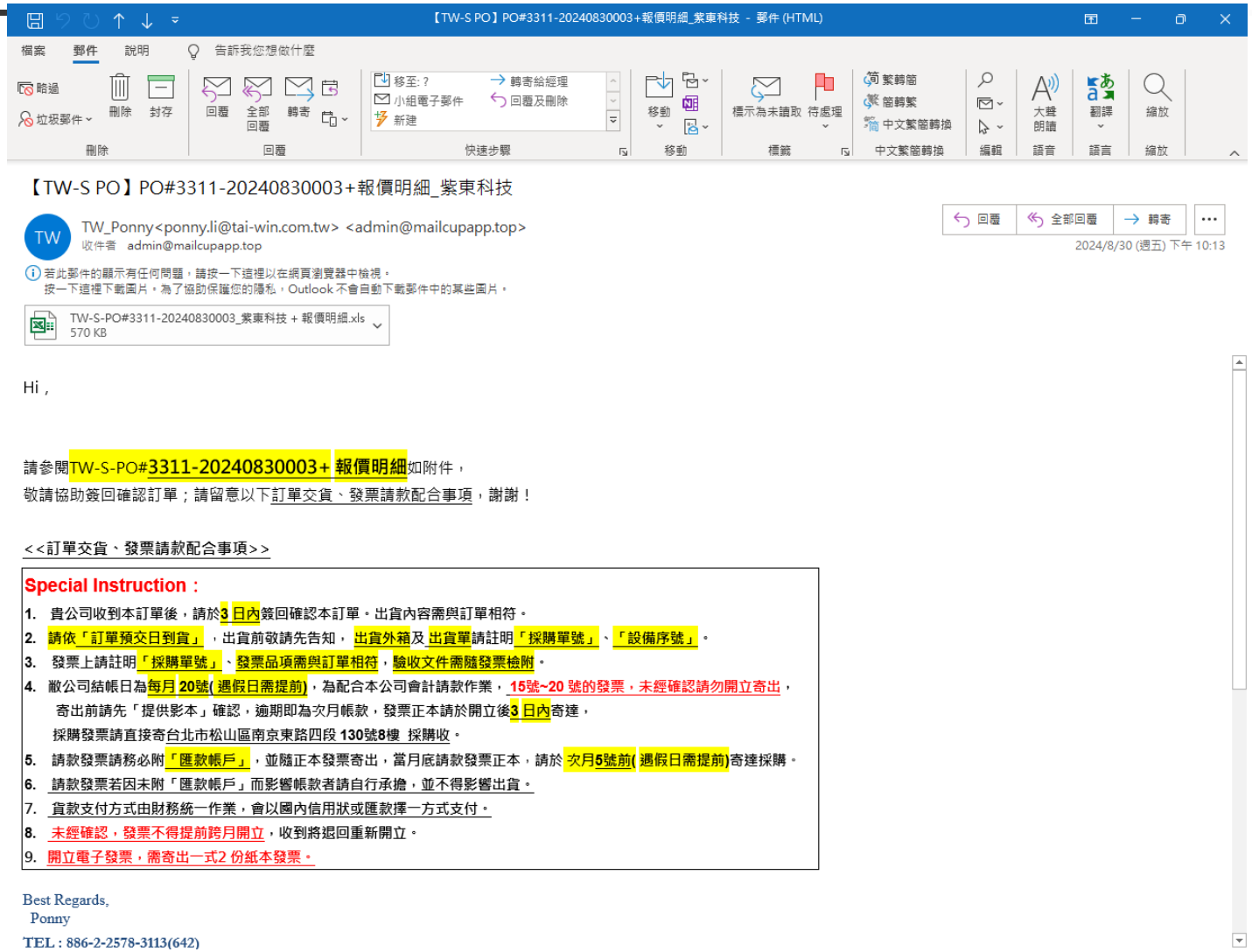
方鈊儒
是正品，做工不錯，風嘴很多，電機聲音做的很小，這個很厲害，風力比傳統吹風機來的猛

以 ASimon Chang 的身分留言

真實的釣魚案例


台北 遠東sogo百貨
贊助
大家好，我是遠東SOGO百貨的櫃姐。
由於403花蓮大地震，我們遠東SOGO敦化店各大奢侈品牌店玻璃被震碎，導致我們無法正常開業。
現修業整頓，由於庫存積壓，為此，我們將各大品牌香水3折出售，以回饋粉絲們歷年的支持!
原價NT$4194，現僅售NT$1290！更有【買一送一，買二送二】限時大促，趕快行動！
立即選購我們最暢銷的香水系列，最高可享3折優惠！
SOGO
Sale
遠東
SOGO
3折起
NT$4194
NT$498
VUUEY.SHOP
品牌授權店，品質保證
附帶發票
瞭解詳情
2,372
1,047則留言 913次分享

真實的釣魚案例



【TW-S PO】PO#3311-20240830003+報價明細_紫東科技 - 郵件 (HTML)

檔案 郵件 說明 告訴我您想做什麼

【TW-S PO】PO#3311-20240830003+報價明細_紫東科技

TW_Ponny<ponny.li@tai-win.com.tw> <admin@mailcupapp.top>
收件者 admin@mailcupapp.top

回覆 全部回覆 轉寄

2024/8/30 (週五) 下午 10:13

若此郵件的顯示有任何問題，請按一下這裡以在網頁瀏覽器中檢視。
按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

TW-S-PO#3311-20240830003_紫東科技 + 報價明細.xls
570 KB

Hi ,

請參閱TW-S-PO#3311-20240830003+ 報價明細如附件，
敬請協助簽回確認訂單；請留意以下訂單交貨、發票請款配合事項，謝謝！

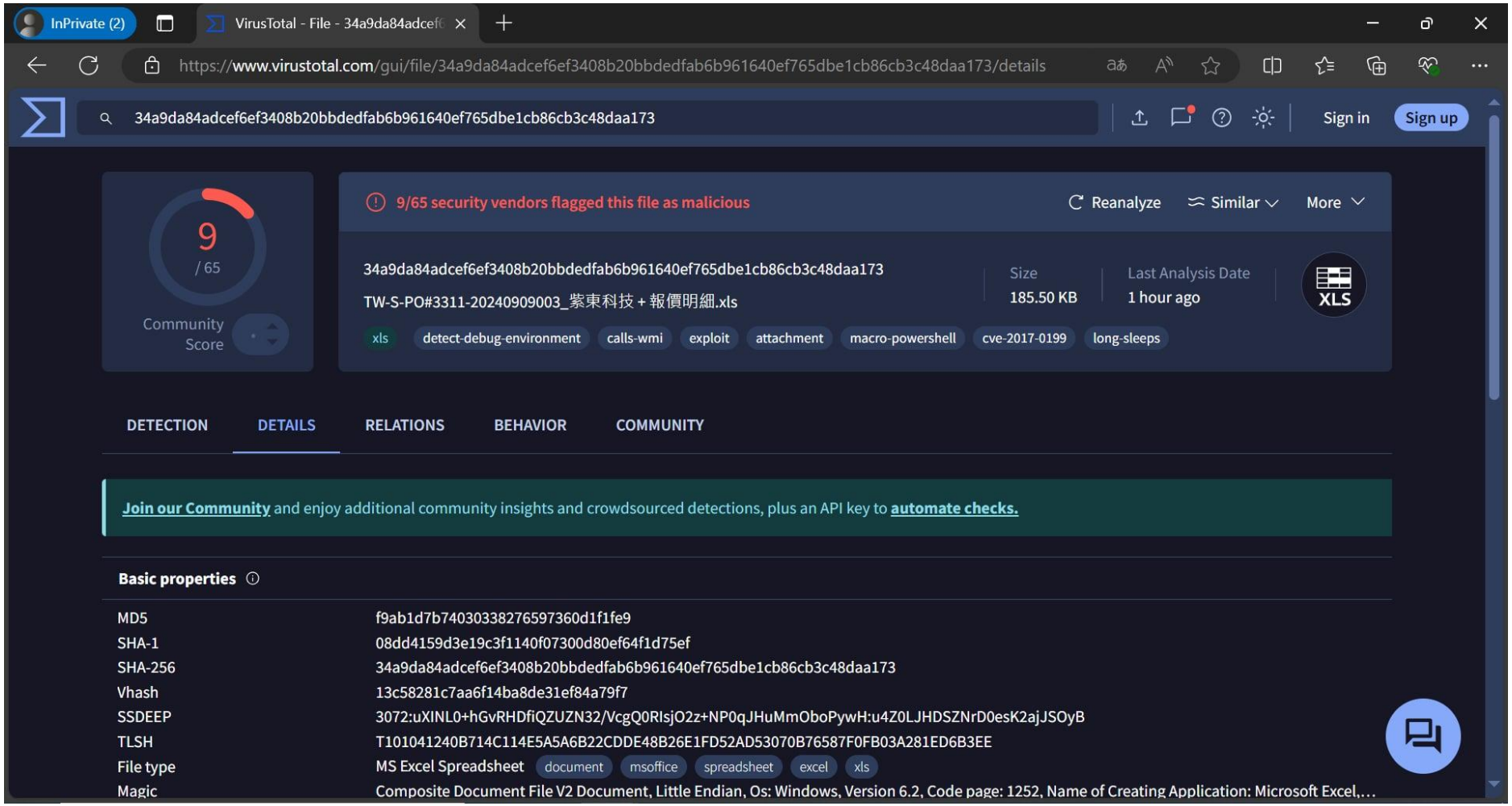
<<訂單交貨、發票請款配合事項>>

Special Instruction :

1. 貴公司收到本訂單後，請於3 日內簽回確認本訂單。出貨內容需與訂單相符。
2. 請依「訂單預交日到貨」，出貨前敬請先告知， 出貨外箱及 出貨單請註明「採購單號」、「設備序號」。
3. 發票上請註明「採購單號」、發票品項需與訂單相符，驗收文件需隨發票檢附。
4. 敝公司結帳日為每月 20號(遇假日需提前)，為配合本公司會計請款作業，15號~20 號的發票，未經確認請勿開立寄出，
   寄出前請先「提供影本」確認，逾期即為次月帳款，發票正本請於開立後3 日內寄達，
   採購發票請直接寄台北市松山區南京東路四段 130號8樓 採購收。
5. 請款發票請務必附「匯款帳戶」，並隨正本發票寄出，當月底請款發票正本，請於 次月5號前(遇假日需提前)寄達採購。
6. 請款發票若因未附「匯款帳戶」而影響帳款者請自行承擔，並不得影響出貨。
7. 貨款支付方式由財務統一作業，會以國內信用狀或匯款擇一方式支付。
8. 未經確認，發票不得提前跨月開立，收到將退回重新開立。
9. 開立電子發票，需寄出一式2 份紙本發票。

Best Regards,
Ponny
TEL : 886-2-2578-3113(642)

真實的釣魚案例

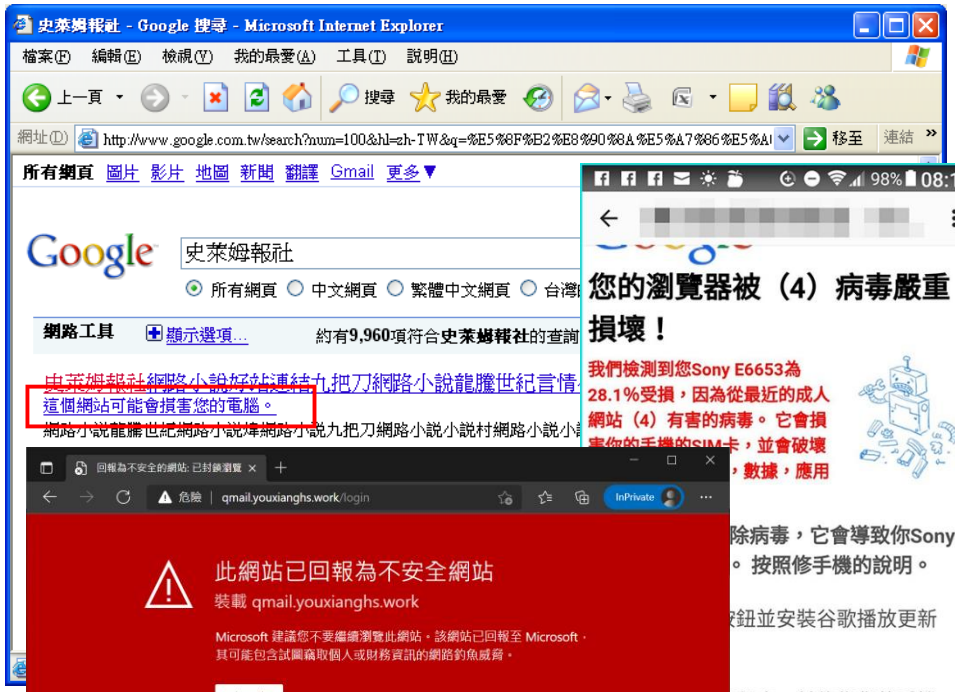

InPrivate (2)
VirusTotal - File - 34a9da84adcef6
https://www.virustotal.com/gui/file/34a9da84adcef6ef3408b20bbdedfab6b961640ef765dbe1cb86cb3c48daa173/details
34a9da84adcef6ef3408b20bbdedfab6b961640ef765dbe1cb86cb3c48daa173
Sign in
Sign up
9
/ 65
Community Score
9/65 security vendors flagged this file as malicious
Reanalyze
Similar
More
34a9da84adcef6ef3408b20bbdedfab6b961640ef765dbe1cb86cb3c48daa173
TW-S-PO#3311-20240909003_紫東科技 + 報價明細.xls
Size
185.50 KB
Last Analysis Date
1 hour ago
XLS
xls
detect-debug-environment
calls-wmi
exploit
attachment
macro-powershell
cve-2017-0199
long-sleeps
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Basic properties
MD5 f9ab1d7b74030338276597360d1f1fe9
SHA-1 08dd4159d3e19c3f1140f07300d80ef64f1d75ef
SHA-256 34a9da84adcef6ef3408b20bbdedfab6b961640ef765dbe1cb86cb3c48daa173
Vhash 13c58281c7aa6f14ba8de31ef84a79f7
SSDEEP 3072:uXINL0+hGvRHDfiQZUZN32/VcgQ0RIsjO2z+NP0qJHuMmOboPywH:u4Z0LJHDSZNrD0esK2ajJSOyB
TLSH T101041240B714C114E5A5A6B22CDDE48B26E1FD52AD53070B76587F0FB03A281ED6B3EE
File type MS Excel Spreadsheet document msoffice spreadsheet excel xls
Magic Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Name of Creating Application: Microsoft Excel,...

短訊驗證碼很安全嗎？

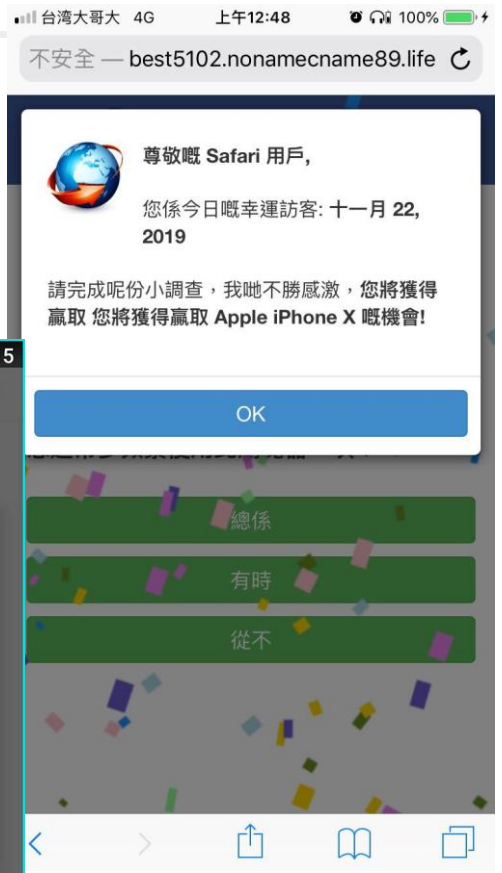
Source: 自由時報

瀏覽網站小心陷阱

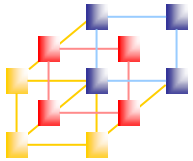
- Google警告標示 & 您中獎了



哪個才是真的?

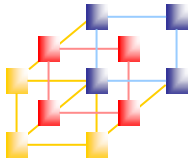


Source: https://www.mygopen.com 及 自行截圖



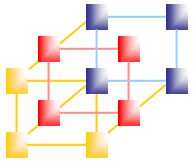
怎麼辦？

- 沒有獎徵答



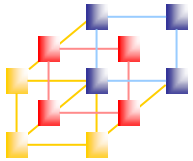
機密性、完整性、可用性

- 保護資訊的
  - 機密性(Confidentiality)
    - 2019/11 中山大學驚傳師生電子郵件被監控長達3年
    - 2021/04 有人在駭客論壇兜售逾8億LinkedIn用戶資料
  - 完整性(Integrity)
    - 2019/11 學生研究漏洞惹禍！臺大教學平臺成績全部變87分
    - 2021/04 竄改190筆資料A走142萬公款，公務員要關5年2月
  - 可用性(Availability)
    - 2021/05 中華電：台灣4月DDoS最大攻擊量較3月大增394%，金融保險業居冠
    - 2021/09 瘋搶五倍券早鳥加碼致當機銀行官網十點半起逐步恢復
    - 2021/10 開放搶BNT「平台準時當機」網轟爆：都第十輪了還卡



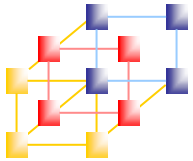
更多案例

- 讀報時間一篇一篇慢慢看



OSI security architecture

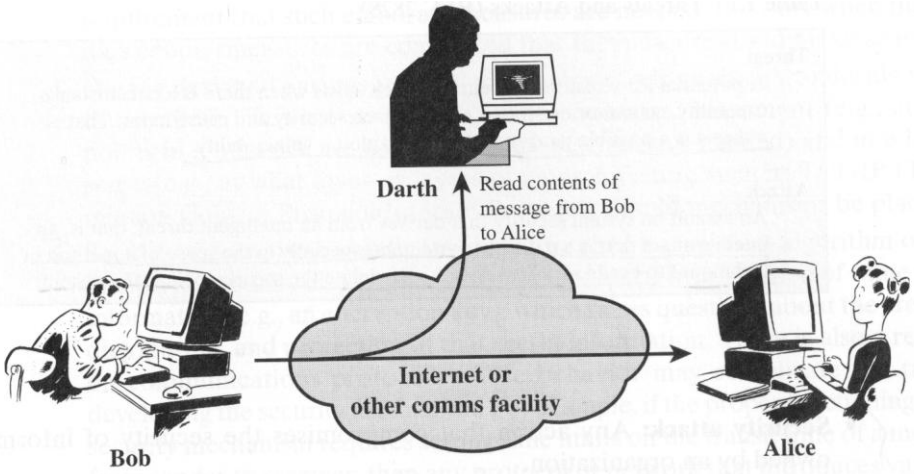
- ITU-T X.800 security architecture for OSI
  - ITU-T is a United Nations-sponsored agency that develops standard related to *telecommunications* and to *open systems interconnection* (OSI)
- The OSI security architecture focuses on
  - Security attacks (安全攻擊)
    - Any action that compromises the security of information owned by an organization (安全攻擊：任何洩漏組織所擁有的資訊安全的行動)
  - Security services (安全服務)
    - A service that enhances the security of the data processing systems and the information transfers of an organization (強化資料處理系統以及資訊傳輸的安全性)
  - Security mechanisms (安全機制)
    - A mechanism that is designed to detect, prevent, or recover from a security attack (用來偵測、防止或者復原安全攻擊的機制)



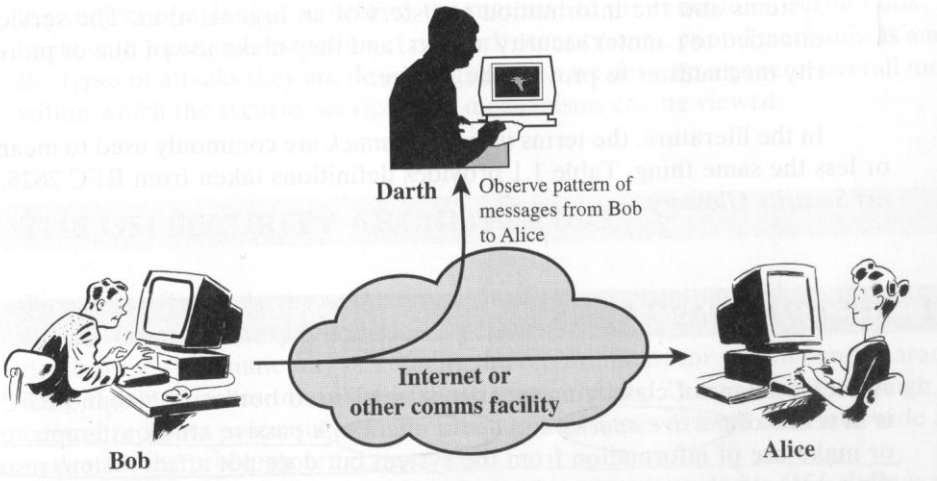
Security attacks

- Any action that compromises the security of information owned by an organization
- Classification (used X.800 and RFC 2828)
  - *Passive attacks*（被動式攻擊）- eavesdropping on, or monitoring of, transmissions to:
    - Release of message contents, or
    - Traffic analysis
  - *Active attacks*（主動式攻擊）– modification of data stream to:
    - Masquerade of one entity as some other
    - Replay previous messages
    - Modify messages in transit
    - Denial of service

Passive attacks



Release of message contents

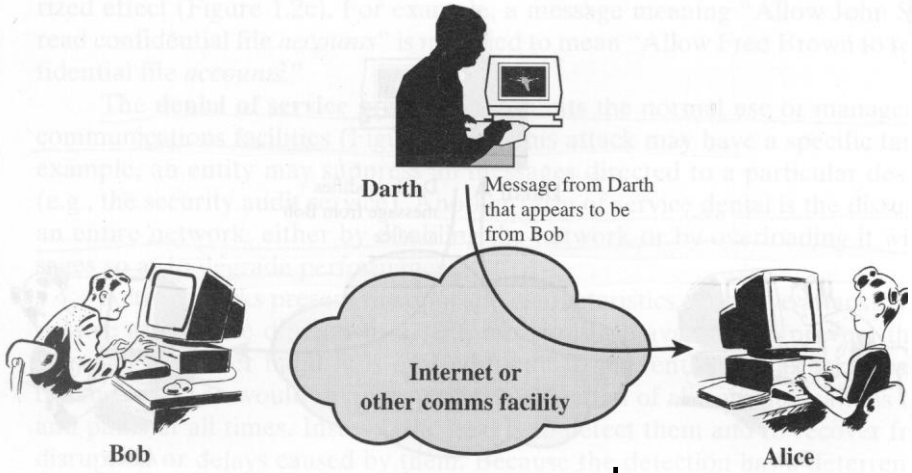


Traffic analysis

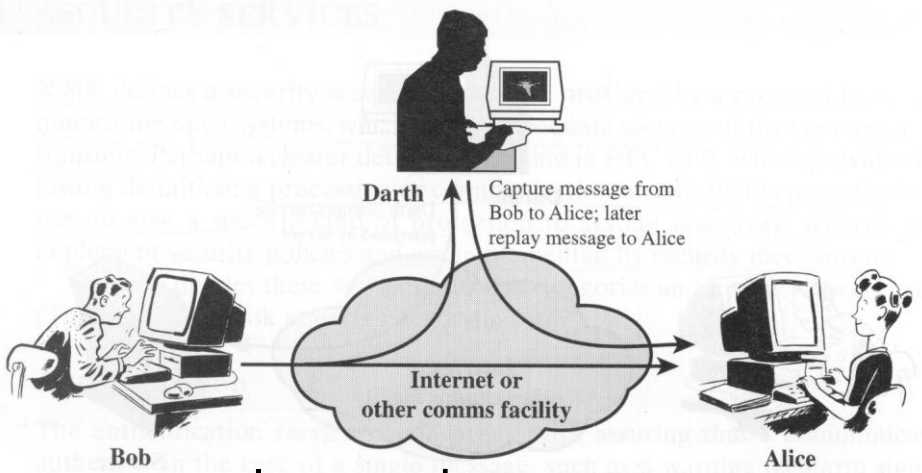
Source: Network Security Essentials 2nd edition, Figure 1.1.

大數據分析、AI

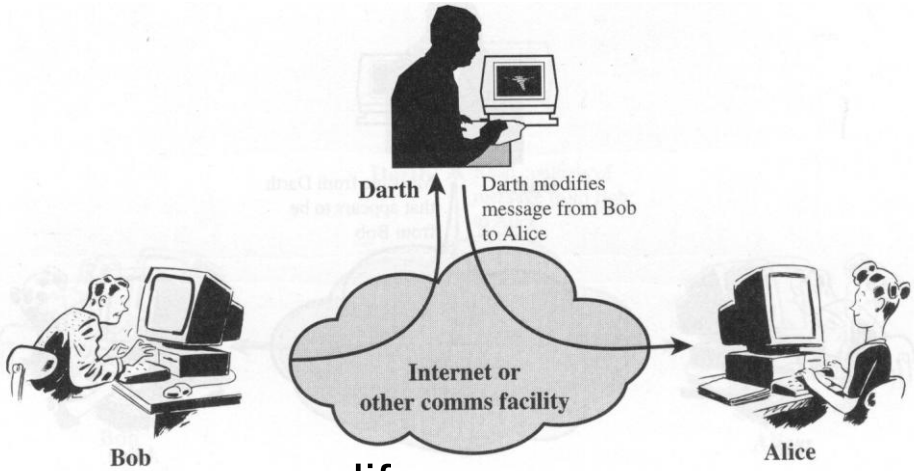
Active attacks



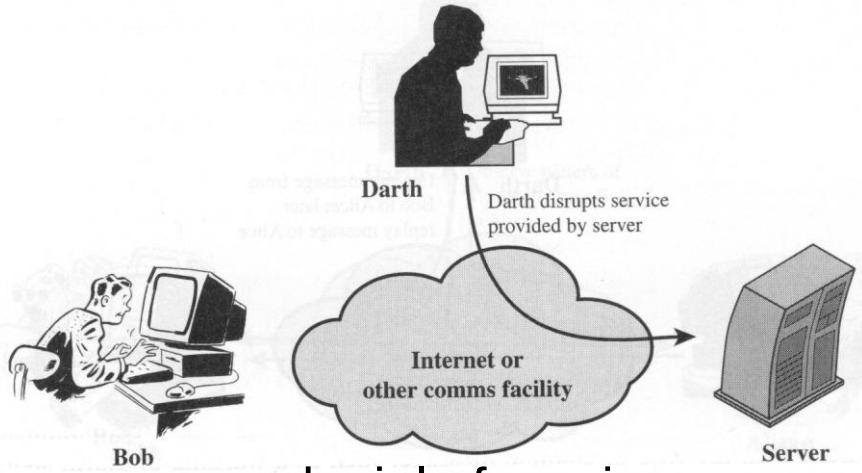
masquerade



replay previous messages

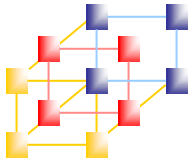


modify messages



denial of service

Source: Network Security Essentials 2nd edition, Figure 1.2



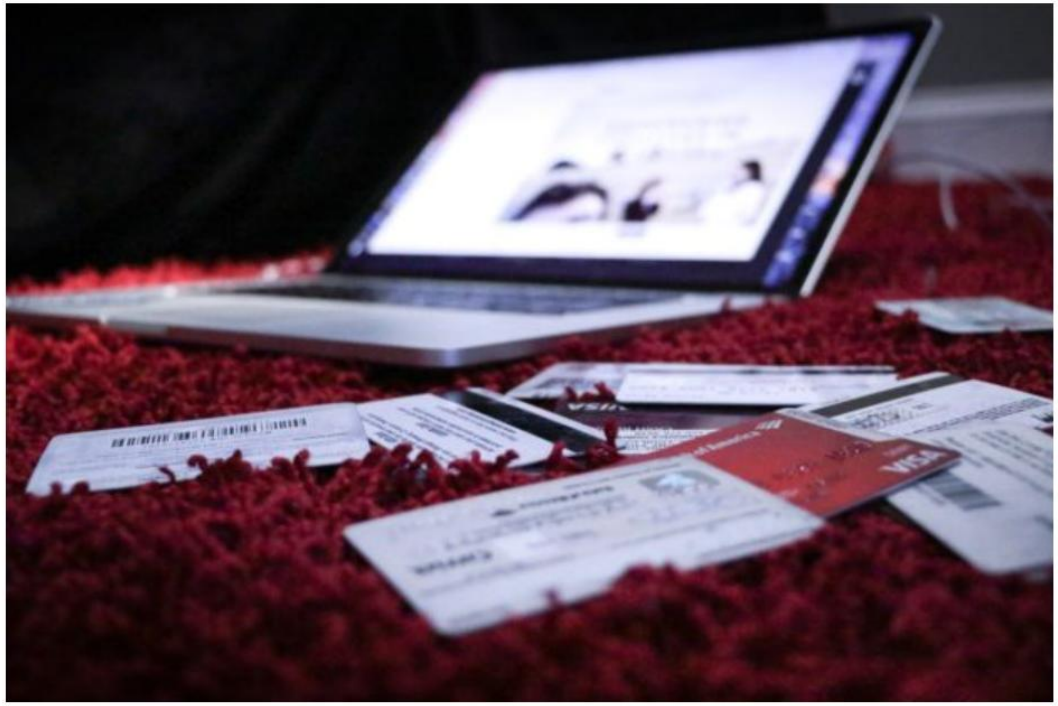
更多攻擊手法

- 主動 v.s. 被動
  - 詐騙電話
  - 網路肉搜
  - 釣魚信件
  - 廣播蓋台
  - 網路蠕蟲
  - 釣魚網站

短訊OTP的安全問題

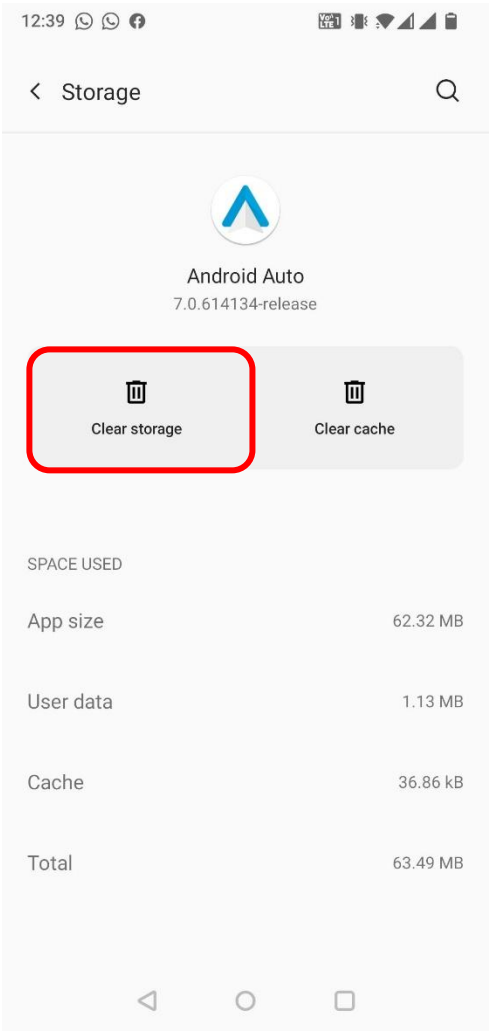
詐騙集團騙個資綁卡盜刷，金管會提醒留意 1 元簡訊

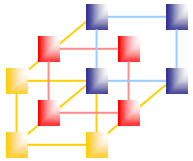
作者 中央社 | 發布日期 2022 年 06 月 29 日 10:30 | 分類 第三方支付 , 網路 , 資訊安全 分享 分享 Follow 讚 273 分享



您曾注意APP要哪些權限嗎？

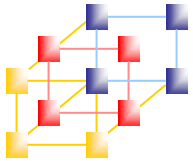
- 網路銀行為什麼需要以下權限？
  - 位置 - 你在哪
  - 相機 - 你拍什麼照
  - 麥克風 - 你說什麼
  - 電話 - 你打給誰
  - 儲存空間 - 你手機有什麼
  - 聯絡人 - 你有哪些朋友
- 不允許還不給用 @?@
- 解決方案
  - 每次使用完均將該APP還原預設值





網銀操作風險

- 非約定轉帳流程？
- 網路銀行用什麼連？
- 驗證短訊用什麼收？
- 攻擊者怎麼玩？
  - 寄惡意連結讓受害者點擊
  - 點擊後受害者手機即被安裝後門程式
  - 透過釣魚網站取得受害者的網銀登入資訊
  - 攻擊者使用網銀轉帳
  - 後門攔截受害者收到驗證短訊並自動轉送給攻擊者
  - 攻擊者在神不知鬼不覺下完成非約定轉帳作業



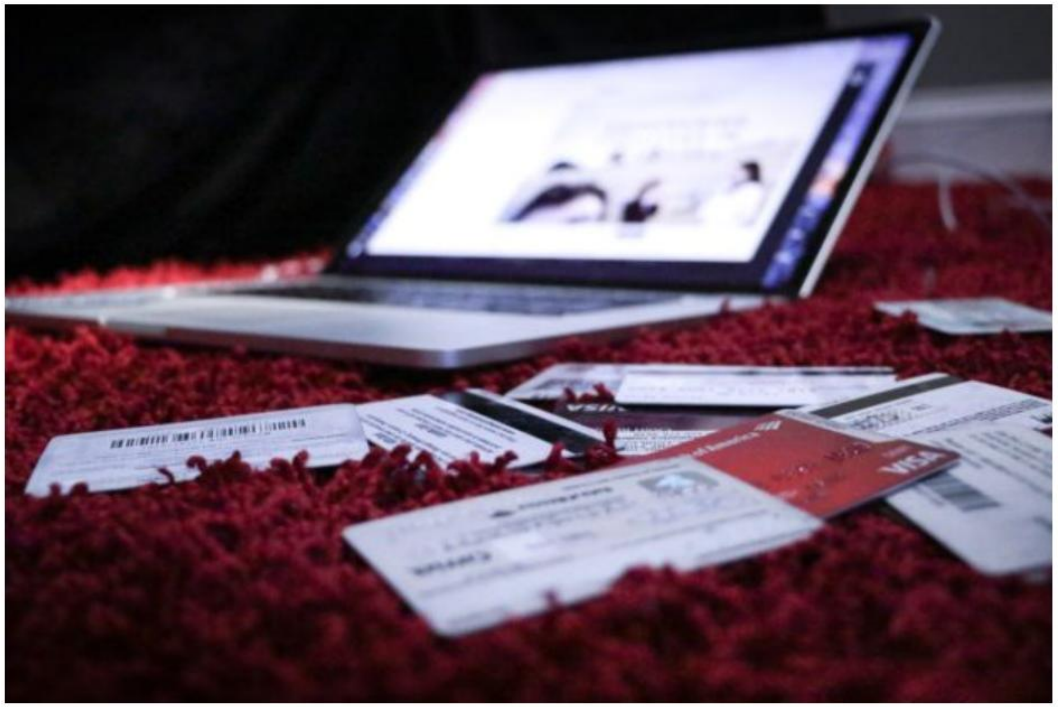
SMS二階段驗證真的不能用？

- 2017年NIST建議企業不要再透過簡訊或電話語音方式進行二次驗證。← 知道為什麼了吧！
- 可是現在還是到處都在用，怎麼辦？！

短訊OTP的安全問題

詐騙集團騙個資綁卡盜刷，金管會提醒留意 1 元簡訊

作者 中央社 | 發布日期 2022 年 06 月 29 日 10:30 | 分類 第三方支付 , 網路 , 資訊安全 分享 分享 Follow 讚 273 分享



最近很流行的FIDO

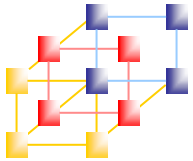
工商時報

銀行攜手券商 推動金融FIDO

孫彬訓 / 台北報導

2024年1月1日

Source: 工商時報



無密碼身分驗證是怎麼回事

沒有密碼 ✕ / 人不需要記憶密碼 ✓

- 密碼安全儲存在手機裡，用人臉、指紋解鎖
  - 手機掉了怎麼辦？
  - 人臉、指紋多次辨識失敗怎麼辦？

-->問題沒有消失，只是不斷轉移

網銀操作風險防範

網銀用：

短訊用：

專家永遠是對的？

簡單一動作防止手機被駭！專家：每天關機5分鐘

2023/06/24 11:25
文 / 記者吳佩樺

專家Priyadarsi Nanda表示，許多使用者經常沒有意識到有應用程式在後台運行，固定將手機關機，可阻止或強制關閉在後台運行的間諜等惡意軟體。類似說法美國國家安全局NSA過去也曾提出過，至少一週將手機關機再重新關機。

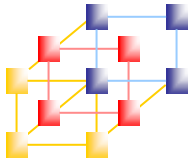
不過報導中也說，該措施對付像NSO的pegasus這樣的高度複雜間諜軟體，可能沒有太大的作用，但還是建議大家這樣做。

https://3c.ltn.com.tw/news/53850

想一想：
惡意程式的目標是什麼？
→持續存活，共存共榮
How？重開機有用嗎？
→有用他們就不會上新聞了

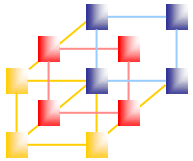
另一個案例

- 您有用過Keyless嗎？
- 您家住透天嗎？
- 您回家怎麼放鑰匙？
- 在門口放鑰匙盤嗎？



一定要認真看看這個神奇影片

- https://www.youtube.com/watch?v=bXfp8F4J2eI



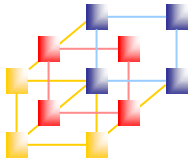
Quiz 2

- 請問這是主動攻擊還是被動攻擊？
  - 請大家寫在紙條上，下課前收來講桌。
  - ((記得寫上班級姓名學號

科技始終來自於惰性

- 電腦下單、手機收OTP → 手機下單、手機收OTP
- 鑰匙 → 遙控器 → Key Less / Push Start

- 漏洞往往不是一開始就有
  - 新科技 → 習慣改變最小化，方便最大化
  - 新攻擊 → 新科技套用舊場景產生的防護缺口



DDoS攻擊

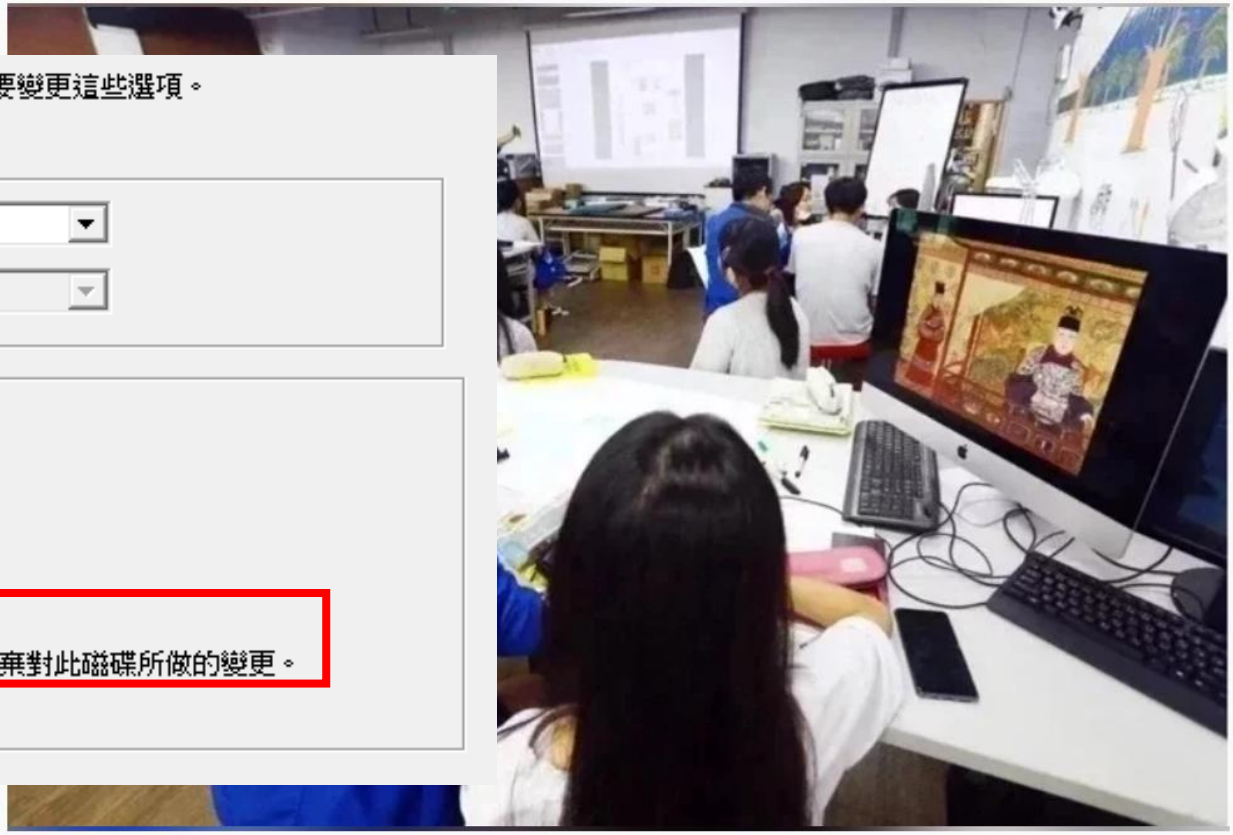
- 7-11門口的黑衣人？！
- 網路設備也變成幫兇

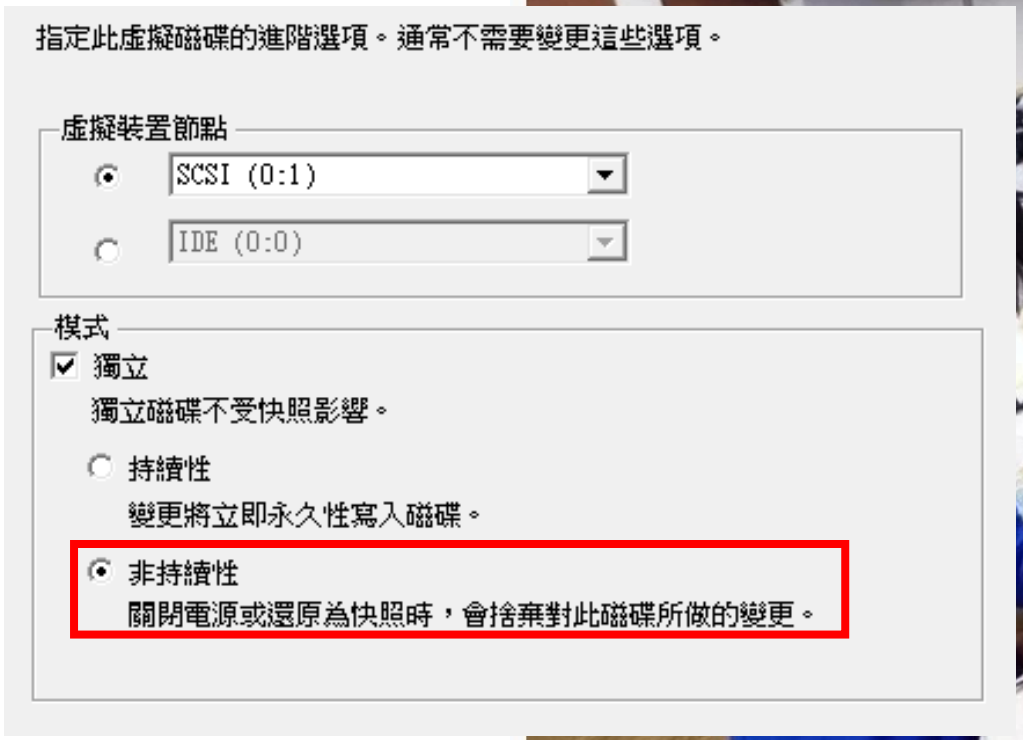
但是...資安事件不只來自攻擊

- 還有手殘

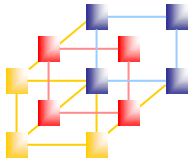
2.5萬筆學習歷程檔案遺失 81校7千人受災

2021-09-26 01:06 聯合報 / 記者趙宥寧、江良誠／連線報導



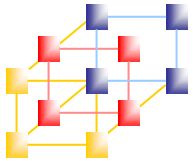


(udn.com)



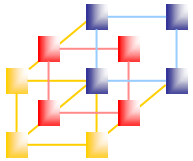
大家怎麼備份自己的資料？

- 上雲一切OK？！
- 快照？磁帶？
- 3-2-1備份
- 備份有沒有倒回測試過？
  - 有次可憐的某客戶被加密怕了
  - 詢問我們該怎麼自動整機備份實體機？



Security services

- Definition of X.800
  - A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- Definition of RFC 2828
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

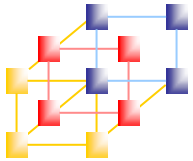


Categories of X.800 security services

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation
- Availability

Authentication

- The assurance that the communicating entity is the one that it claims to be
  - Peer entity authentication
    - Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - Data-origin authentication
    - In a connectionless transfer, provides assurance that the source of received data is as claimed.

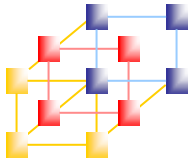


How to Authentication?

- What you know?
- What you have?
- What you are?

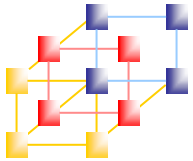
→ 各有優缺點

- 2FA / MFA



有關身分認證方式

- Type I – Something you know
  - ID/PW
  - 優勢？缺點？
- Type II – Something you have
  - Token/OTP
  - 優勢？缺點？
- Type III – Something you are
  - Biometric
  - 優勢？缺點？



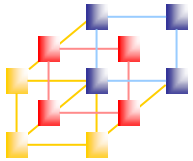
多因子認證 2FA / MFA

同時使用兩個以上的認證類型

– 帳號 + 密碼 + PIN碼？	→I + I	✗
– 晶片卡 + OTP？	→II + II	✗
– 虹膜 + 指紋？	→III + III	✗
– 晶片卡 + 指紋？	→II + III	✓
– 臉部辨識 + 指紋？	→III + III	✗
– PIN碼 + 指紋？	→I + III	✓
– 晶片卡 + PIN碼？	→II + I	✓

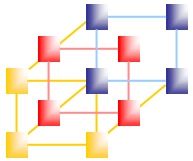
Access control

- The prevention of unauthorized use of a resource

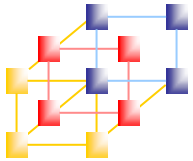
使用者驗證 v.s. 存取控制

- ATM領錢要插卡輸入密碼
- 手機沒繳錢被鎖卡
- 打開手機要壓指紋
- 小朋友撿到iPhone登不進去
- 進出車站有閘門
- 刷悠遊卡可以借Ubike
- 進入摳死摳要出示會員卡
- 在摳死摳結帳要刷會員卡



Data confidentiality

- The protection of data from unauthorized disclosure
  - Connection confidentiality
    - The protection of all user data on a connection.
  - Connectionless confidentiality
    - The protection of all user data in a single data block
  - Selective-field confidentiality
    - The confidentiality of selected fields within the user data on a connection or in a single data block.
  - Traffic-flow confidentiality
    - The protection of the information that might be derived from observation of traffic flows.



有點玄

- 來看看原文：

5.2.3.1 *Connection confidentiality*

This service provides for the confidentiality of all (N)-user-data on an (N)-connection.

Note – Depending on use and layer, it may not be appropriate to protect all data, e.g. expedited data or data in a connection request.

5.2.3.2 *Connectionless confidentiality*

This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU.

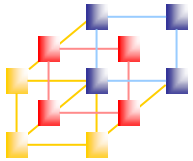
5.2.3.3 *Selective field confidentiality*

This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU.

5.2.3.4 *Traffic flow confidentiality*

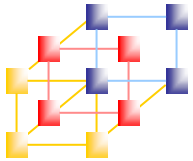
This service provides for the protection of the information which might be derived from observation of traffic flows.

(Source: ITU X.800)



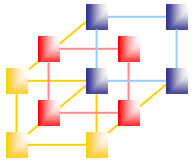
Data integrity (1/2)

- The assurance that data received are exactly as sent by an authorized entity
  - Connection integrity with recovery
    - Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
  - Connection integrity without recovery
    - As above, but provides only detection without recovery.



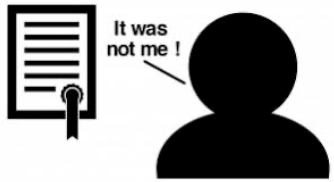
Data integrity (2/2)

- Selective-field connection integrity
  - Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- Connectionless integrity
  - Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- Selective-field connectionless
  - Integrity provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.



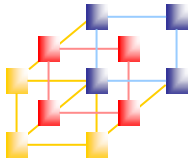
Non-repudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication
  - Non-repudiation, origin
    - `Proof that the message was sent by the specified party.`
  - Non-repudiation, destination
    - `Proof that the message was received by the specified party.`



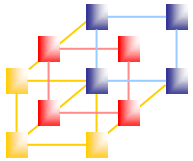
Availability

- The property of a system / resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.



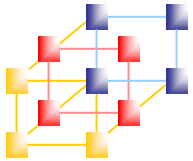
Security mechanisms (X.800)

- Specific security mechanisms
  - May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
- Pervasive security mechanisms
  - Mechanisms that are not specific to any particular OSI security service or protocol layer



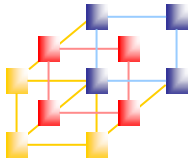
Specific security mechanisms (1/2)

- Encipherment
  - The use of *mathematical algorithms* to transform data into a form that is *not readily intelligible*. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
- Digital signature
  - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit *to prove the source and integrity of the data unit* and *protect against forgery* (e.g., by the recipient).
- Access control
  - A variety of mechanisms that enforce *access rights* to resources.
- Data integrity
  - A variety of mechanisms used to assure the *integrity* of a data unit or stream of data units.



Specific security mechanisms (2/2)

- Authentication exchange
  - A mechanism intended to ensure the identity of an entity by means of information exchange. (透過訊息交換來確保實體身份)
- Traffic padding
  - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- Routing Control
  - Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- Notarization (公正的第三者)
  - The use of a trusted third party to assure certain properties of a data exchange.



Pervasive security mechanisms

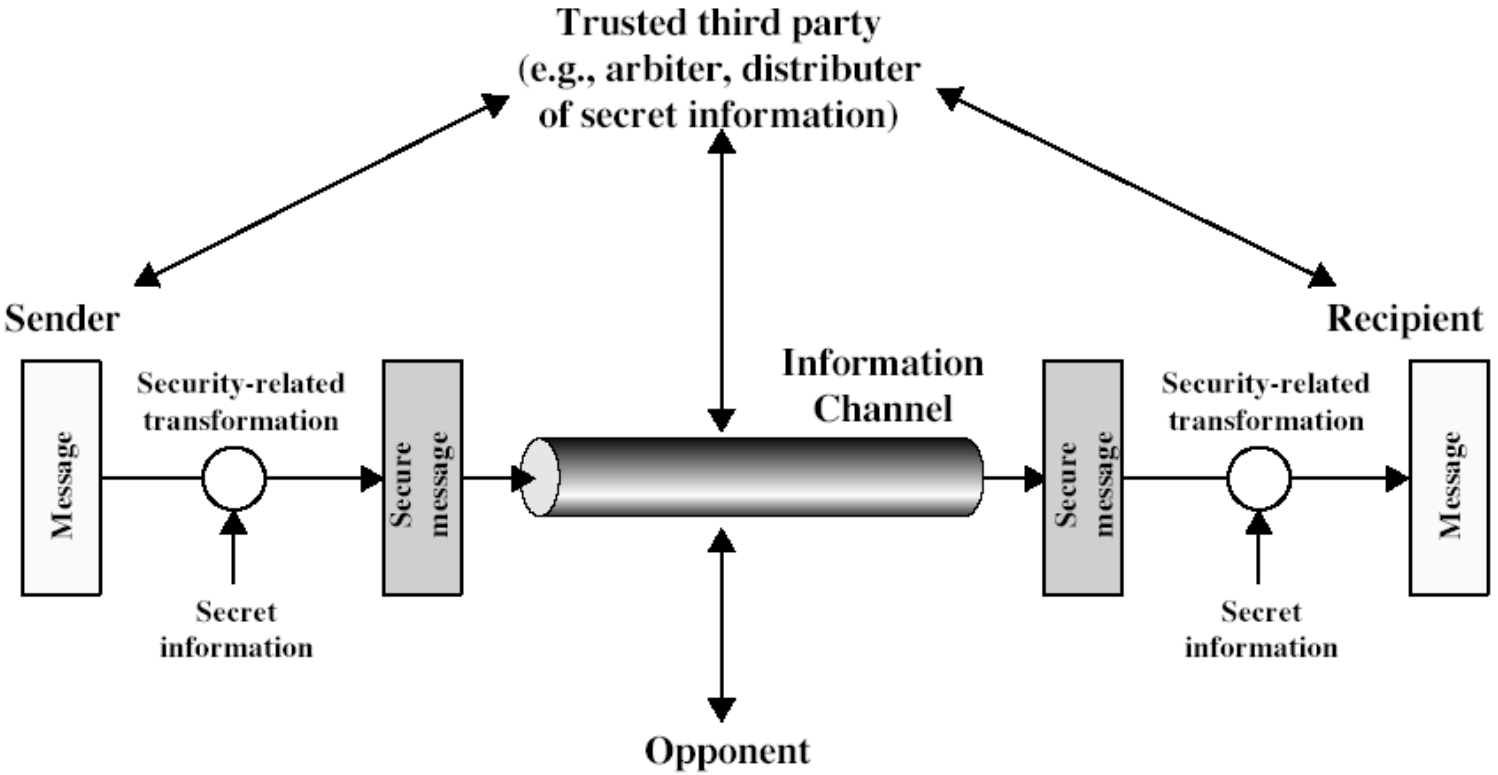
- Trusted functionality
  - That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
- Security label
  - The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- Event detection
  - Detection of security-relevant events.
- Security audit trail
  - Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
- Security recovery
  - Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Relationship between security services and mechanisms

	Mechanism							
Service	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Source: Network Security Essentials 2nd edition, Table 1.5

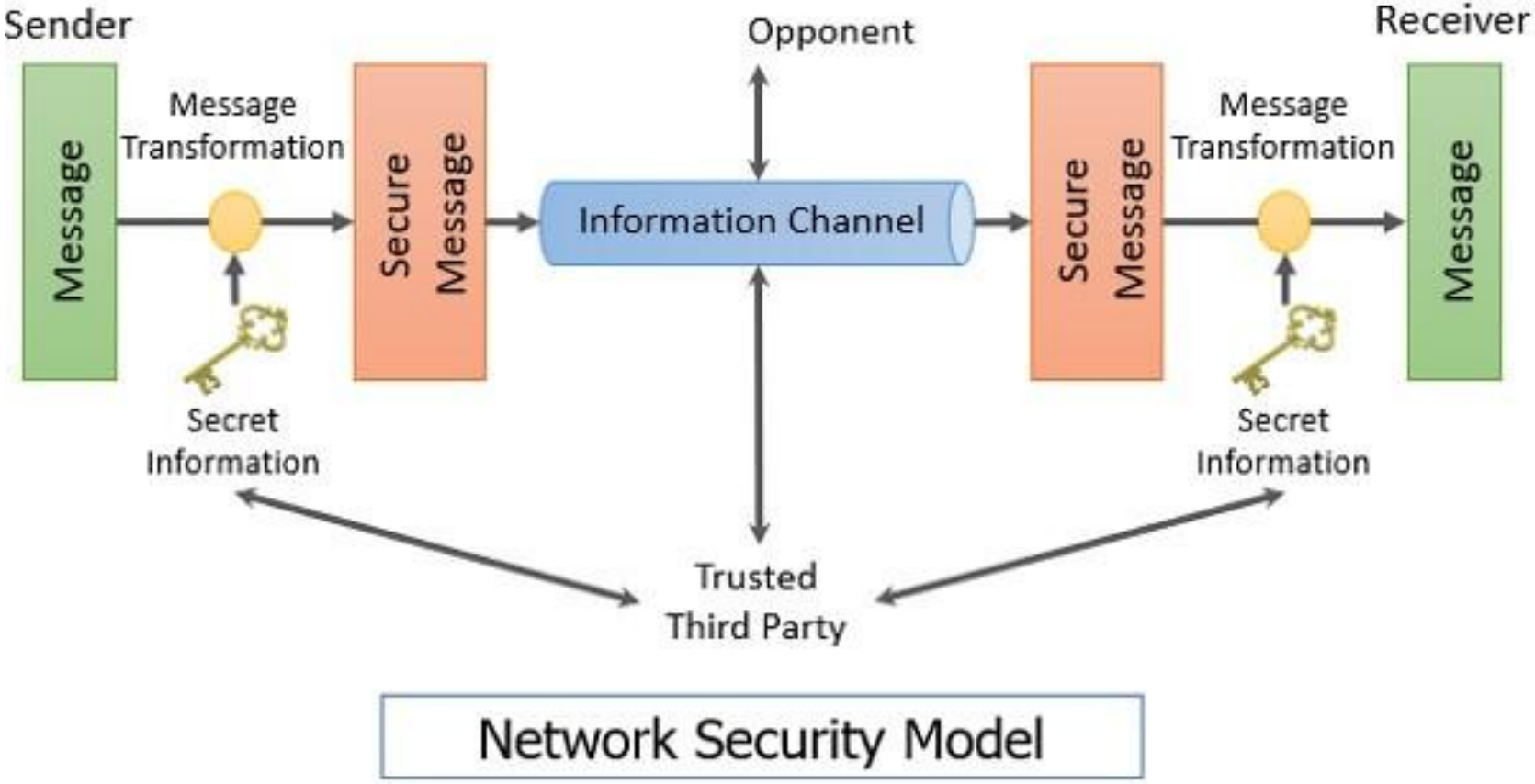
Network security model (1/2)

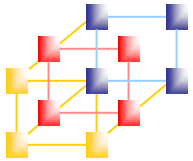


Source: Network Security Essentials 2nd edition, Figure 1.3

其實有更棒的圖

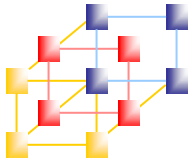
- https://binaryterms.com/network-security-model.html





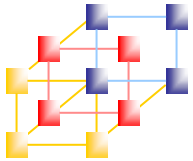
Network security model (2/2)

- Four basic tasks in designing a particular security services
  - Design a suitable *algorithm* for the *security transformation*
  - Generate the *secret information* (*keys*) used by the algorithm
  - Develop methods to *distribute* and *share* the secret information
  - Specify a *protocol* enabling the principals to use the transformation and secret information for a security service



什麼是安全的加解密方法？

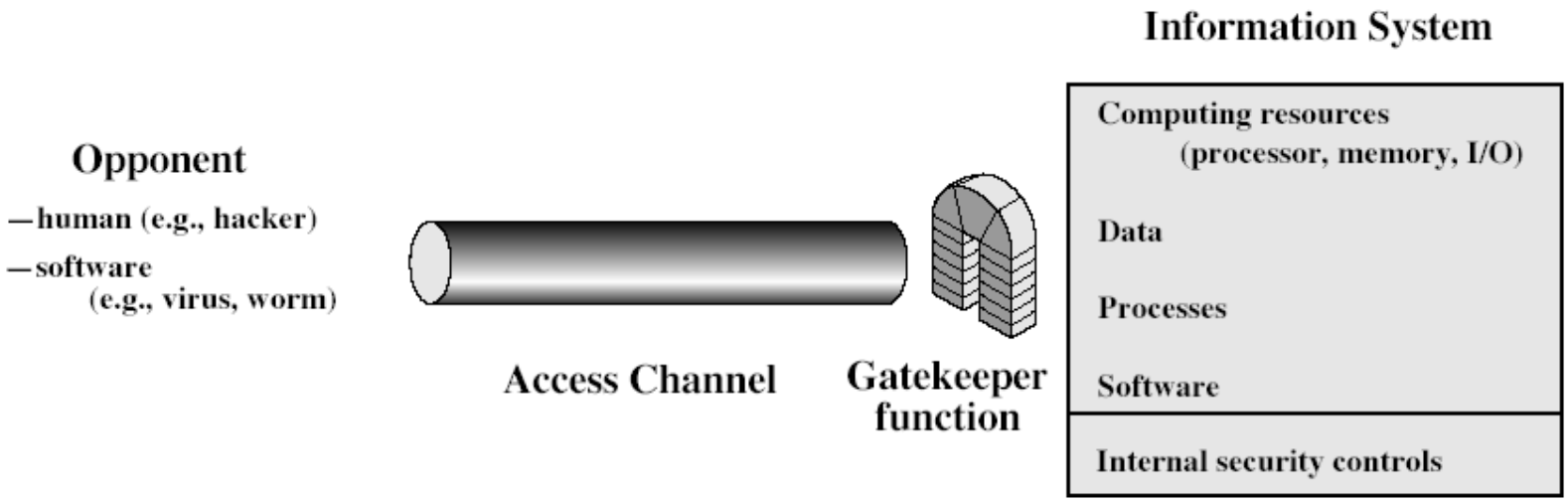
- 你說安全就安全？
- 我說安全就安全？
- 微軟說安全就安全？
- 美國政府說安全就安全？
- 誰說的算數？



安全的加解密方法

- Dutch cryptographer Auguste Kerckhoffs in the 19th century
  "**A cryptosystem should be secure even if everything about the system, except the key, is public knowledge**"
- **除了金鑰以外都可以公開**

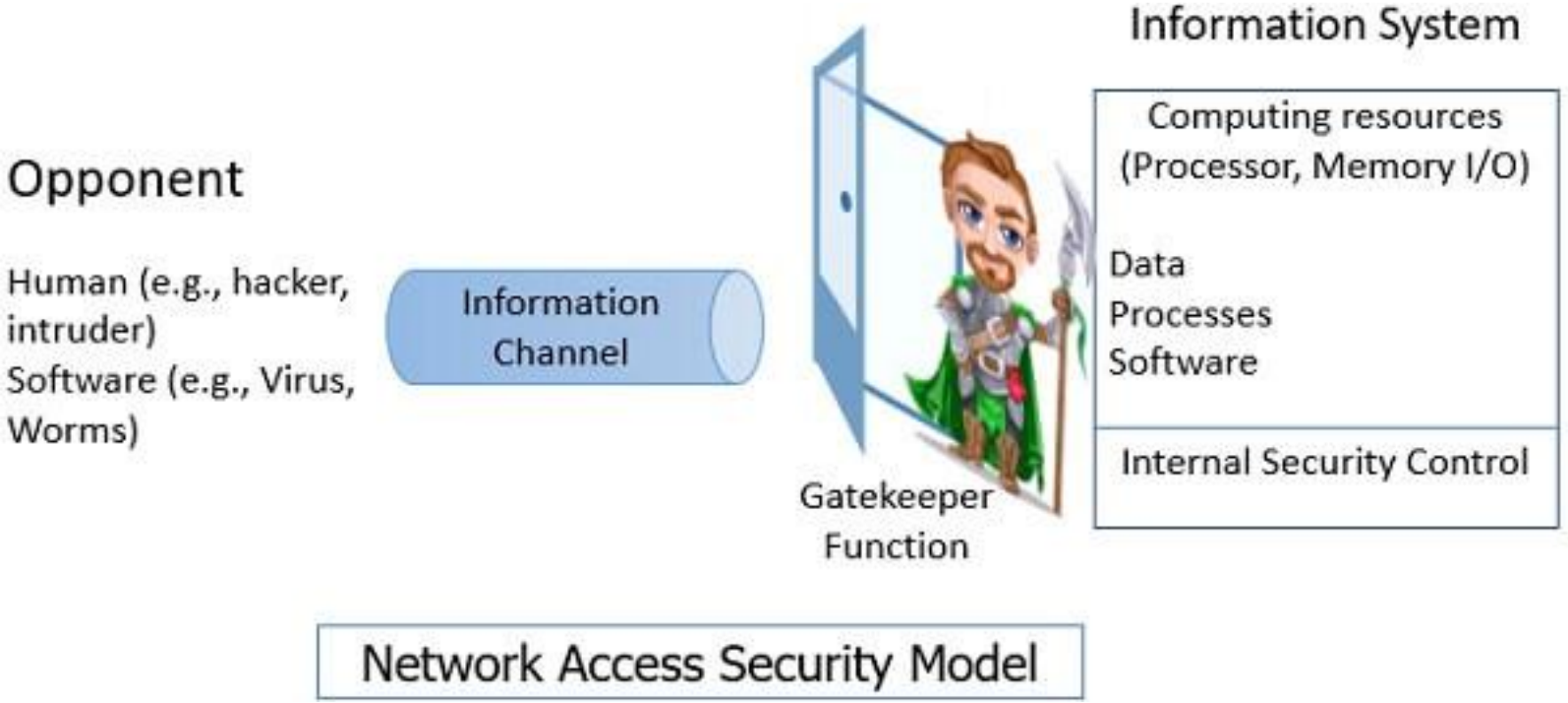
Network access security model (1/2)

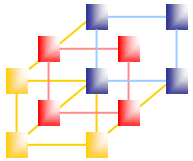


Source: Network Security Essentials 2nd edition, Figure 1.4

其實有更棒的圖

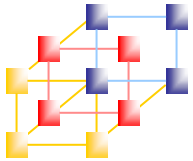
- https://binaryterms.com/network-security-model.html





Network access security model (2/2)

- Two components require by this model
  - An appropriate *gatekeeper* functions to *identify users*
  - Implement security controls to ensure only authorized users access designated information or resources

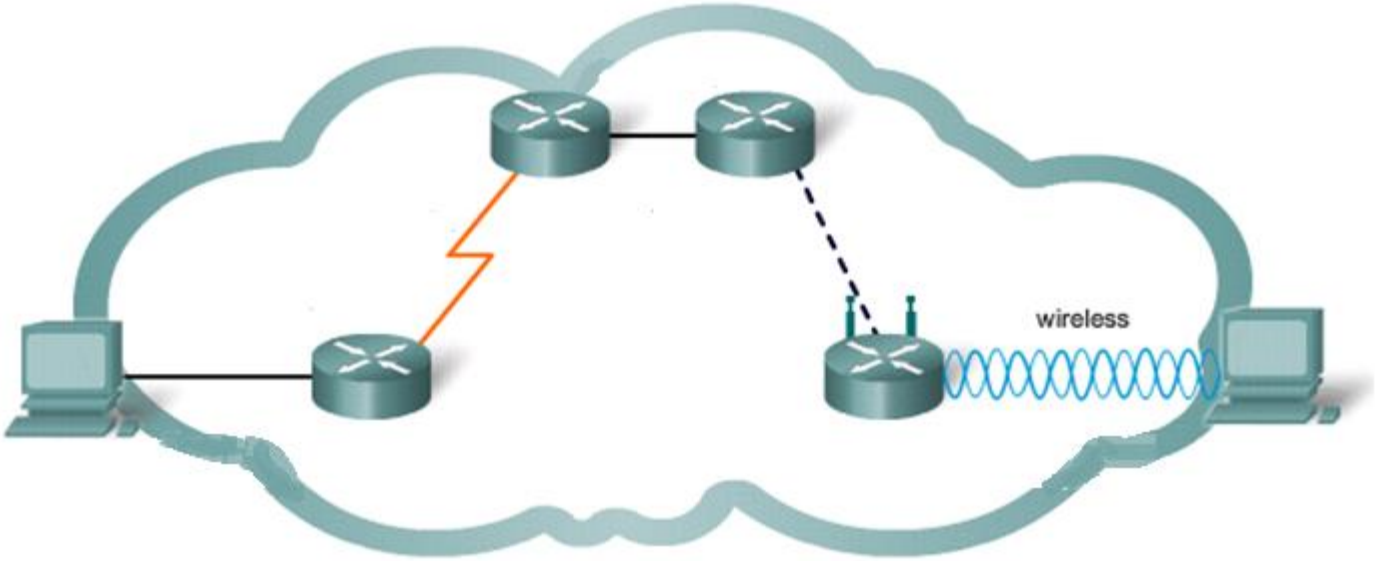


複習一下

- 不記得的趕快Google
  - OSI七層和TCP/IP四層的異同？
  - 每一層有什麼主要功用？
  - IPv4的特性與限制？

About LAN

- Subnet Mask、Default Gateway是什麼？
- 誰跟誰在同一個Subnet？
- 誰連到誰要透過Default Gateway？
- Router、Switch和Hub有什麼不同？



OSI protocol stack *v.s.* protocols

TCP/IP Model	OSI Model	Protocols
Application	Application	HTTP, SMTP, SNMP, FTP, Telnet
	Presentation	XML
	Session	SSL, TLS, SSH, RPC, NetBIOS, ASP
Transport	Transport	TCP, UDP
Internet	Network	IP, ICMP, IPSec
Network Access	Data Link	Ethernet, Token Ring, PPP, PPTP, L2TP
	Physical	Electricity, Radio, Laser


Router

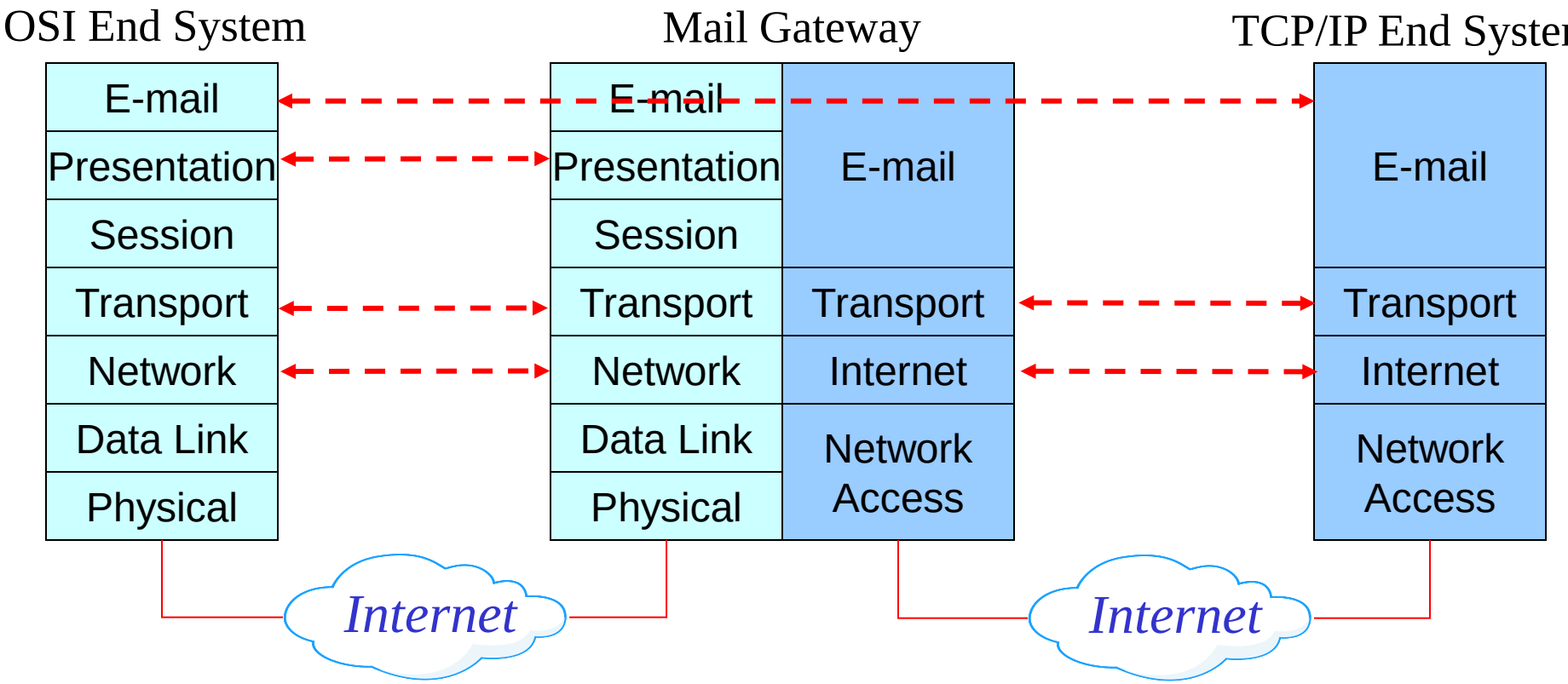

Switch


Repeater

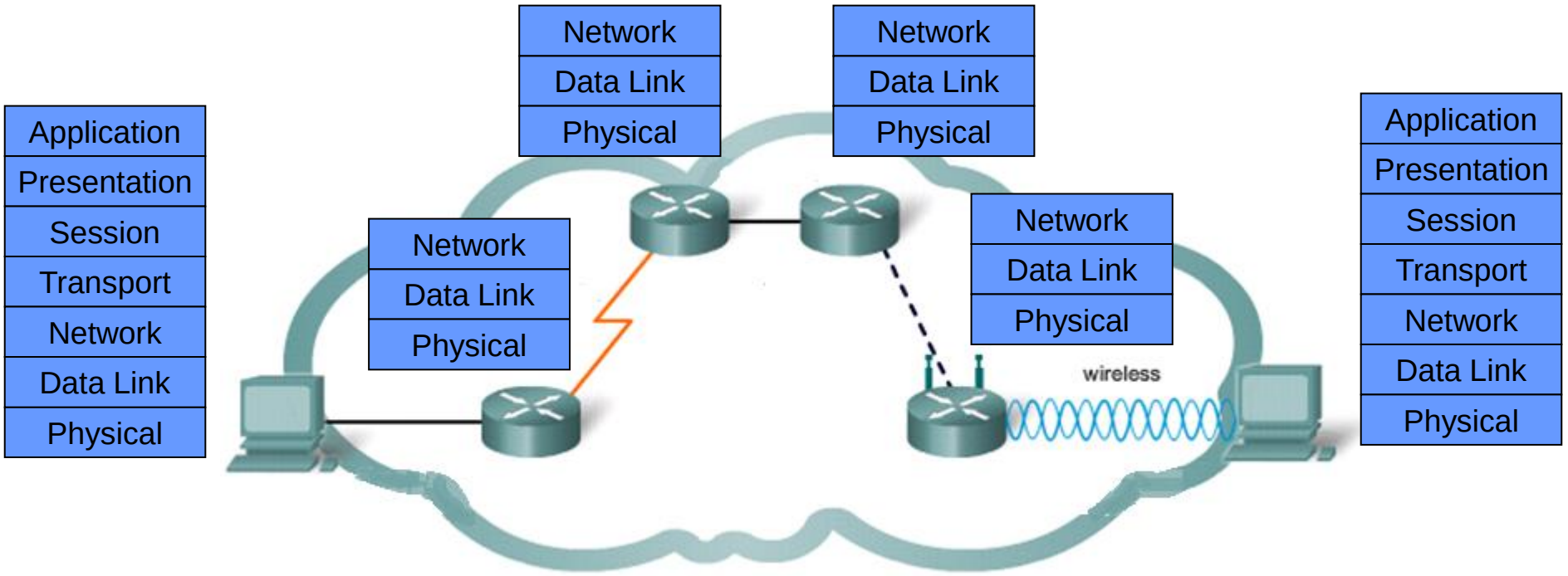
Data encapsulation

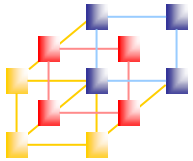
Application	Data	The doorway to the application protocol. (e.g. SMTP)
Presentation	Data	Transform into the common format (e.g. Host order to network order, encryption, compression, …)
Session	Data	Set, maintain, or release connection
Transport	sport, dport | Data	Provide flow control, error detection and correction
Network	S_IP, D_IP, Proto | Data	Logical addressing and path decision
Data Link	S_MAC, D_MAC | Data | FCS	Bits string transmission and frame check sequence
Physical	Data | CRC	Electrical signal

Encryption coverage implications of store-and-forward communication



Network security overview

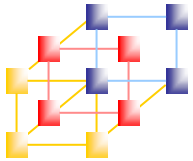




Quiz N

- Authentication v.s. Access Control
  - 這兩者有什麼不同，請用一句話簡述？
  - 實作時的順序為何，誰先誰後？
  - 請暫時先不要交上來 Xda

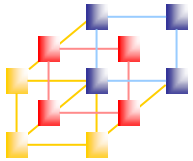
- https://www.movieffm.net/drama/155034/
  → 8:45開始 (SE4EP5)



Quiz N

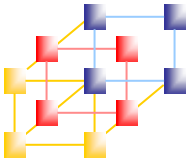
- Authentication v.s. Access Control
  - 請寫下影片中的任何一種身分驗證方法
  - 請寫下影片中的任何一種存取控制方法

- 請將答案寫在紙條上，下課前收來講桌。
- ((請記得寫上班級姓名學號



有關線上支付&盜刷

- 線上支付安全嗎？
- 行動支付、第三方支付、電子支付 - ？
  - Apple Pay / Google Pay → 手機刷卡
  - PayPal / 紅陽 /綠界 / 藍新 → 中介及金流介接
  - 街口 / 歐付寶 → 存錢花錢轉帳…
- 他們安全嗎？
  - 最後的交易媒介到底是什麼？
  - 盜刷風險誰承擔？



有關線上支付&盜刷

- 先看行動支付 – Apple Pay、Google Pay
  - 他們的本質就是信用卡
  - 您知道失卡零風險嗎？ - 例外：3D驗證
  - 我被盜刷的經驗
    - 只是去個威秀售票機買個電影票，電影還沒看完就...
    - 只是在家裡睡覺，睡一睡就...

失卡零風險

失卡零風險

- 持卡人之信用卡/金融信用卡如有遺失、被竊、被搶、詐取或其他遭持卡人以外之第三人占有之情形(以下簡稱遺失或被竊等情形)，應儘速以電話或其他方式通知銀行或其他經銀行指定機構辦理掛失停用手續，並繳交掛失手續費每卡新臺幣200元。惟持卡人如尋獲已掛失之信用卡/金融信用卡並於辦理掛失時起七日內繳還銀行者，其所繳掛失手續費，銀行將全額返還持卡人。另如銀行認有必要時，應於受理掛失手續日起十日內通知持卡人，要求於受通知日起三日內向當地警察機關報案或以書面補行通知銀行。
- 持卡人自辦理掛失停用手續時起被冒用所發生之損失，由銀行負擔，惟自發生信用卡/金融信用卡遺失或被竊等情形時起至辦理掛失停用手續前被冒用所發生損失之百分之五，最高以新臺幣3,000元為限，由持卡人負擔。
  （白金卡以上等級之持卡人免負擔此項費用）

https://www.megabank.com.tw/personal/credit-card/rights/card-claim

失卡零風險

- 如有下列情形之一者，持卡人免負擔自負額：

1. 持卡人於辦理信用卡/金融信用卡掛失手續時起前24小時以後被冒用者。
2. 冒用者在簽單上之簽名，以肉眼即可辨識與持卡人之簽名顯不相同或以善良管理人之注意而可辨識與持卡人之簽名不相同者。
3. 冒用者於銀行同意辦理特定金額內免簽名之特約商店進行免簽名交易，且經確認非與持卡人串謀之交易。

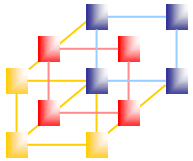
- 如有下列事由之一者，且銀行能證明已盡善良管理人之注意義務者，自發生信用卡/金融信用卡遺失或被竊等情形時起至辦理掛失停用手續前被冒用所發生之損失，概由持卡人負擔：

1. 持卡人得知信用卡/金融信用卡遺失或被竊等情形而怠於立即通知銀行，或持卡人發生信用卡/金融信用卡遺失或被竊等情形後，自當期繳款截止日起已逾二十日仍未通知銀行者。
2. 持卡人違反信用卡約定條款第九條第一項/金融信用卡約定條款之信用卡功能約定條款第八條第一項約定，未於信用卡/金融信用卡簽名致遭第三人冒用者。
3. 持卡人於辦理信用卡/金融信用卡掛失手續後，未提出銀行所請求之文件、拒絕協助調查或其他違反誠信原則之行為者。
4. 在自動化設備被冒用所發生之損失。

- 如有下列事由之一者，無論發生於辦理掛失停用手續前後，被冒用所發生之損失概由持卡人負擔：

1. 第三人之冒用為持卡人容許或故意將信用卡/金融信用卡交其使用者。
2. 持卡人故意或重大過失將使用自動化設備辦理預借現金或進行其他交易之交易密碼或其他辨識持卡人同一性之方式告知第三人知悉者。
3. 持卡人與第三人或特約商店偽造虛構不實交易行為或共謀詐欺者。

https://www.megabank.com.tw/personal/credit-card/rights/card-claim



有關線上支付&盜刷

- 第三方支付 – PayPal…
  - 他們只是中介者，最後還是綁傳統媒介付款
  - 因此回到前一頁的問題
  - 您還害怕信用卡被盜刷嗎？

有關線上支付&盜刷

- 電子支付－以街口為例
  - 街口就是一間軟體公司

街口支付 JKOPAY

最新公告 媒體報導 使用說明 下載 街口電子支付 店家專區

第十一條 責任之限制與排除

1. 致生交易款項之原因事實及其交易關係，僅存在於付款方與收款方之間，本平台服務部分僅依付款方與收款方之委託，代為訂購及通知。使用者與其交易相對人間所涉及之商品或服務之銷售、交易方式及條件、以及交易之履行或不履行（包括但不限於拒絕履行、遲延、未交付、瑕疵、錯誤、退換貨及退款）等，其權利義務關係僅存在於使用者與其交易相對人之間，並由使用者依相關法令及其與交易相對人間之約定互負權利、義務或責任。使用本平台服務不代表本平台對於各該交易之履行有任何明示或默示之保證或承諾。

2. 若收款方或付款方之交易金額及次數受到限制，因而無法接受交易相對人之支付款項時，對於因此所生之交易不便利、或交易無法完成、或交易糾紛，不得以任何理由向本平台請求賠償其損害或補償其損失。

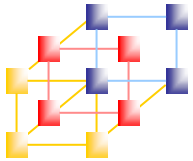
3. 本服務所提供之各項功能，均依該功能當時之現況提供使用，本平台對於其效能、安全性、正確性等，皆不負擔任何明示或默示之擔保責任。

4. 本平台盡力維護應用程式之安全性，惟不保證郵件、檔案或資料之傳輸儲存均正確無誤不會斷線和發生錯誤等，除可歸責於本平台致透過本平台之網頁、伺服器、網域、電子郵件傳輸之郵件、檔案或資料傳送或儲存失敗、遺失或錯誤外，本平台不對因此所致之損害負賠償責任。

5. 因使用者或店家之故意或過失致其帳號及密碼遭盜用、不當使用或有其他相類似之情事時，使用者應自行就因此所致之損害負責。

6. 若本平台依法或依約須負擔賠償責任時，本平台之賠償責任僅限於使用者因本服務所受之金錢上直接損害，而不包括任何衍生之其他損害（包含但不限於間接損失）。

(街口支付)



所以...

- 信用卡和電子支付誰風險比較低呢？