

資安不難， 只怕你太習慣

呂思瑩



目錄

01

資安趨勢

02

資安與你我的關係

03

社交工程破解術

04

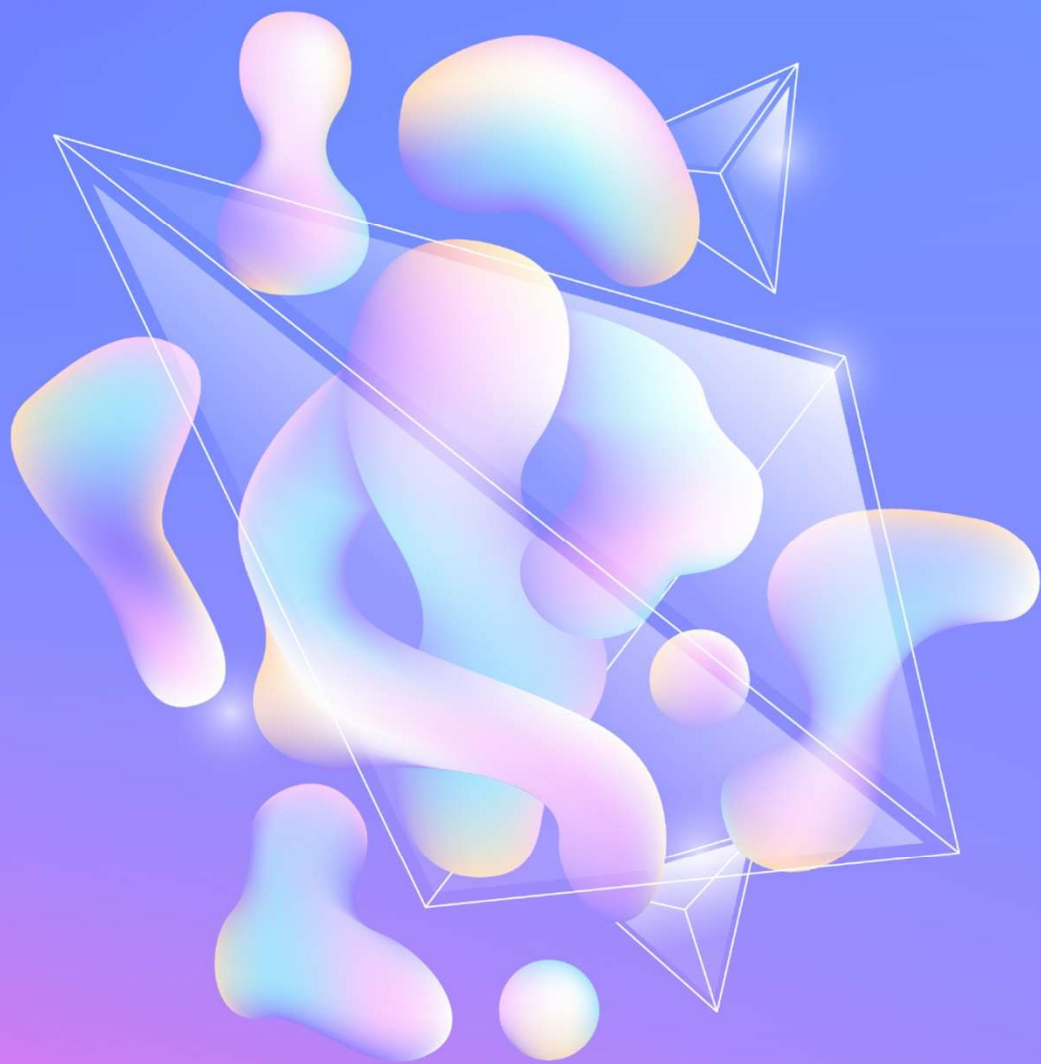
帳號密碼與身份驗證安全

05

資料處理與外洩風險

06

常見的資安NG行為



01

資安趨勢



世界經濟論壇《2025年全球網路安全展望》報告

Global Cybersecurity Outlook 2025


Cybersecurity Complex Factors

Geopolitical tensions

Create uncertainty of risks

Supply chain interdependence

Increase possibility of systemic failures

AI and emerging technocrime

Evolve attack methods, improve effectiveness

Increased regulatory requirements

Add compliance burden on companies

Impact of Geopolitics on Corporate Cyber Strategy

Changing suppliers
16%

Stopping business in certain regions
18%


Stopping business in certain regions
17%

Modifying insurance policies
10%


Public-Private Imbalance in Cybersecurity



Medium-large private



Public sector orgo

Global Cybercrime and Threat Trends



Ransomware attacks
45%

45%



Supply chain attacks
17%



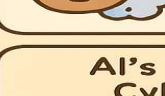
Cyber fraud (phishing, social engineering, etc)
20%

20%



Malicious insiders
7%

7%



Disinformation and cognitive warfare
6%

6%



DDoS attacks
6%

6%

AI's Influence on Cybersecurity



47%
Evolving malicious AI (phishing, deepfake attacks)



Lack of security assessments before AI deployment



63% of organizations lack assessment processes

網路安全日益複雜的因素

主要網路威脅與全球趨勢

地緣政治對企業的網安影響

AI人工智慧對網路安全的影響

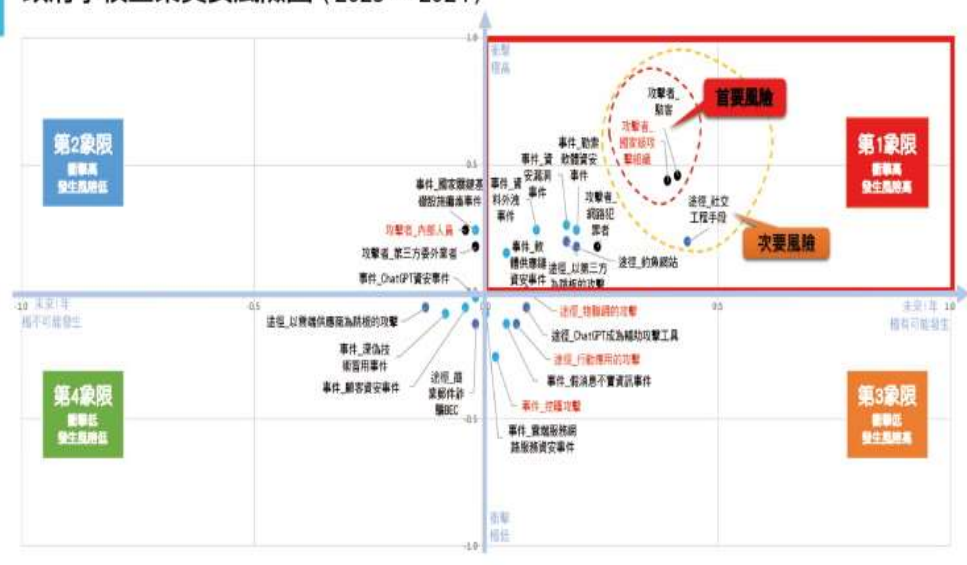
公私部門的網安能力差距

iThome資安大調查-政府學校企業資安風險圖

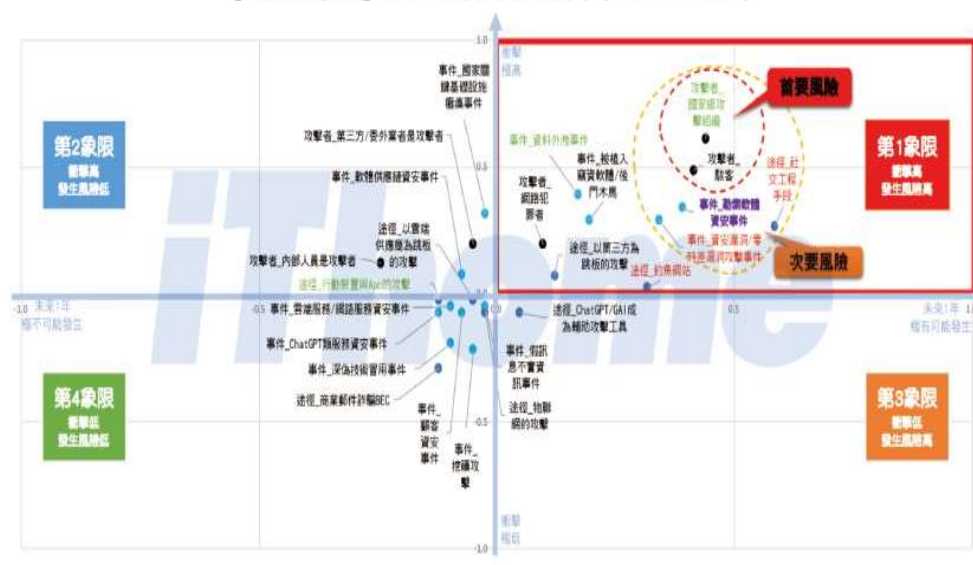
2023~2024

2024~2025

政府學校企業資安風險圖 (2023 ~ 2024)



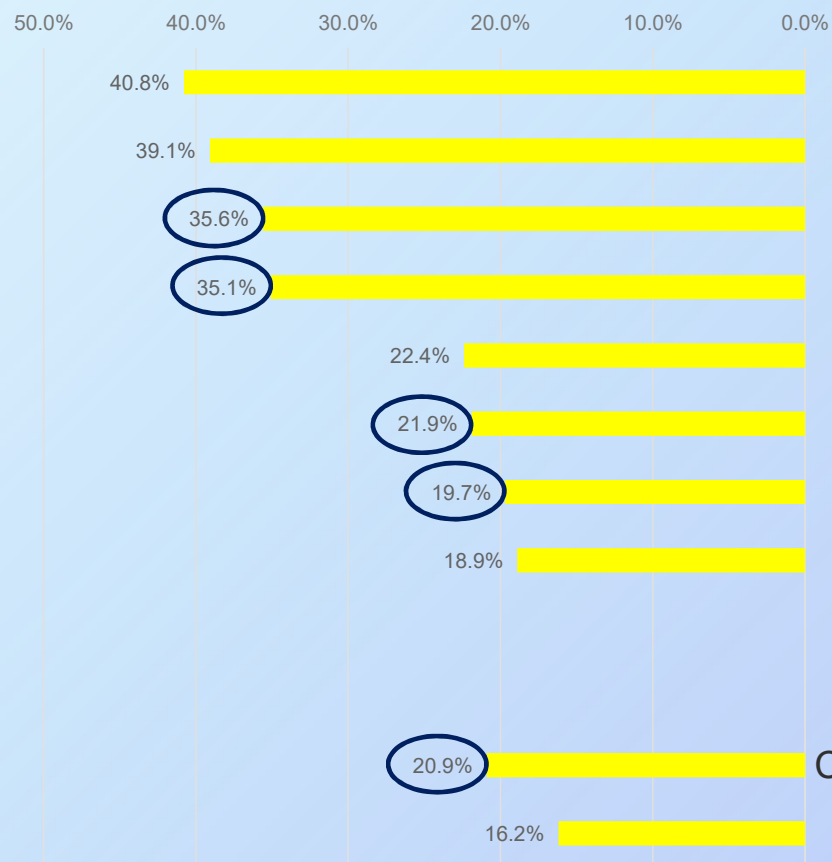
【政府與學校】2024企業資安風險圖 (2024~2025)



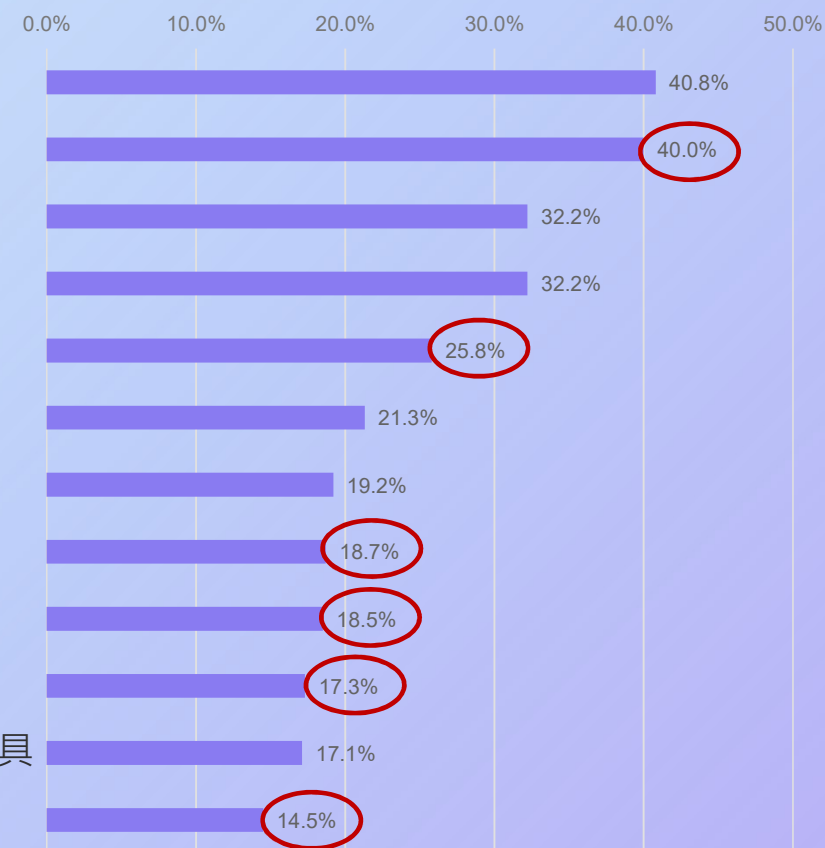
1.主要風險中的國家級攻擊組織的衝擊比去年更大 2.次要風險中的勒索軟體資安事件不論發生風險或衝擊都明顯提高 3.社交工程手段和資安漏洞（零時差漏洞）攻擊事件則是發生風險比去年更高。 4.釣魚網站威脅的發生風險比去年明顯更高 5.資料外洩事件的衝擊也預期會比去年更高。

iThome資安大調查-資安風險

2023年

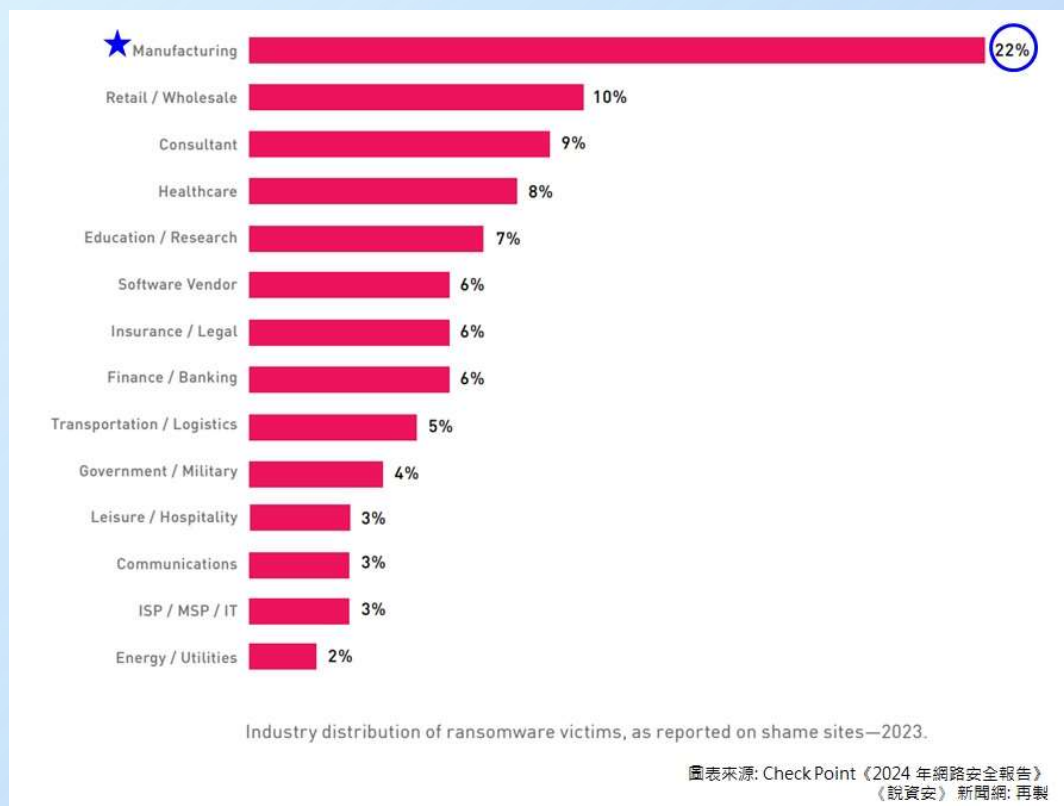


2024年



Check Point 2024 年網路安全報告

勒索軟體攻擊統計

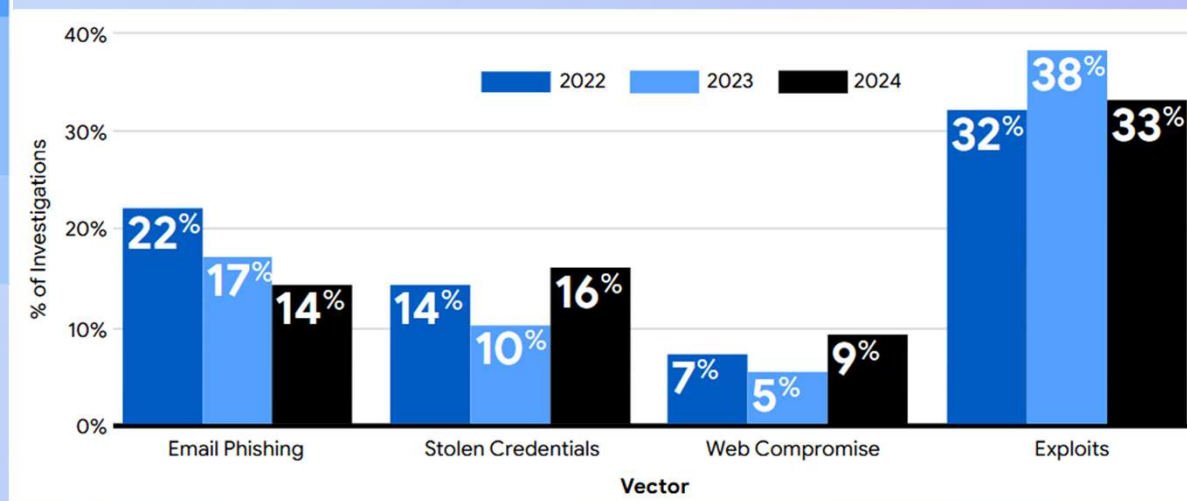


1. 製造業
2. 零售業
3. 顧問業
4. 健康產業
5. 教育、研究
6. 軟體供應廠商
7. 保險業
8. 金融、銀行
9. 交通運輸
10. 政府、國防

資安威脅趨勢分析

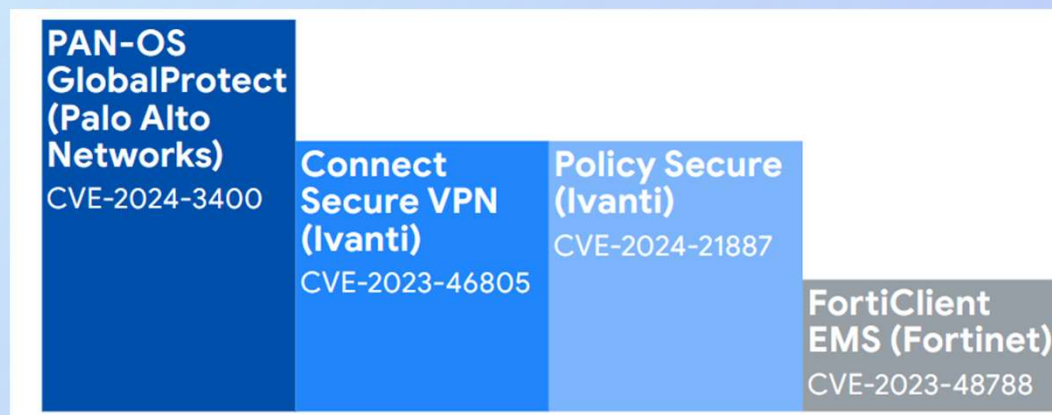
根據Google趨勢報告，持續以弱點利用做為初始入侵手段為主要攻擊策略，社交郵件與權限竊取利用居次

Initial Infection Vector, 2024



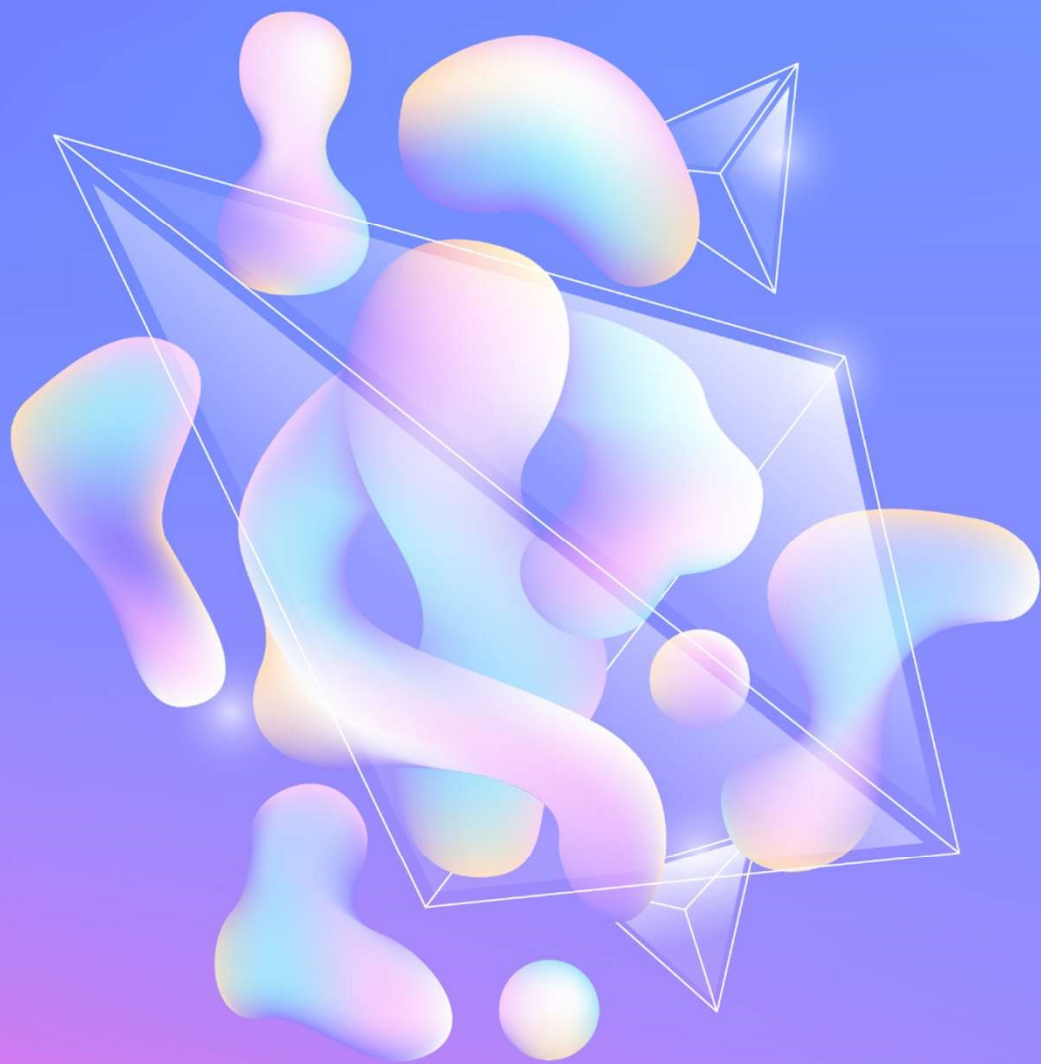
資安威脅趨勢分析

- 根據統計2024年，最常遭利用之弱點包含以下4則，其中有3則在攻擊當下屬於zero-day漏洞，且攻擊目標均為網路邊界設備(edge-device)



- 而綜合各項取得情資可知，網路邊界設備弱點之開採利用依舊為現今攻擊趨勢

Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457)



02

資訊安全與你我的關係



於公



於私



身份盜用風險

當個人資料遭到洩露，竊犯可能冒用身份申請信用卡、貸款或進行其他金融交易，導致信用評分受損

財產損失威脅

網路犯罪可直接導致財務損失，例如銀行存款被盜、信用卡盜刷，或是被勒索軟體要求贖金

隱私侵害問題

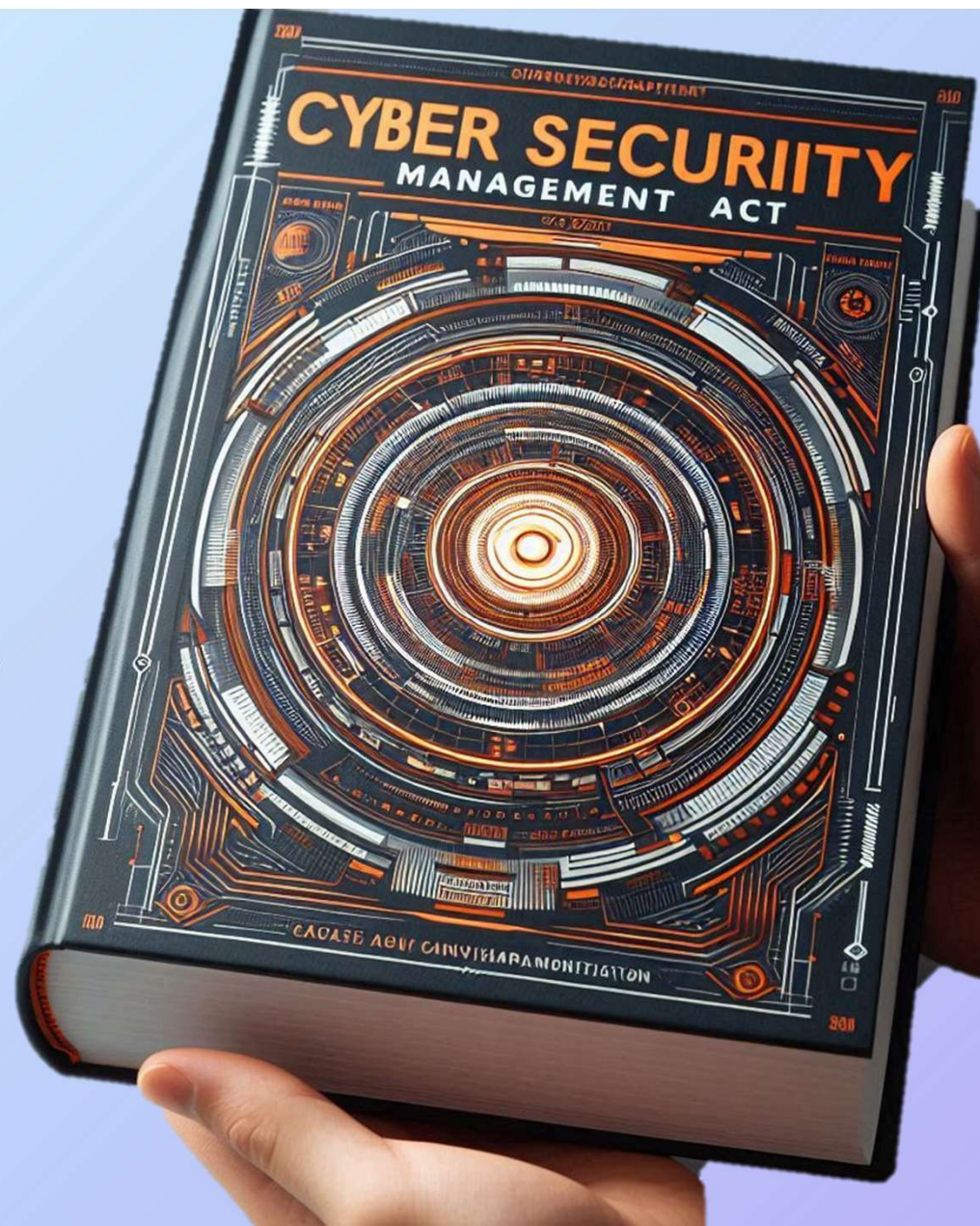
個人照片、資料或敏感資訊被洩露，可能造成聲譽受損，
或衍生勒索或騷擾事件

於公



資通安全管理法

實施日：108.01.01





數位發展部資通安全署

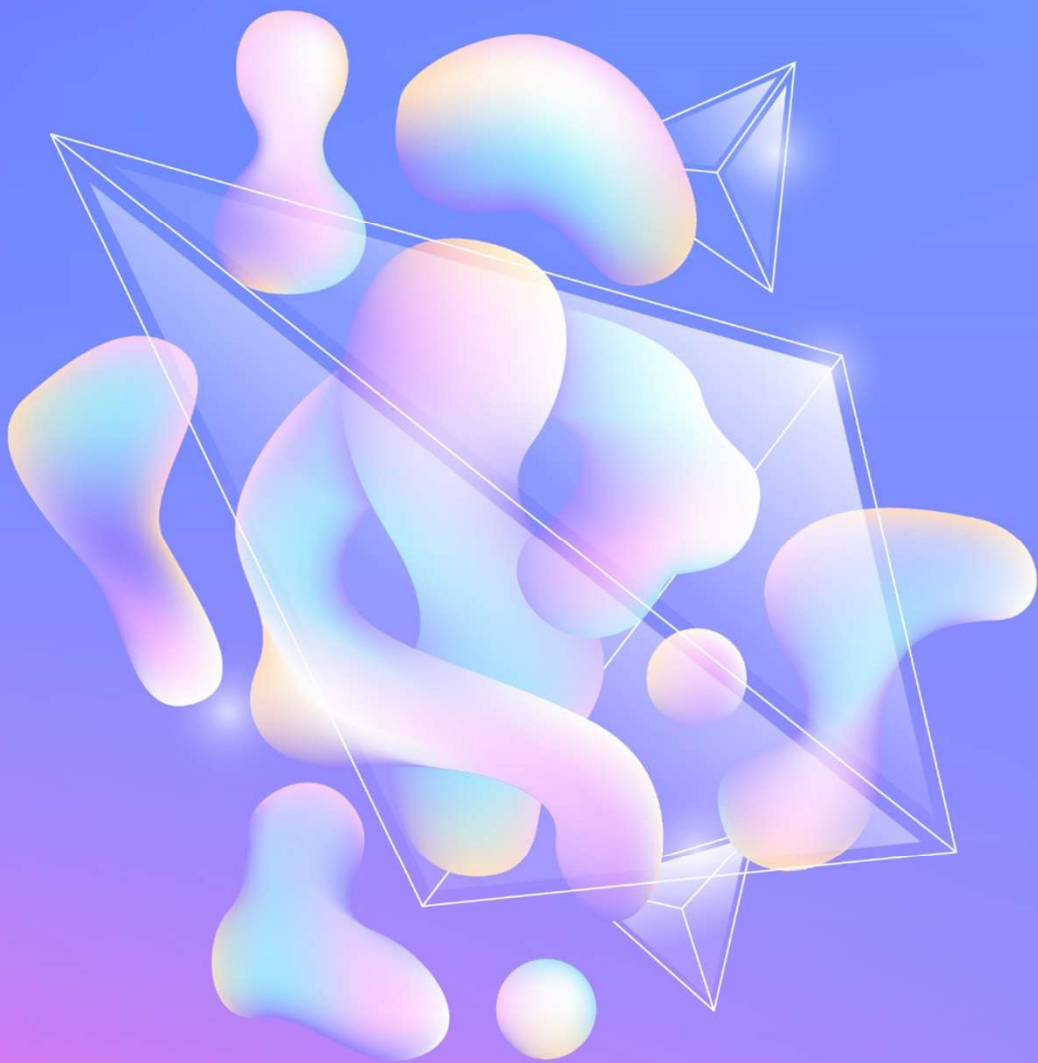
Administration for Cyber Security, moda

資安是 持續精進的風險管理

資通安全責任等級分級辦法

附表1~8 - 應辦事項 - 認知與訓練

辦理事項	辦理內容	A	B	C	D	E
資通安全教育訓練	資通安全專職人員 每人每年至少接受 1 2 小時以上之 資通安全專業課程訓練或職能訓練	至少 4 人	至少 2 人	至少 1 人	X	X
	資通安全專職人員以外之資訊人員	每人每二年至少接受 3 小時以上之資 通安全專業課程訓練且每年 3 小時以 上資通安全通識教育訓練			X	X
	一般使用者及主管	每人每年 3 小時以上 資通安全通識教育訓練				
資通安全專業證 照及職能訓練證 書	資通安全專職人員分別各自持有證 照及證書各一張以上，並持續維持 證照及證書之有效性。	至少 4 人	至少 2 人	至少 1 人 (僅證照)	X	X



03

社交工程破解術



iThome資安大調查-資安風險

2024年



- 社交工程
 - 資通安全事件通報及應變辦法
 - 第八條
- 勒索軟體資安事件
 - 責任等級分級辦法
 - 管理面
 - 備份程序
 - 技術面
 - 邊界防護→防火牆
 - 認知及訓練面
 - 資通安全事件通報及應變辦法

社交工程

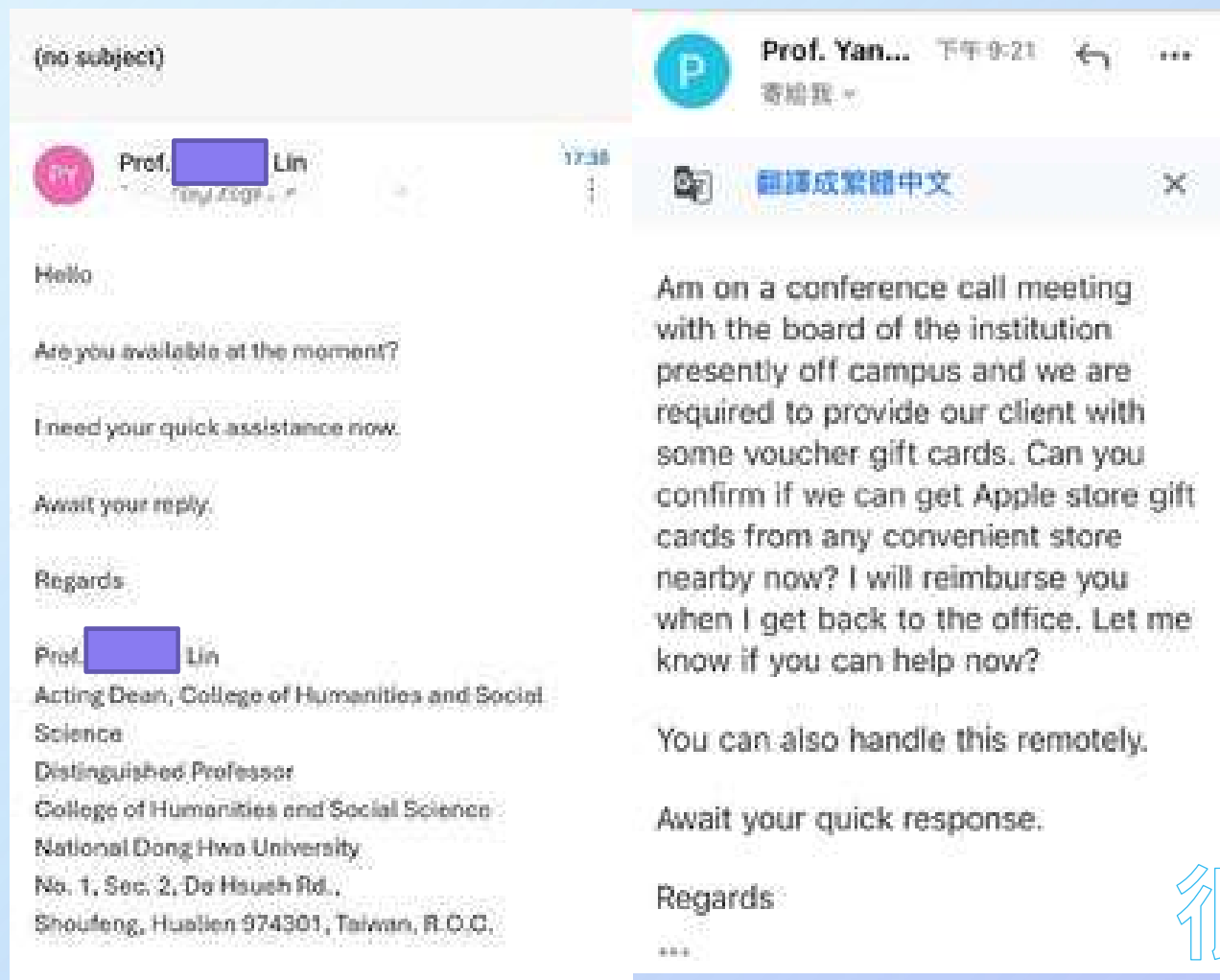


社交工程



通過心理操縱、人際互動、或其他非技術手段來獲取機密信息或達成其他目標的技術。這通常涉及欺騙或利用人的信任、好奇心、恐懼等情感，以獲取他們的敏感數據，如密碼、銀行賬戶信息等。

學校職員被社交工程信騙了～～



- 學校的職員收到老師的郵件，老師表示在外參加研討會要送給與會的對方蘋果商店禮物卡，請夥伴幫忙採購.....

- 來自外部的郵件(icloud)
- 全英文的內容
- 寄件者是學校老師
(都是很容易取得的資訊)

很老套，但是有效

Netflix遭詐團冒用發送釣魚郵件

[world journal](#)



Netflix全球上億的訂閱用戶成為詐騙集團目標，假冒Netflix官方發出的釣魚郵件近日在網路大量發送，謊稱帳戶因付款問題而暫時不能使用。

紐約郵報（New York Post）報導，這封假冒Netflix的郵件在周末大量發送，主旨是「處理你的付款問題」（let's tackle your payment details），信件內容通知用戶帳號被鎖住，因為上面的帳單資訊有問題必須更新付款資訊才能解鎖，郵件下方有個看起來和Netflix的紅色一樣的紅色按鈕，上面寫「立刻更新帳戶」，再下方還有連結到官方反應問題頁面的連結。

用戶一旦按下按鈕，就會被重新引導至一個很像Netflix的登入頁面，要求填上用戶名稱、密碼、地址和信用卡資訊，不法之徒只要這些資訊就能竊取輸入者的錢。

網路資安公司ESET全球網路安全顧問摩爾（Jake Moore）說，AI科技讓詐騙集團可以更快速、更大量地向更多人發送釣魚郵件，他們製作以假亂真的登入網頁，再用「立刻」、「被凍結」、「被鎖住」等字眼營造出急迫感，使人慌亂並誤信，不驗證來源或再想一想而是趕快輸入個資和帳戶或信用卡資訊，摩爾說，有幾個方法可以避免自己成為詐騙集團的肥羊。首先是檢查寄件人的郵件地址，Netflix寄出的信件會是以「netflix.com」，但詐騙集團的是iCloud 郵件。

應注意而未注意

1. 檢查寄件人的電子郵件地址

2. 檢查有沒有憑證

3. 檢查郵件內容

4. 不依靠連結，手動輸入

5. 開啟附加檔案前，再想想

<http://ctbc-bonk.com>

【中國信託】你的網路銀行更新失敗，請立即輸入你的驗證碼以更新資料，超時請重新輸入。
<http://ctbc-bonk.com/>



<https://www.ctbcbank.com>

應注意而未注意

1. 檢查寄件人的電子郵件地址

2. 檢查有沒有憑證

3. 檢查郵件內容

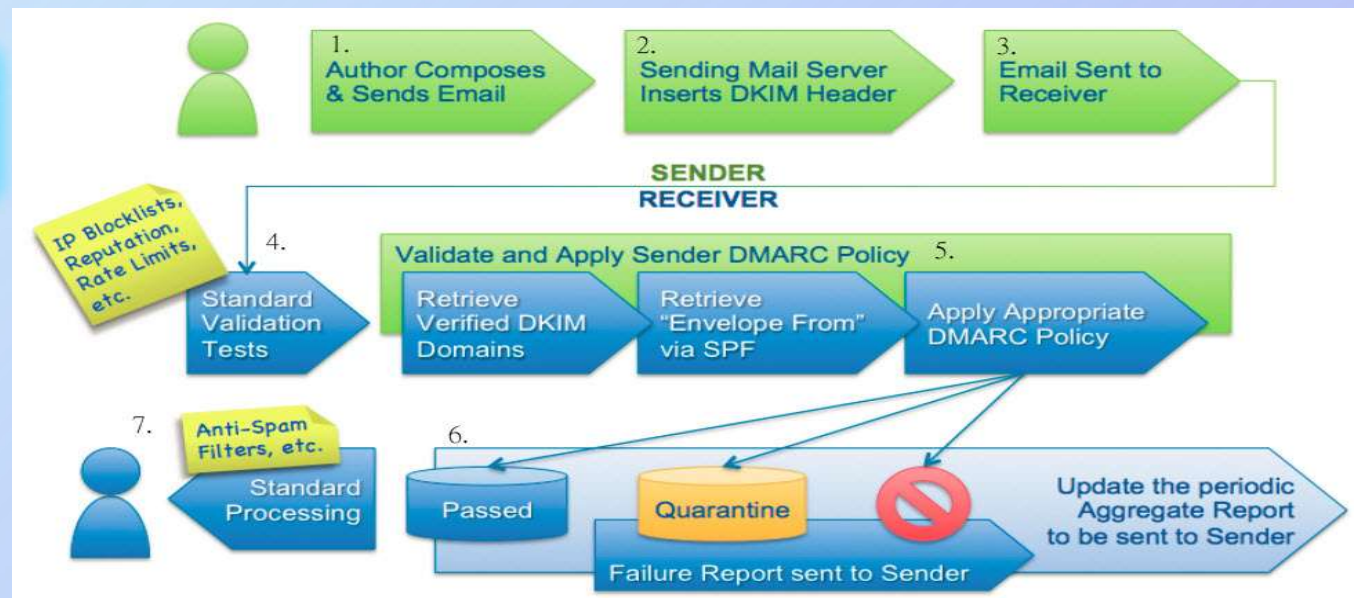
4. 不依靠連結，手動輸入

5. 開啟附加檔案前，再想想

寫信

郵件主機在
Header中加入
DKIM簽章資訊

寄出郵件



Anti-SPAM判斷流程
(IP、RBL)

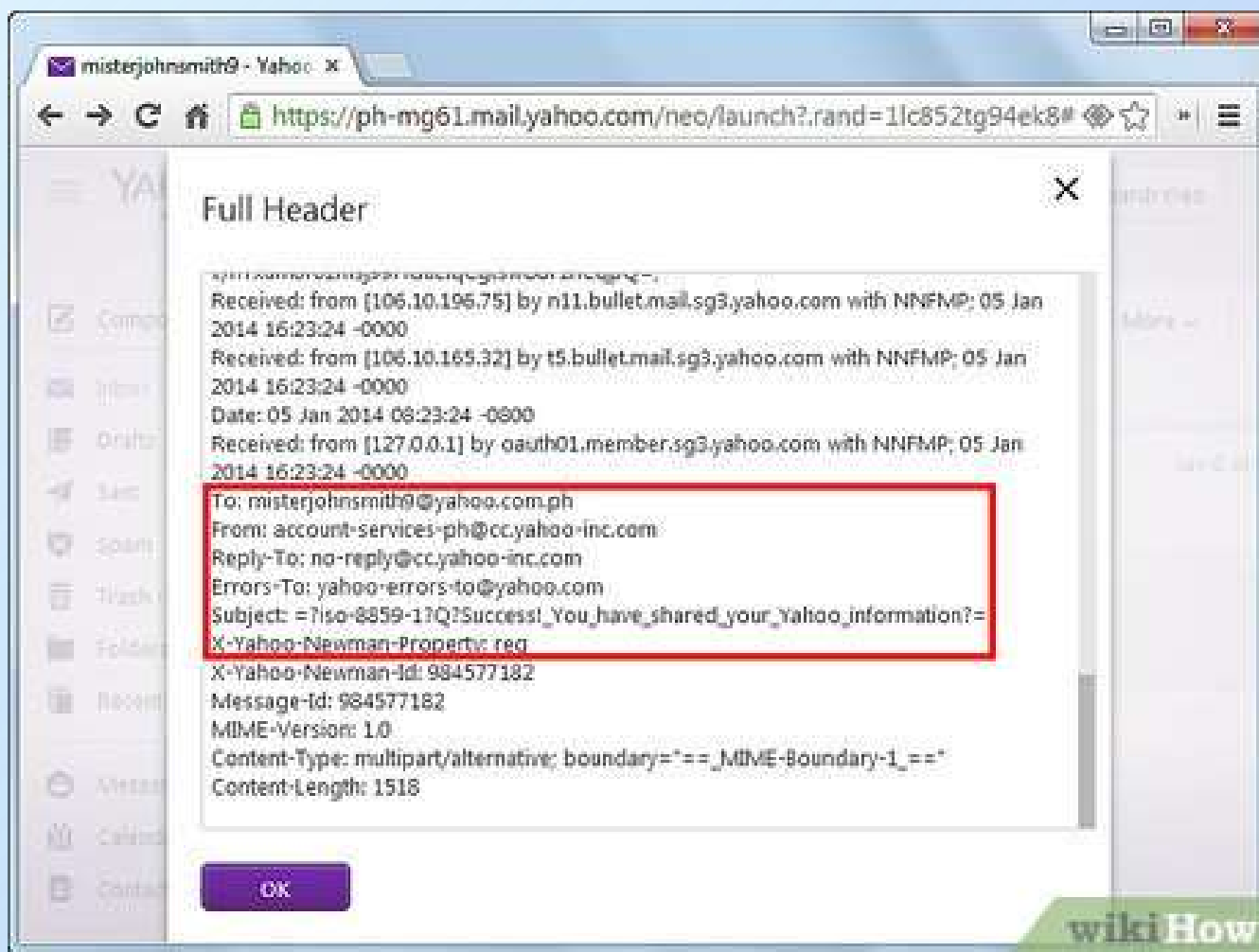
透過DKIM、SPF驗證

結果：三種
none (PASS)、
Quarantine(SPAM)、
REJECT

林志玲



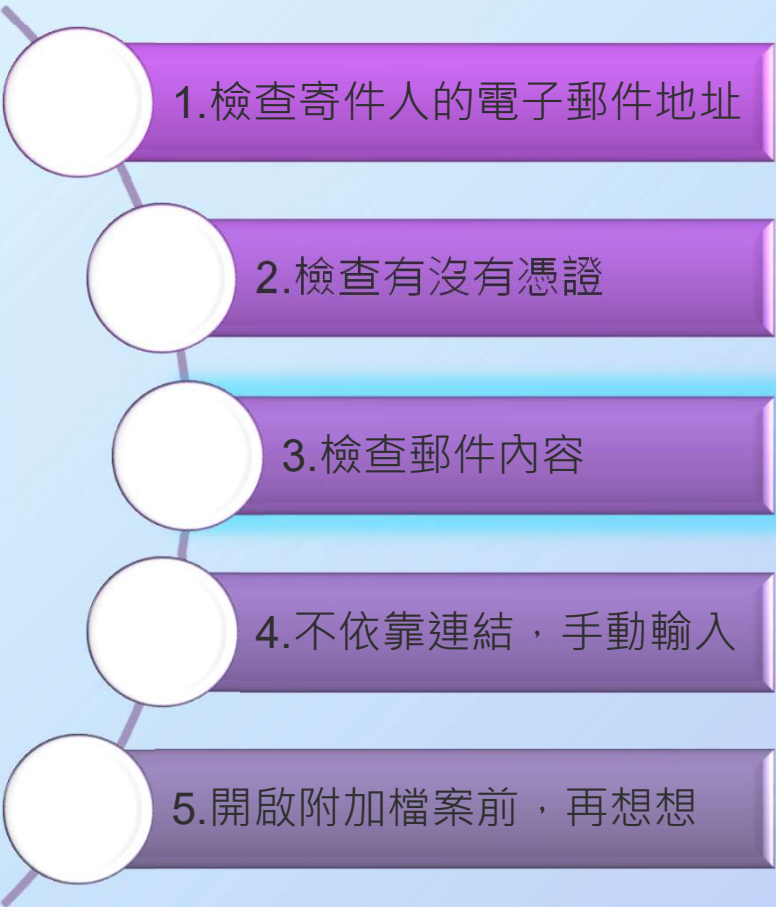
Mail Header



Mail Header 是信件的真實身分證，記錄寄件來源、經過路徑等資訊。

有時候信件看起來像是某人寄的，但其實很容易偽造，要從header查看真相。

應注意而未注意



1. 檢查寄件人的電子郵件地址

2. 檢查有沒有憑證

3. 檢查郵件內容

4. 不依靠連結，手動輸入

5. 開啟附加檔案前，再想想

- 因為AI的出現，製作社交工程信件變得比較輕鬆，但是仔細地看看內容，你還是可以發現有些不自然的地方，譬如措辭、語氣、常用語、語法錯誤、翻譯等現象。
- 例如：
 - 我說「簡訊」，它寫「訊息」
 - 我說「電腦」，它寫「計算機」
 - 我說「印表機」，它寫「打印機」
 - 我說「資料庫」，它寫「數據庫」



詐騙簡訊提醒

遠傳電信溫馨提示

親愛的用戶您好，截止 2023 年 3 月 25 日您的遠傳幣餘額：5559，將於三個工作日內到期，為避免影響，請及時兌換獎賞。

<https://www.fetnete.cn>
請回復 1 激活鏈接領取

中華電信：會員回饋提示，您的
賬戶 5340 積分將於今日內到期，逾期將作廢，請及時兌換獎品：
<http://www.chtcom-vip.com>
請回復 1 激活鏈接領取

請蘋果用戶請儘速升級為 iOS 16.2 以上版本
避免收到 iMessage 詐騙訊息



whoscall X 165 防詐快報

本週高風險簡訊

小心！物流業者遭偽冒



上午 1:23

通知：您的國際包裹長期無人認領，請
支付運費並確認是否重發：
cutt.ly/jNLrBHF 退訂回復【T】

DHL：由于收货地址不正确，您的包裹无法送达。请填写以下表格以输入新地址：
<https://mydelivery-express.com/>

台灣中華郵政：由于额外费用，您最近的
订单的交付已延迟，请查看以下内容：
<https://chunghwa-post.info>

注意

包裹
詐騙簡訊
持續出沒！

切勿點擊
可疑連結



應注意而未注意

1. 檢查寄件人的電子郵件地址

2. 檢查有沒有憑證

3. 檢查郵件內容

4. 不依靠連結，手動輸入

5. 開啟附加檔案前，再想想

- 社交工程郵件常常會有惡意連結，帶你去錯誤的地方。

使用者，可以將游標懸停在連結上（不要點擊），查看實際網址是否跟你想像中的相同



應注意而未注意

1. 檢查寄件人的電子郵件地址

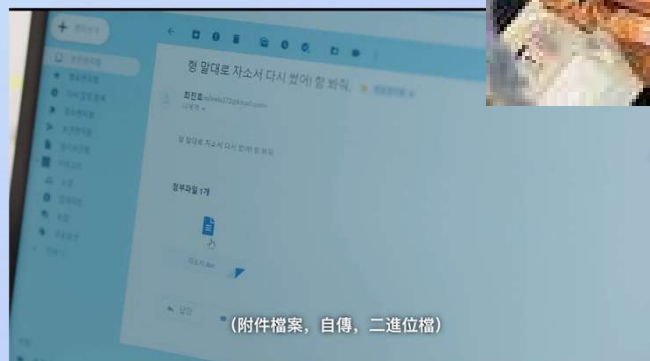
2. 檢查有沒有憑證

3. 檢查郵件內容

4. 不依靠連結，手動輸入

5. 開啟附加檔案前，再想想

- 詐騙郵件會夾帶 .zip、.exe、.pdf、.docx 等附件，當你開啟時，可能會自動執行惡意軟體，導致病毒感染、系統漏洞被利用，甚至觸發勒索攻擊



推薦的
解決方案



CISA提供阻絕釣魚的三步驟



BLOCK The BAIT 阻擋誘餌

- 辨識郵件來源
- 透過資安設備阻擋
- 避免出現URL

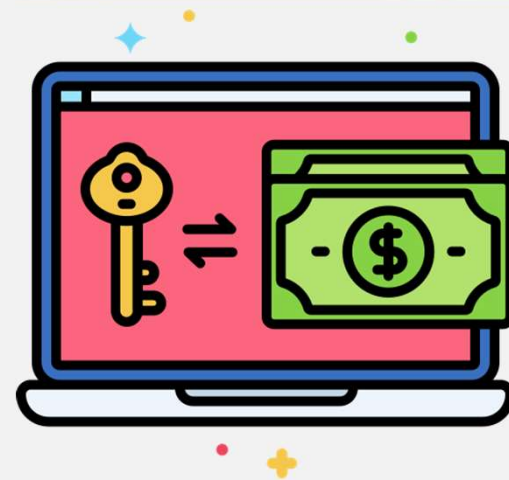
DON'T TAKE THE BAIT 不被誘騙

- 加強識別能力
- 不同管道的網路釣魚

REPORT THE HOOK 回報釣魚事件

- 教育處置方式
- 不要轉寄惡意郵件
- 防範入侵範圍擴大

勒索軟體



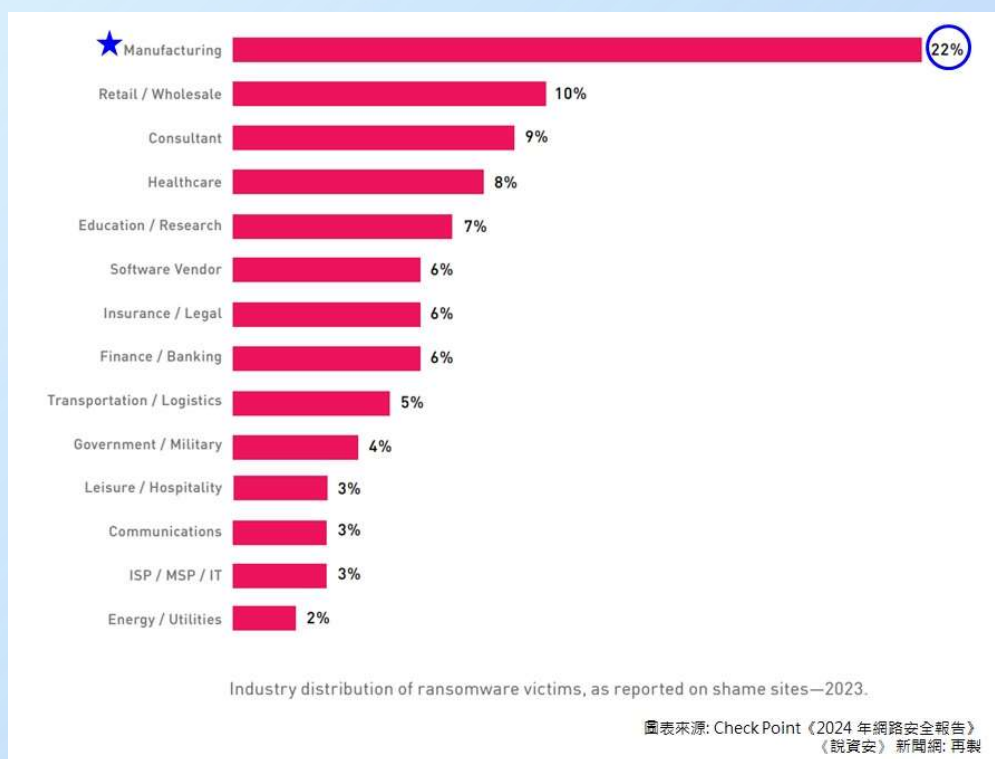
勒索軟體

勒索軟體為一種透過加密、阻擋封鎖使用者存取檔案、應用程式或系統的惡意軟體，透過以上方式來勒索受害者支付贖金以重獲權限或檔案，否則可能永遠失去存取權限。



Check Point 2024 年網路安全報告

勒索軟體攻擊統計



1. 製造業
2. 零售業
3. 顧問業
4. 健康產業
5. 教育、研究
6. 軟體供應廠商
7. 保險業
8. 金融、銀行
9. 交通運輸
10. 政府、國防

Coveware調查，勒索軟體主要的入侵管道

遠端桌面

網路釣魚

漏洞利用



常被利用的CVE漏洞

資訊來源：Tenable、Help Net Security、BleepingComputer

CVE-2024-49138

- Windows Common Log File System (CLFS) 權限提升漏洞

CVE-2024-43491

- Windows Update 遠端程式碼執行漏洞

CVE-2024-38080

- Windows Hyper-V 權限提升漏洞

CVE-2024-38112

- Windows MSHTML 平台偽造漏洞

CVE-2024-30051

- Windows DWM Core Library 權限提升漏洞

CVE-2024-30040

- Windows MSHTML 安全功能繞過漏洞

CVE-2024-43451

- Microsoft Exchange Server 權限提升漏洞

CVE-2024-49039

- Windows Kernel 權限提升漏洞

CVE-2024-38094

- Microsoft SharePoint 遠端程式碼執行漏洞

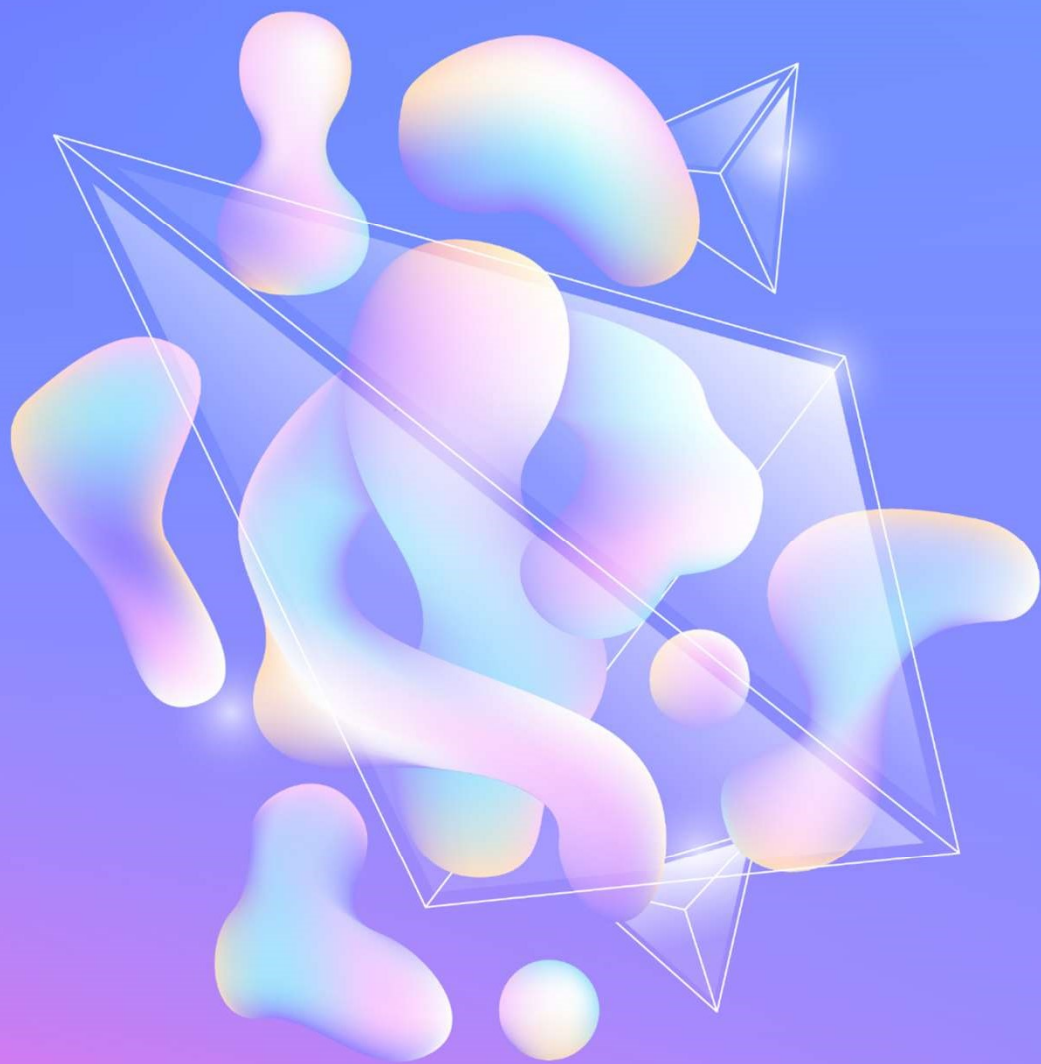
以上是 2024 年被廣泛利用的 Microsoft 漏洞，涵蓋 Windows、Hyper-V、SharePoint 等產品

推薦的
解決方案





- 注意系統重大更新
- 注意防毒軟體更新



04

帳號密碼與身份驗證安全



介紹撞庫攻擊

Hi, I'm
John Huang.



Johnh@gmail.com



Johnh@outlook.com



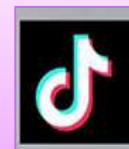
Johnh@yahoo.com



Johnh



Johnh



Johnh



Johnh

Johnh



駭客攻破了某個網站

看到了

- 帳號名稱：Johnh
- 聯絡郵件：Johnh@gmail.com



Hive Systems公布2024年密碼破解時間表

總部位於美國維吉尼亞州的資訊科技公司 Hive Systems 最新評估，駭客短短 37 秒就能暴力破解簡單的八字元密碼，攻克 16 字元密碼則可耗費上百年。

Hive Systems公布2024年密碼破解時間表，詳列駭客破解不同組合密碼所需的時間。這份表格每年都會更新。

許多網站目前要求至少八字元密碼，須含字母、數字或符號；但專家說，這要求可能要升級，因更長密碼代表排列組合更多，駭客就必須花更多時間去猜。

只有數字的簡單八字元密碼，只要37秒就能「暴力」破解，即嘗試盡可能多組合反覆試驗。若設定只有數字16字元密碼，需119年才能試出正確答案。

專家提倡更長密碼，即使相對簡單也可以。

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years



> Hardware: 12 x RTX 4090 | Password hash: bcrypt

強化密碼管理



密碼強度判斷標準

密碼長度至少12位元；包含大小寫字母、數字和符號；避免使用個人資訊、字典單字或常見詞彙。



密碼管理工具

密碼管理工具可以安全儲存及自動填寫密碼；部分工具提供密碼強度評估功能；選擇信譽良好的密碼管理工具。



定期更換密碼

定期更換密碼可以降低帳戶被盜用的風險；避免所有帳戶使用相同密碼；切勿在多個網站重複使用相同密碼。



05

資料處理與外洩風險



昇銳電子涉進口中國監視器 貼標MIT流入企業及政府

到以下平台觀看： YouTube



發布時間：2025/3/21 12:31 更新時間：2025/3/21 20:33

陳冠勳 陳弘屹 / 綜合報導

結論先講

國內安控大廠昇銳電子從2009年起，涉嫌從中國進口監視器主機等零件，在台重新組裝、貼上台灣製造標籤出售，經檢調追查更發現，相關主機有回連中國雲端服務伺服器，公司董事長經訊問後昨（20）日以100萬交保。而昇銳電子發重訊指出，全力配合檢調調查，對公司財務業務無影響。

調查官登門查扣大批貨物，相關監視設備本來出貨在即，如今都被扣下。查封的安控產品標榜國產，但檢調發現業者涉嫌購入中國零件在台組裝、重新貼牌，把商品搖身一變成為MIT。

調查局資安工作站副主任林惠賢說明，「經統計，該公司自中國進口監視器主機相關設備逾美金1億元，相關中國製產品已大量流入我國境內。」

涉嫌洗產地的安控大廠就是上櫃公司昇銳電子，從錄影系統、門禁設備全部一手包辦，但小至線材、外殼，大到主機板都被查出來自中國，更早從2009年就已開始進口的相關設備，折合台幣高達33億。

昇銳電子發重訊指出，全力配合調查，對公司財務業務沒影響。董事長與副董事長經檢方訊問，各獲100萬與30萬交保，但違法的10多年來銷往私人企業外，連政府機關都有採購。

2025/03/21

國內安控大廠昇銳電子從2009年起，涉嫌從中國進口監視器主機等零件，在台重新組裝、貼上台灣製造標籤出售，經檢調追查更發現，**相關主機有回連中國雲端服務伺服器**，公司董事長經訊問後昨（20）日以100萬交保。而昇銳電子發重訊指出，全力配合檢調調查，對公司財務業務無影響。

- <https://news.pts.org.tw/article/743238>

資通安全責任等級分級辦法 第11條....

各機關應依其資通安全責任等級，辦理附表一至附表八之事項。

各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。

各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；查後，免執行該事項或控制措施；其為主管機關者，經其為主管機關者，經其同意後，免予執行其同意後，免予執行。

資通安全責任等級分級辦法 附表一覽

- 附表一 資通安全責任等級A級之公務機關應辦事項
- 附表二 資通安全責任等級A級之特定非公務機關應辦事項
- 附表三 資通安全責任等級B級之公務機關應辦事項
- 附表四 資通安全責任等級B級之特定非公務機關應辦事項
- 附表五 資通安全責任等級C級之公務機關應辦事項
- 附表六 資通安全責任等級C級之特定非公務機關應辦事項
- 附表七 資通安全責任等級D級之各機關應辦事項
- 附表八 資通安全責任等級E級之各機關應辦事項
- 附表九 資通系統防護需求分級原則
- 附表十 資通系統防護基準執行控制措施

資通安全責任等級分級辦法

附表1~8 - 應辦事項 - 管理面

辦理事項	辦理內容	A	B	C	D	E
針對自行或委外開發之資通系統	依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性	1 年內	1 年內	1 年內	X	X
	完成附表十之控制措施（防護基準）	1 年內	1 年內	2 年內	X	X
資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入資訊安全管理系統，完成第三方驗證，並持續維持其驗證之有效性	2 年內	2 年內	2 年內 (導入)	X	X
資通安全專責人力		4 人 專職	2 人 專職	1 人 專職	X	X
辦理內部資通安全稽核		1 年 2 次	每年 1 次	2 年 1 次	X	X
業務持續運作演練	全部核心資通系統	每年 1 次	2 年 1 次	2 年 1 次	X	X
資安治理成熟度評估 (公務機關)		每年 1 次	每年 1 次	X	X	X

資通安全責任等級分級辦法

附表1~8 - 應辦事項 - 技術面(1/3)

辦理事項	辦理內容	A	B	C	D	E
安全性檢測	全部核心資通訊系統弱點掃描	每年 2 次	每年 1 次	2 年 1 次	X	X
	全部核心資通訊系統滲透測試	每年 1 次	2 年 1 次	2 年 1 次	X	X
資通安全檢診	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器及防火牆連線設定檢視	每年 1 次	2 年 1 次	2 年 1 次	X	X
政府組態基準 (公務機關)	依主管機關公告之項目，完成政府組態基準導入作業，並持續維運	1 年內	1 年內	X	X	X

資通安全責任等級分級辦法

附表1~8 - 應辦事項 - 技術面(2/3)

辦理事項	辦理內容	A	B	C	D	E
資通安全威脅偵測管理機制	依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄	1 年內	1 年內	X	X	X
資通安全弱點通報機制(VANS)	應於修正施行(110.08.23)後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。	1 年內	1 年內	2 年內	X	X
端點偵測及應變機制	(公務機關)依主管機關指定之方式提交偵測資料	2 年內	2 年內	X	X	X

資通安全責任等級分級辦法

附表1~8 - 應辦事項 - 技術面(3/3)

辦理事項	辦理內容	A	B	C	D	E
資通安全防護 防護措施之啟用 並持續使用之及 適時進行軟硬體 之必要更新或升 級	防毒軟體	1 年內	1 年內	1 年內	1 年內	X
	網路防火牆	1 年內	1 年內	1 年內	1 年內	X
	具電子郵件伺服器者，應備電子郵件過 濾機制	1 年內	1 年內	1 年內	X	X
	入侵偵測及防禦機制	1 年內	1 年內	X	X	X
	具對外服務之核心資通系統者，應備應 用程式防火牆	1 年內	1 年內	X	X	X
	進階持續性威脅攻擊防禦措施	1 年內	X	X	X	X

資通安全責任等級分級辦法

附表1~8 - 應辦事項 - 認知與訓練

辦理事項	辦理內容	A	B	C	D	E
資通安全教育訓練	資通安全專職人員 每人每年至少接受 1 2 小時以上之 資通安全專業課程訓練或職能訓練	至少 4 人	至少 2 人	至少 1 人	X	X
	資通安全專職人員以外之資訊人員	每人每二年至少接受 3 小時以上之資 通安全專業課程訓練且每年 3 小時以 上資通安全通識教育訓練			X	X
	一般使用者及主管	每人每年 3 小時以上 資通安全通識教育訓練				
資通安全專業證 照及職能訓練證 書	資通安全專職人員分別各自持有證 照及證書各一張以上，並持續維持 證照及證書之有效性。	至少 4 人	至少 2 人	至少 1 人 (僅證照)	X	X

資通安全責任等級分級辦法

附表9 - 資通系統防護需求分級原則(1/2)

		機密性 <u>未經授權之資訊揭露</u>	完整性 <u>資訊錯誤或遭竄改</u>	可用性 <u>資訊、資通系統之存取或使用之中斷</u>
對機關 營運、資產或信譽 等方面	有限影響	普	普	普
	嚴重影響	中	中	中
	非常嚴重 或 災難性影響	高	高	高

資通安全責任等級分級辦法

附表9 - 資通系統防護需求分級原則(2/2)

		法律遵循性
資通系統設置或運作於法令有相關規範之情形	普	
如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性	中	使機關或其所屬人員受行政罰、懲戒或懲處。
	高	使機關所屬人員負刑事責任

資通安全責任等級分級辦法

附表10 - 資通系統防護基準(1/2)

存取控制			事件日誌與可歸責性							營運 持續 計畫		識別與鑑別				
帳號 管理	最小 權限	遠端 存取	記錄 事件	日誌 記錄 內容	日誌 儲存 容量	日誌 處理 失效	時戳 及校 時	日誌 資訊 之保 護	系統 備份	系統 備援	內部 使用者之 識別與鑑 別	身分 驗證 管理	鑑別 資訊 回饋	加密 模組 鑑別	非內 部使 用者 之識 別與 鑑別	

資通安全責任等級分級辦法

附表10 - 資通系統防護基準(2/2)

系統與服務獲得

系統與
通訊保
護

系統與資訊
完整性

系統發展生命週期需求階段

系統發展生命週期設計階段

系統發展生命週期開發階段

系統發展生命週期測試階段

系統發展生命週期部署與維護階段

系統發展生命週期委外階段

獲得程序

系統文件

傳輸之機密性與完整性

資料儲存之安全

漏洞修補

資通系統監控

軟體及資訊完整性

資通安全責任等級分級辦法

附表10 - 資通系統防護基準 - 存取控制

控制措施	系統防護需求分級			項目	
帳號管理	高	中	普	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序	
			已逾期之臨時或緊急帳號應刪除或禁用		
			資通系統閒置帳號應禁用		
			定期審核資通系統帳號之申請、建立、修改、啟用、停 用及刪除		
		機關應定義各系統之閒置時間或可使用期限與資通系統之使用況及條件			
		逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出			
		應依機關規定之情況及條件，使用資通系統			
		監控資通系統帳號，如發現帳號違常使用時回報管理者			
最小權限	高	中	普	無要求	
			採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取		
遠端存取	高	中	普	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化	
				使用者之權限檢查作業應於伺服器端完成	
				應監控遠端存取機關內部網段或資通系統後臺之連線	
				應採用加密機制	
		遠端存取之來源應為機關已預先定義及管理之存取控制點			

院臺護字第 1100165761 號

行政院資通安全處 函	
地址：10058 臺北市忠孝東路1段1號 聯絡人：侯奇仁 電子信箱：hsr@ey.gov.tw	
受文者：教育部	
發文日期：中華民國110年3月2日	
發文字號：院臺護字第1100165761號	
類別：普通件	
密等及解密條件或保密期限：	
附件：	
主旨：近期迭發生機關開放委外廠商自遠端進行資通系統維護致存取機制遭駭客利用，間接攻擊機關資通系統事件，為降低資安風險，請各機關加強遠端存取控制機制如說明，請查照並轉知所屬。	
說明：	
一、各機關開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，若機關因地域限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：	
(一)依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。	
(二)開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。	
(三)於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如 VPN)登入密碼。	
二、未依前述規定辦理遠端存取控制措施，致機關發生資安事	件，情節重大者，機關應依「公務機關所屬人員資通安全事項獎懲辦法」規定予以懲處。
正本：總統府第二局、國家安全會議秘書處、立法院資訊處、司法院資訊處、考試院資訊室、監察院綜合業務處、各部會行總處等、各直轄市政府、各縣市政府、各直轄市議會、各縣市議會、本院資訊處	
副本：[印章]	

第 1 頁，共 2 頁

110029358 發文日期:110/03/02

第 2 頁，共 2 頁

• 原則禁止、例外允許

– 審核機制(申請單)

– 開放原則

- 短天期
- 限定時間
- 限制來源
- 限制方式

– 記錄留存

- VPN
- 監控



遠端連線

- 如非必要，請避免
- 應有良好的對應作業
 - 管理作為
 - 申請制度
 - 限制開啟日程、時段
 - 限制來源位置
 - 限制連線設備
 - 技術作為
 - VPN
 - Proxy



院臺護長字第1090201804A號函

行政院秘書長 函

地址：10058臺北市忠孝東路1段1號
傳真：02-23973457
聯絡人：余柏賢02-3356500#8060
電子信箱：bsyu@ey.gov.tw

受文者：教育部

發文日期：中華民國109年12月18日
發文字號：院臺護長字第1090201804A號
類別：嚴密件
密等及解密條件或保密期限：
附件：

主旨：為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，請依說明事項辦理，請查照並轉知所屬公務機關。

說明：

- 一、依據本(109)年8月7日中央及地方政府資通安全長及資訊主管會議(下午場次)主席裁示事項第3項辦理。
- 二、為利旨揭事宜，爰重申各公務機關使用資通訊產品(含軟體、硬體及服務)相關原則：
 - (一)公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
 - (二)個人資通訊設備不得處理公務事務，亦不得與公務環境交接。
 - (三)各機關應就或使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境交接。
- 三、請各公務機關於110年底前完成汰換或使用或採購大陸廠牌資通訊產品(含硬體、軟體及服務)作業，並配合擴大盤點，其辦理方式如下：



(一)請各機關擴大盤點，並於110年1月4日至15日至本院國家資通安全會報資通安全作業管考系統(<https://spm.nat.gov.tw/>)「大陸廠牌資通訊產品」填報相關資料，並請直轄市及縣(市)政府協助轉知山地原住民區民代表會及鄉鎮市民代表會配合辦理。

(二)本次盤點範圍為全機關(非機關內部之資訊單位或特定單位)，其中「大陸廠牌認定方式」及「資通訊產品定義」，說明如下：

- 1、大陸廠牌認定方式：由填報機關「從嚴認定」，所有屬大陸廠牌者，無論其原產地於我國、大陸地區或第三地區等，渠等產品均須納入填報範圍。
- 2、資通訊產品定義：參考資通安全管理法第3條用詞定義，包含軟體、硬體及服務等項，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品，如無人機、網路攝影機、印表機等。
- 3、如各機關無法於期限內完成汰換作業或有窒礙難行之處，須填報正當理由，後續由本院協助評估其妥適性或其他可行作法。

四、本案相關諮詢窗口：

- (一)填報內容問題：余柏賢先生、02-3356-8060、bsyu@ey.gov.tw。
- (二)系統操作問題：柯旻圻先生、02-3356-8170、minchiko@ey.gov.tw。
- (三)帳號申請問題：劉桂琳小姐、02-6631-1890、smile@ncst.nat.gov.tw。

正本：總統府秘書長、國家安全會議秘書長、立法院秘書長、司法院秘書長、考試院秘書長、監察院秘書長、行政院資訊處、各部會行總處署、直轄市政府、各縣市政府、各直轄市議會、各縣市議會
副本：行政院國家資通安全會報技術服務中心



重點歸納

原則

- 一. 公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
- 二. 個人資通訊設備不得處理公務事務，亦不得與公務環境介接。
- 三. 各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

※ 管考系統「大陸廠牌資通訊產品」填報資料的盤點範圍為「全機關」

定義

- 大陸廠牌認定方式：由填報機關「從嚴認定」，所有屬大陸廠牌者，無論其原產地於我國、大陸地區或第三地區等，渠等產品均須納入填報範圍。
- 資通訊產品定義：參考資通安全管理法第3條用詞定，包含軟體、硬體及服務等項，另具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品，如無人機、網路攝影機、印表機等

常見問題

研究室中的無線分享器

- 學校佈署的無線分享器，總是會有些地理環境無法克服
- 有些角度，無線網路的訊號就是差了一點點

 <p>AC750 主流款 小資首選 Archer C24</p>	 <p>雙頻Wi-Fi MU-MIMO 支援 AGO Archer C54</p>	 <p>Archer MR4000</p>	 <p>300Mbps N 4G LTE 路由器 4G 行動寬頻網路 分享 中文APP設定</p>
【TP-Link】 Archer C24... NT\$1,399.00 momo購物網	【TP-Link】 Archer C54... NT\$1,799.00 momo購物網	【TP-Link】 Archer MR40... NT\$7,888.00 momo購物網	【TP-Link】 TL-MR100... NT\$4,888.00 momo購物網



體積雖小、威力十足
小米 WiFi 放大器 Pro(R03)

- 操作設定簡單
- 300Mbps電板
- 2x2外置天線

市售價 499 元 促銷價 **449** 元 直營通盤

品牌名稱：小米

結帳方式：信用卡 \ 無卡分期 \ 貨到付款 \ 刷momo卡消費回饋最高3%!

紅利折抵：共22家銀行

保固資訊：30天保固期

- 剛好，家裡有個閒置的分享器
- 剛好，小孩畢業帶回了一顆分享器

很重要 ~ 很重要 ~ 很重要 ~

- ◆ 只要你有連結上校園內的網路，都算是「機關內」
- ◆ 檢查的方式：查詢網通設備的身分證號碼(MAC 位置)
- ◆ 臺廠老字號品牌，看起來，相對安心點

MAC 位址介紹

3C:4D:5E:6F:7A:8B



- MAC 位置由12個十六進位數組成，通常被視為網路通訊設備的身分證號
- 在區域網路中作為「識別」的用途



ANA事件單通知：TACERT-ANA-2023053111053939

發佈編號：TACERT-ANA-2023053111053939

發佈時間：2023-05-31 11:17:39

事故類型：ANA-漏洞預警

發現時間：2023-05-31 11:08:39

影響等級：低

[主旨說明:]

【漏洞預警】ASUS RT-AC86U 存在漏洞 (CVE-2023-28703、CVE-2023-28702)

[內容說明:]

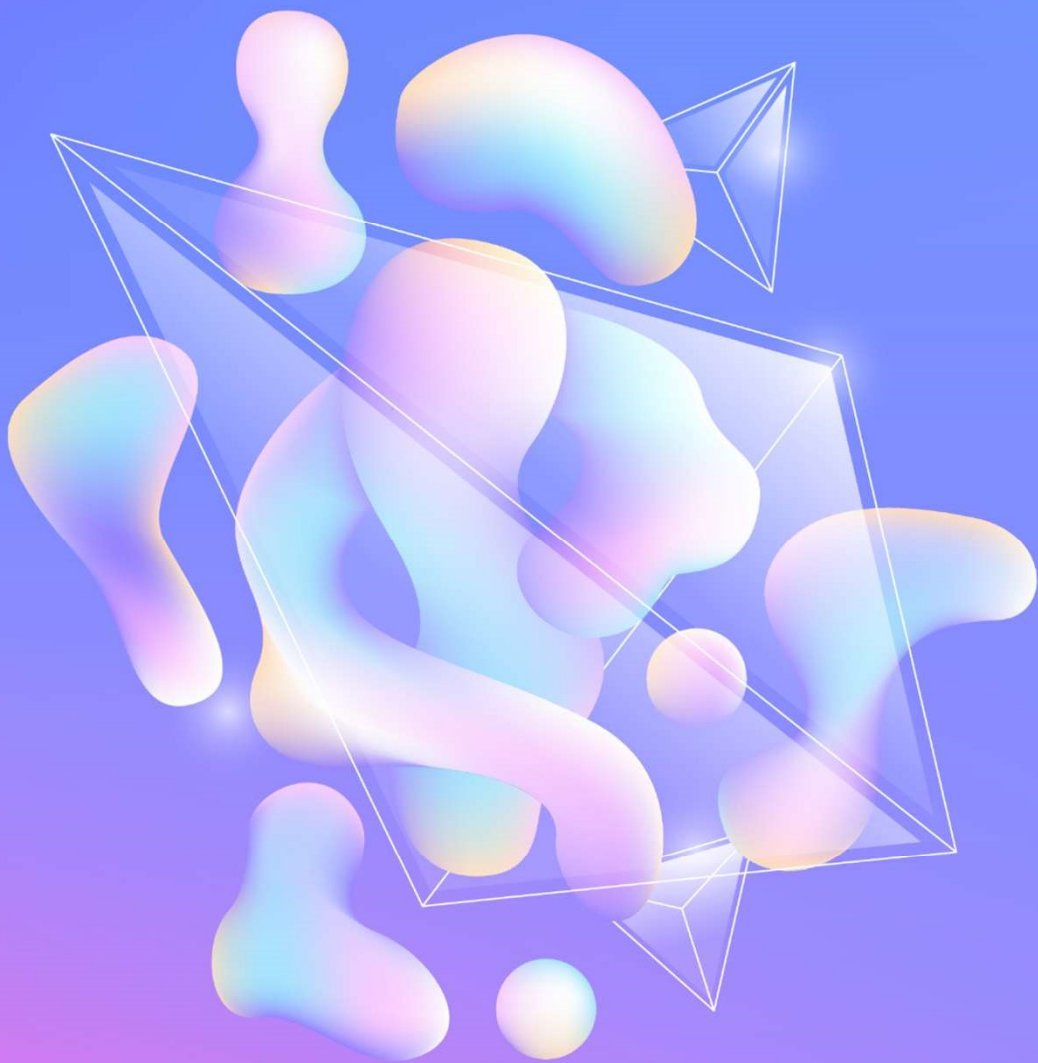
轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-ANA-202305-0005

ASUS RT-AC86U漏洞說明如下：

- CVE-2023-28703: ASUS RT-AC86U特定cgi功能未作長度驗證，導致Stack-based buffer overflow漏洞，遠端攻擊者以管理者權限登入後，即可利用此漏洞執行任意程式碼、任意系統操作或中斷服務。
- CVE-2023-28702:ASUS RT-AC86U未對特定功能網址之參數進行特殊字元過濾，遠端攻擊者以一般使用者權限登入後，即可利用此漏洞進行Command Injection攻擊，執行系統任意指令，並導致阻斷系統與終止服務。



[建議措施:]
將ASUS RT-AC86U
更新至最新版



06

常見的資安NG行為



Ethan 的 資訊安全旅程

Ethan's Information Security Journey



你好，我是Ethan

很榮幸可以加入OO公司這個大家庭，請各位前輩多多指教。



我是OO公司的業務人員，很高興能為您服務。

您如果要找我，建議撥打我的電話或SMS比較方便，我有時候需要外出開會，不會在辦公室。





Ethan總覺得，他正在寫報告、趕文件的時後，電腦就喜歡冒出「系統更新」的提示.....

好煩好煩好煩啊！

除了系統更新之外，電腦也會跳出另外另一個提醒，定期掃描。



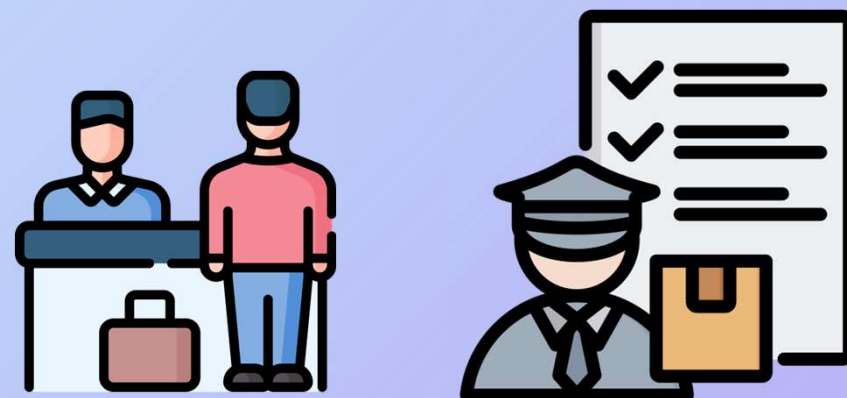


計程車上Ethan接到廠商OO小姐的電話

OO小姐：Ethan，報價單要麻煩你幫我做些調整

Ethans臉上帶有責任感地回應：我正在搭車，等下就到機場了，可以等我過完海關後找地方修改，再寄給你嗎？大約1小時左右，行嗎？

OO小姐：可以的，那就麻煩你囉！





你好，一杯Iced Americano

Ethan在機場咖啡廳連上公用 Wi-Fi，
熟練地打開筆電修改報價單並寄出

- ◆可是他沒有注意到，WIFI有好多個，
直接連結了訊號最強又剛好不用密碼
的WIFI
- ◆修改好的報價單，直接地放到郵件附
加檔案中，按下寄出按鍵

OO小姐，修改後的報價單已經寄送給
您了，再請您看看有沒有問題





客戶：Ethan，我剛剛寄了郵件給你，有些我想要問的參考，你幫我看看，再給我些資訊

Ethan開啟客戶的來信，點擊客戶給的連結看看商品的圖片，了解客戶的需要。

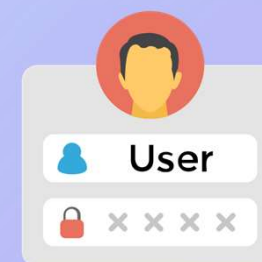




這天，電腦跳出提示，『密碼到期請變更』。

Ethan覺得心好累，因為公司電腦有螢幕保護程式，常常需要輸入密碼。

他的密碼長度不好輸入，電腦上Key-in就有點麻煩了，有時候用手機看信也要輸入，超級不方便，所以這次變更，他想了個辦法，把密碼改的簡單點





今天Ethan發現，他執行的搜尋作業，都要花好久的時間才有結果

而且，電腦時不時地跳出一些廣告視窗，工作的節奏被打亂外，效率也特別低



你發現了 伊森 的幾個NG行為

01

弱密碼

02

隨意點擊不明連結

03

忽略安全性更新

04

公用Wi-Fi

05

重要檔案未加密

06

不用純文字格式讀信

感謝出席

