

陌生隨身碟使用行為與風險認知之探討：

以中原大學為例

[第五組]

許至昀 | 鍾昀翰 | 趙永騫 | 黃乙家



- 索引 -

Introduction

前言 文獻探討

參考文獻

Methods

研究方法

AI 協作

Results

實驗與問卷結果

抄襲檢測

and

小組分工

Discussion

研究結論

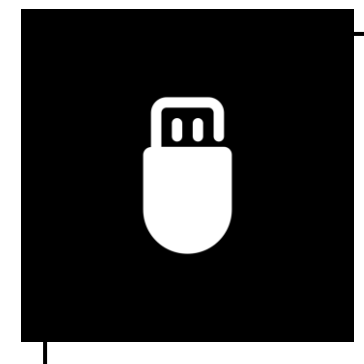
心得

前言



資通安全、社交工程威脅日益複雜且多樣化

據研究，98 % 陌生隨身碟被人撿起或移走
45 % 的隨身碟被插入電腦並開啟檔案



當今社會，真的是如此嗎？

文獻探討

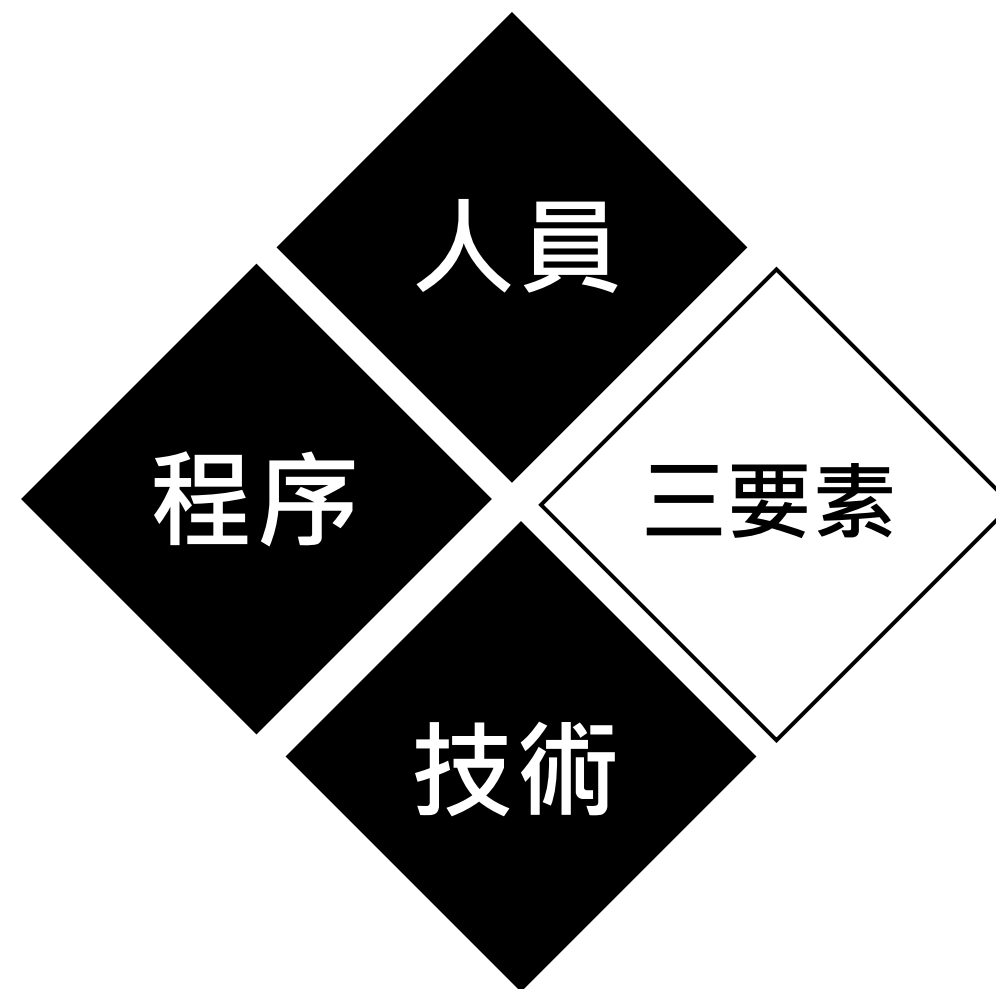
資通安全

《資通安全管理法》

第三條 第一款

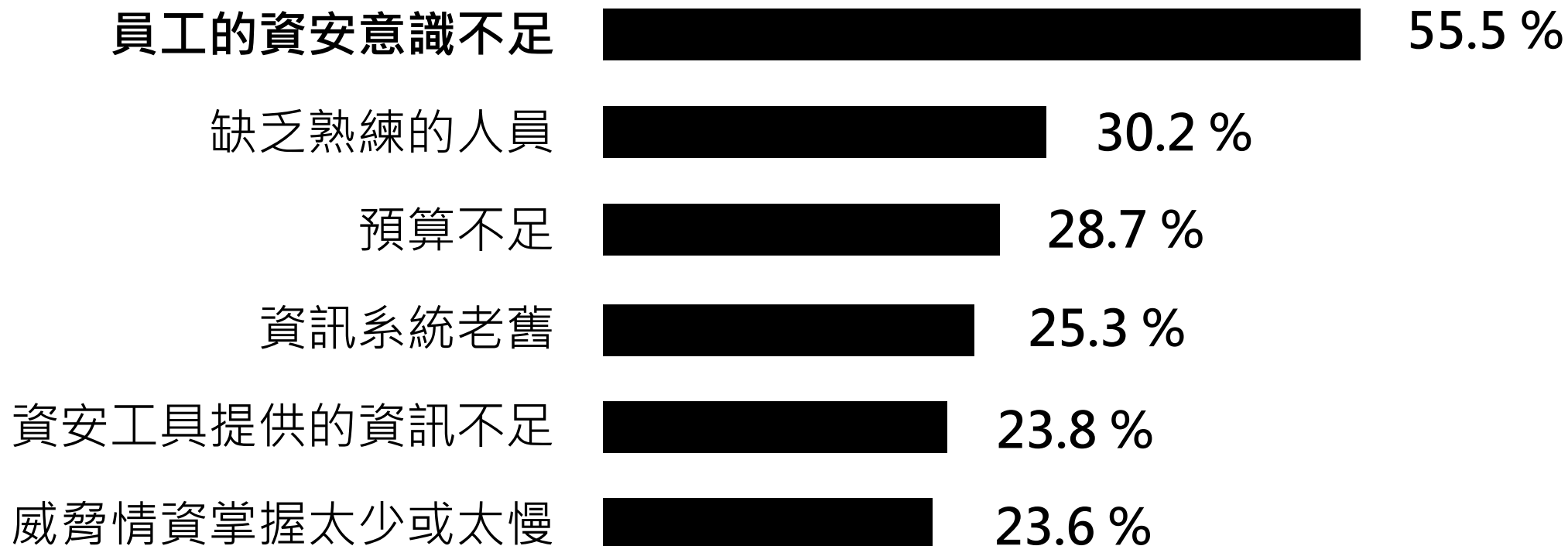
資通安全：

指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。



資通安全

2023 ~ 2024 最可能發生的十大資安風險 (iThome)



資通安全

為何企業難以抵抗資安攻擊（2023 資安弱點排名，iThome）



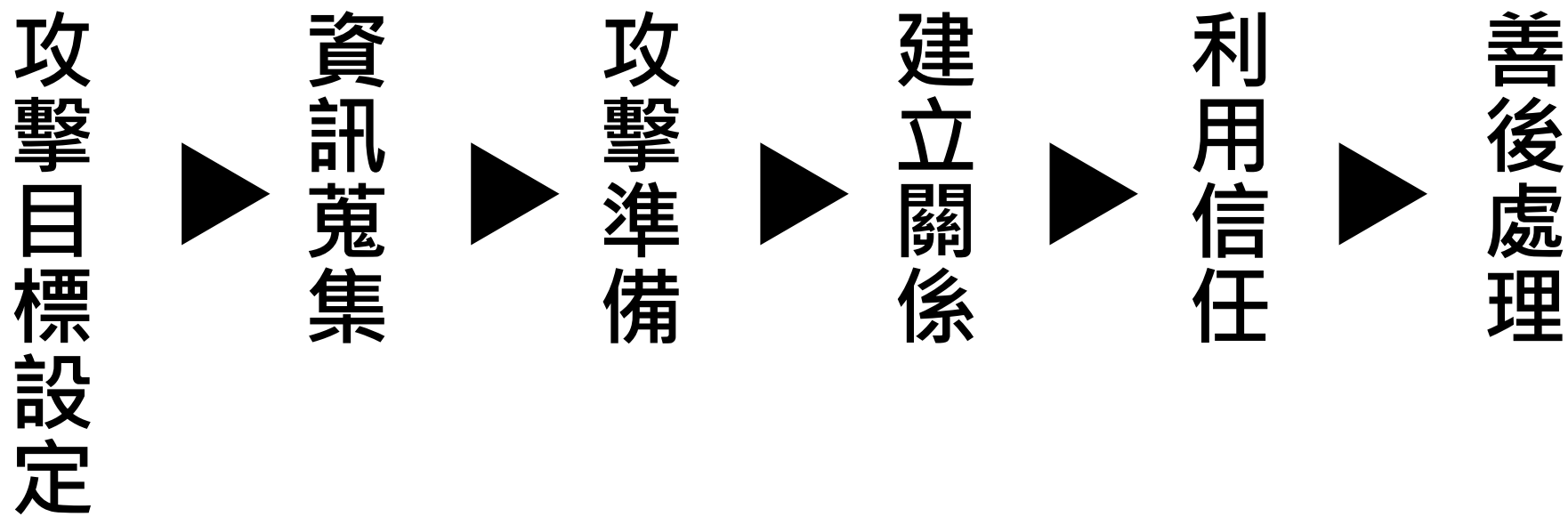
■ 社交工程

利用人際影響力或說服技巧來欺騙他人的手段
透過人們之間的社會互動來獲取或危害組織的系統資訊
從而展開攻擊行為

人員對於社交工程認知的不足

惡意人士不需要備頂尖的電腦專業技術

■ 社交工程攻擊



■ 不明連結被訪問研究

1

Zinaida Benenson 等人 (2014)

Facebook 和 電子郵件發送 看似來自「上週照片」的個人化連結

398 位受試者中，實際進行點擊行為有 179人 (39 %)

不明隨身碟被執行研究

1

Isaac Yaw Ferguson (2017)

6 個隨身碟中，有 3 個成功產生了連線，成功率 50 %

2

Matthew Tischer (2015)

297 個隨身碟， 290 個 (98 %) 被移動， 135 個 (45 %) 被開啟

從投放到開啟的時間平均為 6.9 小時，最快插入時間不到 6 分鐘

有 87.5 % 的隨身碟在當天就被撿起

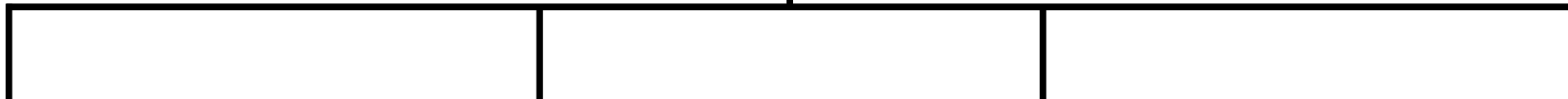
多數動機是想尋找失主 (68 %)，也有出於好奇 (18 %)

■ 資通安全素養

資通安全素養



資訊素養



傳統素養

媒體素養

電腦素養

網路素養

研究方法

■ 研究設計

社會實驗

於中原大學校園內多個地點隨機放置隨身碟

1

問卷調查

隨身碟中，放置連結檔案並嵌入問卷表單

2

實驗工具

夾鏈袋

防水、防塵

人為自然使用之意



檔案內容

「 Info_2025-05.pdf 」的 HTML 檔案

仿造一般文件，以及加上日期提供時事感

HTML 檔案可以跨平台、跨裝置使用

```
1  <!DOCTYPE html>
2  <html>
3      <head>
4          <meta charset="UTF-8">
5          <script>window.location.href = "https://cycu.site/ {隨身碟編號} ";</script>
6      </head>
7      <body>
8          <p>檔案預覽失敗，請點擊
9          <a href="https://cycu.site/ {隨身碟編號} ">這裡</a>開啟完整檔案。</p>
10     </body>
11 </html>
```

連線紀錄

日期時間 隨身碟編號 IP位址 瀏覽器

```
69 @app.route("/<code>", methods=["GET", "POST"])
70 def survey(code):
71     time = get_local_time()
72     ip, is_internal = get_ip_info()
73     ua = request.headers.get("User-Agent")
74
75     usb_number, error = decode_code(code)
76
77     if error:
78         # 詳細記錄錯誤訊息
79         error_message = f"ERROR<br>編碼錯誤: {code}"
80
81         # 記錄錯誤到 invalid_log.txt
82         with open("/home/cocoalbertcocoalbert/11127110/CYCUUSB/logs/invalid_log.txt", "a", encoding="utf-8") as f:
83             f.write(f"[{time}] 錯誤編碼: {code} | 錯誤原因: {error} | IP: {ip} | UA: {ua} | Error: {error}\n")
84
85         # 回傳錯誤訊息
86         return error_message
87
88     # 如果編碼合法，記錄正常訪問信息
89     with open("/home/cocoalbertcocoalbert/11127110/CYCUUSB/logs/access_log.csv", "a", encoding="utf-8", newline='') as f:
90         writer = csv.writer(f)
91         # 寫入一系列資料
92         writer.writerow([time, usb_number, code, ip, is_internal, ua])
```

問卷表單

恭喜您成為受試者！

- ※ 本研究旨在探討大眾對於「陌生隨身碟的使用行為及風險認知」。
- ※ 透過實地設置與問卷調查的方式，了解您在撿拾、插入及開啟未知隨身碟時的考量與行動。
- ※ 以下問卷資料僅作為學術研究分析使用，將保密處理，不涉及個人識別。
- ※ 本研究已向校安單位完成報備，相關作業均依校內規範進行。
- ※ 本研究由中原大學1132資訊素養概論第五研究團隊執行。
- ※ 若您對本研究有任何疑問，歡迎與我們聯絡；研究專案主持人alberthsu919@cycu.org.tw。
- ※ 按下「提交」即表示您已了解研究內容並同意參與本研究。

1. 您的性別：

- ☐ 男
- ☐ 女
- ☐ 非二元性別 / 不願透露

2. 您的年齡層：

- ☐ 17歲以下
- ☐ 18-24歲
- ☐ 25-34歲

研究倫理

已取得「學生事務處校安專責導師室」、「軍訓室」同意
隨身碟不含惡意程式，或是主動收集個人資料的系統
不涉及任何個人識別 所有數據僅作為學術研究分析使用

報備「陌生隨身碟的使用行為及風險認知」研究計畫

5 封郵件

Albert Hsu <alberthsu919@gmail.com>

2025年5月16日 下午4:55


收件者: hcchin@cycu.edu.tw

主任您好，
我們是資訊素養概論第五研究團隊，我們將進行「陌生隨身碟的使用行為及風險認知」的研究。預計於下週二(5/20)至週五(5/23)，於中原大學校園內投放約120個隨身碟。
隨身碟內容為一個HTML檔案（如附件），不含任何惡意程式，或是任何主動收集個人資料的系統；僅在受試者親自開啟檔案，才會進行紀錄，不涉及任何個人識別，所有數據僅作為學術研究分析使用，符合現行規定與研究倫理原則。

此封信件特此報備校安單位，敬請知悉，並感謝主任、老師與相關單位的支持與理解。

（此封信件有於昨日(5/15)寄給孔慶壽專案助理kungso1234@cycu.edu.tw，未收到任何回覆，於此再次向校安單位報備說明。）

資訊素養概論第五研究團隊
學生／研究專案主持人
許至均
資訊三甲 11127110
alberthsu919@gmail.com

 Info_2025-05.pdf.html
1K

秦漢忠 <hcchin@cycu.edu.tw>
回覆: 秦漢忠 <hcchin@cycu.edu.tw>
收件者: Albert Hsu <alberthsu919@gmail.com>

2025年5月19日 下午5:35

許同學，午安
已收來信，我會轉知教官們，也請你們在研究過程中必須完全在老師指導之下，並確保不造成受試師生誤會，祝一切順利。

秦教官

資料分析方法

定性資料

開放式問項

意圖動機

定量資料

隨身碟追蹤

時間、地點



PLACING



實驗與問卷結果

隨身碟行為數量統計

投放時間：5 月 19 日 至 24 日
統計時間：5 月 19 日 至 6 月 5 日

準備數量：125 個隨身碟
實際投放：62 個隨身碟

	數量（ 個 ）	比例（ % ）
總投放	62	100
被移動、撿拾	47	75.81
被開啟	8	12.90
有填寫問卷	4	6.45

隨身碟行為地圖

		數量（個）	區域比例（%）
校區A	投放	57	100
	被開啟	7	12.28
校區B	投放	2	100
	被開啟	0	0
校區C	投放	3	100
	被開啟	1	33.33

樣本數差異大，無有效結論

隨身碟行為地圖

		數量 (個)	地域比例 (%)
室內	投放	44	100
	被開啟	4	9.09
室外	投放	18	100
	被開啟	4	22.22

室外開啟比例高

隨身碟行為地圖



隨身碟開啟紀錄

編號	訪問時間	IP位址	作業系統	瀏覽器 (系列)
93	2025/5/22 05:37	2001:b011:6c0e:****:****:****:****:****	Windows	Chrome
103	2025/5/23 09:46	2001:b400:e23b:****:****:****:****:****	Windows	Chrome
82	2025/5/23 12:41	140.135.37.**	Windows	Chrome
62	2025/5/26 09:06	140.135.184.***	Windows	Edge
57	2025/5/26 17:27	140.135.140.**	Windows	Chrome
87	2025/5/27 09:38	140.135.40.***	Windows	Edge
101	2025/5/28 13:00	140.135.237.***	Windows	Chrome
77	2025/5/31 23:00	2a09:bac1:7400:***::**:*	Windows	Chrome

校內IP 5個

全為 Windows

Chrome 系列 5 個

隨身碟開啟紀錄

編號	投放時間	投放地點	投放地域	投放校區	被訪問所經時間（天）
93	2025/5/20 13:16	電資學院外鐵椅子	室外	A	1.68
103	2025/5/21 15:06	莊敬大樓穿堂桌上	室內	A	1.78
82	2025/5/19 19:00	教學大樓402教室桌上	室內	A	3.74
62	2025/5/19 19:00	鐘塔草皮的白色餐桌	室外	A	6.59
57	2025/5/24 12:00	篤信大樓地下室教室	室內	A	2.23
87	2025/5/19 19:00	圖書館地下自習室電腦區	室內	A	7.61
101	2025/5/20 18:53	熱誠宿舍二樓空橋	室外	C	7.75
77	2025/5/19 19:00	全人村練舞區	室外	A	12.17

最短 1 天 16 小時 21 分鐘

最久 12 天 4 小時

平均 5.44 天

問卷紀錄

編號	性別	年齡	職業	單位 / 系級
62	男	51-60歲	學校職員	軍訓室
57	非二元性別 / 不願透露	61歲以上	學校職員	工業系辦
87	非二元性別 / 不願透露	18-24歲	其他 / 不願透露	
77	女	18-24歲	學生	我不要說

推論職員與學生各半

問卷紀錄

編號	發現地點	撿起、讀取動機	開啟檔案動機
62	維澈樓	基於助人意圖，確認隨身碟是否包含可協助尋找失主的線索	基於助人意圖，確認隨身碟是否包含可協助尋找失主的線索
57	206飲水機櫃子旁	出於好奇心，探索隨身碟內可能包含的資訊	出於好奇心，探索隨身碟內可能包含的資訊
87	維澈樓1F	出於好奇心，探索隨身碟內可能包含的資訊	出於好奇心，探索隨身碟內可能包含的資訊
77	在全人教育	這樣我就能知道是否有任何最深最黑暗的秘密	同樣的原因（同左）

3 個與原投放位置差距極大

好奇占多數

問卷紀錄

編號	是否顧慮讀取	是否顧慮開啟檔案	使用裝置	是否採取預防措施
62	是：怕中毒	是：不明檔案	個人電腦裝置	是：掃毒
57	是：怕有色情內容	否	學校實驗室或圖書館等公共裝置	否
87	否	否	學校實驗室或圖書館等公共裝置	否
77	是：當然有，也許像病毒？	是：同樣的原因（同左）	個人電腦裝置	否

僅一人掃毒

群組及校版討論

5月22日至23日

宿舍群組

Dcard 兩篇貼文



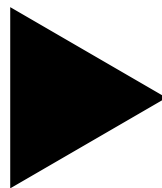
■ 系統缺失

5 月 27 日約 10 時 30 分至 18 時

中斷實驗記錄約 7 小時 30 分鐘



中原大學雲平台系統政策更新



研究結論

隨身碟使用行為觀察

1

拾取比例高

75.81 % 被移動撿拾，與前人研究之 98 % 有降低的趨勢，但還是有十分高比例

2

開啟比例低

12.90 % 被開啟，與前人研究之 39 %、50 %、45 % 有明顯下降
多數人在拾取後具備風險意識或猶豫態度

3

地域差異明顯

室外 22.22 % 明顯高於室內 9.09 %，
推測室外隨身碟較不為尋常，易吸引注意，引發熱心與好奇心

4

校區影響行為

B、C 校區樣本數偏少，無有效結論

開啟行為分析

1

Windows 作業系統及 Chrome 系列瀏覽器為主

所有開啟行為皆於 Windows，瀏覽器以 Chrome 系列為主 62.5 %

2

多數開啟行為來自校內網路

62.5 % 之訪問來自校內 IP 環境設備，風險較低
大眾對於使用個人電腦訪問陌生隨身碟仍保有一定警覺性

3

開啟時間間隔大

最短為 1.68 天，最長超過 12 天，平均為 5.44 天，與前人研究差異甚大
大眾對於使用陌生裝置之顧慮與考量有明顯增加

問卷調查結果

1

開啟動機以好奇心為主

以好奇心為開啟動機占多數
推測可能與隨身碟無任何標籤有關

2

風險認知存在但行動不足

多數受試者自述存在風險顧慮，但僅一人事前掃毒
風險意識未能有效轉化為實際防範行動

3

不同背景皆有開啟行為

受試者包含職員與學生
校園內各類人員均有潛在之資訊安全風險

研究反思與未來展望

1

樣本數需擴增

62 個樣本數有限，研究結果可能存在偏差
未來可擴大投放數量，設計多元的問卷、投放地點與隨身碟呈現形式

2

系統中斷影響資料完整性

伺服器系統一度中斷，行為資料可能遺漏，影響實驗完整性
後續研究可採取備援機制，提升系統穩定性與資料保全性

3

強化風險教育

不少受試者終仍「不敵好奇心」
強化資訊安全教育、社交工程認知、資訊素養能力
職員行為於校內環境中，將可能威脅校內資訊系統
加強校內職員相關風險管理與行為規範

- 參考文獻 -

- [1] 方仁威 (2016) 。論社交工程安全威脅之研究。發展與前瞻學報，(11)，33-52。 [https://doi.org/10.6737/jdp.201603_\(11\).03](https://doi.org/10.6737/jdp.201603_(11).03)
- [2] 林方昌 (2024) 。資通安全素養與認知對遵守資通安全政策行為之影響 [未出版之碩士論文] 。中原大學企業管理學系。
- [3] 唐善智 (2011) 。資訊安全事件與資訊安全認知關係之研究 - 以社交工程為例 [未出版之碩士論文] 。中原大學資訊管理研究所。
- [4] Benenson, Z., Girard, A., Hintz, N., & Luder, A. (2014). Susceptibility to URL-based Internet attacks: Facebook vs. email. 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS).
- [5] Ferguson, I. Y. (2017). The Effectiveness of Social Engineering as a Cyber-Attacking Vector: People Do Use Unknown USB Drive, They Find. In.
- [6] Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. 2014 Information Security for South Africa.
- [7] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89. <https://www.mdpi.com/1999-5903/11/4/89>
- [8] Sèdes, F., & Degrace, J. (2024). Social Engineering and Security: from human vulnerabilities to malicious threats. 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
- [9] Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users really do plug in USB drives they find. 2016 IEEE Symposium on Security and Privacy (SP).
- [10] Tischer, M. A. (2015). *Testing the malicious USB anecdote* University of Illinois at Urbana-Champaign].

- AI 協作 -

OpenAI (2025). *ChatGPT (GPT-4o)* [Large language model]. <https://chatgpt.com/>

資料統整

重點擷取

文句潤飾

文本翻譯

錯誤引註

超意答覆

內容查證

※ 簡報封面圖由 Copilot 生成



- 抄襲檢測 -

原創性報告

7%

相似度指數

6%

網際網絡來源

2%

出版物



4%



學生文稿


1	Submitted to National Chung Hsing University	1%
	學生文稿	
2	ndltd.ncl.edu.tw	1%
	網際網絡來源	
3	repozitorij.efzg.unizg.hr	1%
	網際網絡來源	
4	Submitted to Edith Cowan University	1%
	學生文稿	
5	Submitted to University of Nebraska at Omaha	1%
	學生文稿	
6	www.jissec.org	<1%
	網際網絡來源	
7	erepository.uonbi.ac.ke	<1%
	網際網絡來源	
8	Submitted to metubudapest	<1%
	學生文稿	
9	Submitted to iGroup	<1%
	學生文稿	
10	www.ixma.org	<1%
	網際網絡來源	
11	www.796t.com	<1%
	網際網絡來源	
12	rportal.lib.ntnu.edu.tw:8080	<1%
	網際網絡來源	
13	www.phic.org.cn	<1%
	網際網絡來源	
14	docsplayer.com	<1%
	網際網絡來源	
15	www.e-cancer.fr	<1%
	網際網絡來源	
16	www.lac.org.tw	<1%
	網際網絡來源	
17	www.nordangliaeducation.com	<1%
	網際網絡來源	
18	www.turansam.org	<1%
	網際網絡來源	
19	"Financial Cryptography and Data Security", Springer Science and Business Media LLC, 2017	<1%
	出版物	

- 小組分工 -

資訊三甲	11127110	許至昀				
------	----------	-----	---	---	---	---

化工生化組四乙	11021247	鍾昀翰		
---------	----------	-----	---	---

工業工程組二甲	11224133	趙永騫		
---------	----------	-----	---	---

資訊三甲	11127137	黃乙家	
------	----------	-----	---



組長 / 研究專案主持人



系統架設



隨身碟投放與紀錄



簡報統整製作



線上口頭報告

- 心得 -

許至昀

說到陌生隨身碟，如果透過口頭的方式詢問大眾開啟意願，幾乎所有人都不會。秉持實事求是的精神，我們設計實體的校園實驗，得出有 12.9 % 的隨身碟被開啟，低於我原先預估的 20 %。大眾的資安意識確實有所提升，但還需要加強，替別針對學校職員。

身為組長與研究的發想人，有責任將這份研究報告完成。我期待能以自動自發、團隊合作的方式讓所有組員一同參與，有想法則檢索，有資料則加上，有空缺則補齊，而不是使用強制的分工。遺憾的是，這樣的理想合作方式未能如預期實現。

在課業繁重之際，能完成這項研究並非易事。感謝組員，感謝相關協助的人員，感謝受試者，也感謝我自己。雖然過程中充滿挑戰，但我們仍然完成了目標，並從中學習、反思與成長。願未來持續運用資訊素養的能力，秉持探究實作的精神，面對每一次學術與人生歷程。

- 心得 -

鍾昀翰

這次實驗讓我覺得很新奇，因為我們只是隨便把幾個隨身碟放在學校裡，居然真的有人去插來看。那一刻我突然覺得，原來還有人對這種風險真的沒什麼警覺心。說實話，一開始我們只是想看看結果會怎樣，沒想到真的有人上鉤，有點好笑又有點毛毛的。雖然我們沒有真的去做什麼壞事，但看到那些數據，還是會想：「如果今天不是我們做這實驗，而是駭客怎麼辦？」這也讓我開始反思，平常自己在用電腦或接觸外部裝置時，是不是也太大意。做完這次實驗後，我覺得資安這東西不是只有工程師要懂，每個人都應該有點基本警覺才行。

- 心得 -

趙永騫

這是一個挺有挑戰性的實驗，不管是內容的發想又或是實驗的實形，都充滿了挑戰性。而從中我也了解到人們對於現今社會中陌生物品的警惕性有提高，不會因為好奇心而去做一些可能會構成危險或是安全洩漏的問題。當今數位時代，資訊安全變得越來越重要。無論是個人資料、企業機密，甚至國家安全，都可能因為一個小小的疏忽而遭到威脅。駭客技術日新月異，網路攻擊方式層出不窮，因此我們除了依賴科技手段防護，更應提升自己的資安意識，從日常生活中培養良好的使用習慣。

- 心得 -

黃乙家

我覺得這是一個很有趣的實驗，可以了解中原大學師生的資安觀念。在現實情況下，攻擊者可以在隨身碟寫入腳本，讓電腦以為插入的隨身碟是鍵盤，實際上卻是在監聽使用者輸入的文字並將帳號密碼傳給攻擊者。另一種攻擊向量（ Attack Vector ）是將腳本寫成 Reverse Shell 後連回攻擊者的 C2（ Command & Control ） Server，達成 Remote Code Execution，有些甚至可以把受害者電腦的防毒軟體關掉、繞過 UAC（ User Access Control）、進行持久化（後門），如果是在企業網路還可以進行 Lateral Movement，完全接管系統，即使啟用 BitLocker 也可能在登入前就受到威脅！而且這類攻擊的成本不到 100 台幣。因此我們更應該建立起良好的資安觀念，以避免資產的損毀。

“

完整詳細內容請參見書面報告

”



感謝聆聽

陌生隨身碟使用行為與風險認知之探討：以中原大學為例

許至昀¹、鍾昀翰²、趙永騫³、黃乙家⁴

^{1、4} 中原大學資訊工程學系三年級甲班

² 中原大學化學工程學系生化工程組四年級乙班

³ 中原大學工業與系統工程學系工業工程組二年級甲班

¹alberthsu919@cycu.org.tw、²heny9184@gmail.com、

³tim157278@gmail.com、⁴u810025@gmail.com

摘要

本研究旨在探討中原大學師生對陌生隨身碟的使用行為及其風險認知，透過社會實驗與問卷調查，分析資訊安全意識在實際情境中的表現。研究設計分為兩階段：首先於校園不同地點投放共 62 個隨身碟，觀察其是否被撿拾及開啟；其次在隨身碟中嵌入 HTML 檔案連結至問卷平台，蒐集開啟者的相關資料。

結果顯示，有 75.81 % 的隨身碟被撿拾，12.90 % 被開啟，與過往研究中的開啟率（約 45%）相比大幅下降，顯示校園師生已有初步的資安風險認知。室外地點的開啟率（22.22 %）高於室內（9.09 %），可能因環境影響使用者的好奇與行為動機。開啟行為多發生於校內網域，以 Windows 系統及 Chrome 系列瀏覽器為主。問卷結果顯示，大多數開啟者出於好奇動機，但僅少數在讀取前採取掃毒等防範措施，顯示認知與實際行動間仍存在落差。

研究亦指出，即使是學校職員也會有開啟不明隨身碟的行為，這可能對校內資訊系統造成潛在風險。未來應加強資訊素養與社交工程防範教育，並透過多樣化實驗設計與更完善的系統架構，提升研究的準確性與應用價值。本研究提供具體實證資料，可作為校園資訊安全教育及政策制定之重要參考。

關鍵字：資訊安全、社交工程、隨身碟行為、風險認知、校園實驗

Abstract

This study aims to explore the behavior and risk perception of Chung Yuan Christian University faculty and students regarding the use of unknown USB flash drives. Through a combination of field experiments and questionnaire surveys, the study analyzes how information security awareness manifests in real-life situations. The research was conducted in two stages: first, 62 USB drives were strategically placed in various campus locations to observe whether they would be picked up and opened; second, an HTML file embedded in the USB drives linked to a questionnaire platform to collect data from users who opened the drives.

The results show that 75.81 % of the USB drives were picked up and 12.90% were opened. This opening rate is significantly lower than that reported in previous studies (around 45 %), indicating that campus faculty and students have developed an initial awareness of cybersecurity risks. The opening rate was higher in outdoor locations (22.22 %) compared to indoor locations (9.09 %), suggesting that environmental factors may influence curiosity and behavioral motivation. Most opening incidents occurred within the campus network, predominantly using Windows systems and Chrome-based browsers. Questionnaire responses indicated that most users opened the drives out of curiosity, but only a few took preventive measures, such as scanning for malware, before accessing the files—revealing a gap between risk awareness and actual behavior.

The study also found that even university staff engaged in opening unknown USB drives, posing potential risks to the campus information systems. The findings suggest the need for enhanced information literacy and education on preventing social engineering attacks. Future research should employ more diverse experimental designs and improved system architectures to increase both the accuracy and practical value of the results. This study provides concrete empirical data that can serve as a valuable reference for campus cybersecurity education and policy development.

Keywords: Information Security, Social Engineering, USB Flash Drive Behavior, Risk Perception, Campus Experiment

壹、前言

隨著科技快速發展，人工智慧（AI，Artificial Intelligence）、網際網路應用、軟硬體技術的進步，資通安全的威脅變得日益複雜且多樣化。其中，社交工程（Social Engineering）作為一種常見且有效的攻擊手法，常透過惡意連結或外接裝置誘使使用者執行危險操作，進而達到入侵目的。

Matthew Tischer（2015）研究指出，有 98% 的陌生隨身碟（USB，Universal Serial Bus）被人撿起或移走，有 45% 的隨身碟被插入電腦並開啟一個或多個檔案 [9][10]。這樣的比例十分高，與本研究團隊以及大眾普遍的預期相差甚遠。

本研究旨在探討現代社會中，人們對於陌生隨身碟的使用行為與風險認知。研究將以中原大學校園為實驗場域，透過設計社會實驗，收集實際數據，分析學生、教職員工等對於陌生隨身碟的應對行為。

隨著資通安全教育的推廣與資訊科技素養的提升，大眾對於相關風險的認識應更加全面。在實際生活情境中，是否有人因為好奇、善意或其他動機，而撿拾並使用來源不明的隨身碟？開啟陌生隨身碟所可能引發的風險，是否潛伏於臺灣校園的日常環境中？同時，亦將探討隨身碟投放地點是否對其被開啟的比例產生顯著影響。

本研究將透過實地觀察與資料分析，為資通安全與社交工程領域提供具體的實證資料，藉以提升校園大眾對於惡意連結及不明外接裝置潛在風險的認知，並作為未來資通安全教育推廣與政策制定的重要參考依據。

貳、文獻探討

2.1 資通安全（Cybersecurity / ICT Security，資安）

依據《資通安全管理法》第三條第一款，資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性（數位發展部，2020）。

人員（People）、程序（Process）和技術（Technology）是影響資安的三個要素 [3]。其中，人員是穩定性最低、重要性最高的要素，人員的認知與意識是影響資安的重中之重。

資訊網路活動中存在一定風險，人們感知道的風險可謂「知覺風險」，知覺風險可分為六個面向，財務風險、績效風險、身體（實體）風險、心理風險、社會風險和時間風險，又以心理風險和社會風險為之顯著 [2]。

根據臺灣企業 2023 年資安弱點排名 (iThome, 2023)，第一名為「員工資安意識不足」，佔 55.5%；臺灣企業 2023 年~2024 年最可能發生的十大資安風險 (iThome, 2023)，第一名為「社交工程手段」，佔 40.8% [2]。大眾對於資安意識與風險認知仍顯著匱乏，特別是面對社交工程方面的攻擊。

2.2 社交工程

社交工程是一種利用人際影響力或說服技巧來欺騙他人的手段，透過人們之間的社會互動來獲取或危害組織的系統資訊，從而展開攻擊行為 [1]。

社交工程造成廣泛普遍的資安危害，其主要原因有二：「人員對於社交工程認知的不足」以及「惡意人士不需要備頂尖的電腦專業技術」，有心人士得以輕易騙取個人資訊，不亞於駭客系統性攻擊 [1] [3]。

2.3 社交工程攻擊

社交工程攻擊，可以分為四個階段：研究 (Research)、誘導 (Hook)、行動 (Play)、退出 (Out) [7]。根據 Francois Mouton 等人 (2014) 研究，社交工程攻擊的詳細流程可分為以下六個步驟 [6] [8]：

1. 攻擊目標設定 (Attack Formulation)
2. 資訊蒐集 (Information Gathering)
3. 攻擊準備 (Preparation)
4. 建立關係 (Develop Relationship)
5. 利用信任 (Exploit Relationship)
6. 善後處理 (Debrief)

常見的社交工程攻擊類型與形式，以及其所使用的心理、技術操作手法，本研究整理繪製下表 (表一) [1] [7]。

表一：社交工程攻擊類型與形式手法統整表

類型	形式	手法
網絡釣魚 Phishing	勒索軟體 Ransomware	偽裝修補程式或新功能安裝程式
	肩窺攻擊 Shoulder Surfing	直接索取重要資訊
	逆向社交工程 Reverse Social Engineering	信任關係建立
	假軟體	偽裝修補程式或新功能安裝程式

	Fake Software	
誘餌攻擊 Baiting	客服冒充 Impersonation on Help Desk	身分偽冒
	等價交換詐騙 Quid Pro Quo	貪小便宜心理、 直接索取重要資訊
	在線社交工程 Online Social Engineering	信任關係建立、 直接索取重要資訊
	網路域名欺騙 Pharming	偽裝修補程式或新功能安裝程式
假藉理由 Pretexting	貨物轉移詐騙 Diversion Theft	身分偽冒
	彈出視窗欺騙 Pop-Up windows	恐懼心理、 偽裝修補程式或新功能安裝程式
	電話社交工程 Phone Social Engineering	身分偽冒、 信任關係建立
	短信釣魚 SMSishing	偽裝修補程式或新功能安裝程式、 貪小便宜心理
尾隨攻擊 Tailgating	垃圾搜集 Dumpster Diving	直接索取重要資訊
	機器電話詐騙 Robocalls	身分偽冒、 恐懼心理
	竊取重要文件 Stealing Important Documents	直接索取重要資訊
	白名單欺騙 Whitelisting flow	偽裝修補程式或新功能安裝程式

2.4 不明連結被訪問研究

Zinaida Benenson 等人（2014）的研究，藉由 Facebook 和電子郵件發送內容包含一個看似來自「上週照片」的個人化連結給受試者，進行點擊行為觀察，以及問卷分析。總共 398 位受試者中，有 339 人（85%）完成問卷填答，自述點擊連結有 68 人（20%），而實際進行點擊行為有 179 人（39%） [4]。

2.5 不明隨身碟被執行研究

Isaac Yaw Ferguson（2017）的研究，實驗總共使用了 13 個隨身碟，有效投放的 6 個隨身碟中，有 3 個成功產生了連線，成功率 50% [5]。

Matthew Tischer（2015）進行大規模研究，於伊利諾大學厄巴納——香檳

分校（University of Illinois Urbana-Champaign）投放 297 個隨身碟，其中有 290 個（98%）被移動，且有 135 個（45%）被開啟。從投放到開啟的時間平均為 6.9 小時，最快插入時間不到 6 分鐘，有 87.5% 的隨身碟在當天就被撿起。隨身碟外標籤、投放位置以及投放時間對成功率未有顯著差異；除了有「歸還資訊標籤」，受試者可以透過標籤聯絡失主，成功率較低。多數使用者插入隨身碟的動機是想尋找失主（68%），也有出於好奇（18%） [9] [10]。

2.6 資通安全素養

素養，亦指邏輯推理和批判性思考的能力。資訊素養涵蓋以下四大面向，傳統素養、媒體素養、電腦素養以及網路素養；資通安全素養是建立在資訊素養的基礎上，搭配通訊裝置（電腦、平板、手機等）操作與系統和網路使用的能力 [2]。

可以透過專業訓練課程來提升大眾資通安全的素養，或是透過經過設計的互動式遊戲，讓大眾了解資通安全的素養的重要性，也可以藉由測試實驗來評估受試者，喚醒其對資通安全的素養的重視。除了大眾自身的預防意識，透過輔助程式偵測安全風險，打造到更有效的防護網 [8]。

2.7 理論基礎與研究連結

前述文獻指出，人員資安意識薄弱是資通安全最大風險，社交工程則是最常見且成功率高的攻擊手法，常藉由好奇心、信任等心理因素影響受害者行為。

大約有四成的民眾會點擊不明連結或插入陌生隨身碟。本研究以中原大學為實驗場域，結合前人研究方法，觀察實際行為並分析風險認知，進一步探討當今社會對資通安全素養能力是否有所提升。同時，也藉由本研究喚起大眾對資通安全的素養以及社交工程攻擊風險的重視。

參、研究方法

本研究以中原大學校園為主要研究場域，結合社會實驗與問卷調查法，蒐集定量資料與分析。研究目的為觀察並了解大學生與教職員工對陌生隨身碟的使用行為與潛在風險的認知情形。

3.1 研究設計

本研究主要分為兩個階段：

1. 第一階段：社會實驗

模擬真實情境，於中原大學校園內多個地點（如教室、圖書館等）隨機放置隨身碟，觀察其被移動撿拾及插入裝置連線的情形，並記錄相關數據。

2. 第二階段：問卷調查

在隨機放置的隨身碟中，放置連結檔案並嵌入問卷表單，收集受試者資訊。包含開啟動機、開啟裝置等。

3.2 實驗工具

本研究共使用 125 個隨身碟。隨身碟外觀顏色有紅色、黑色、藍色、綠色、白色、橙色等，並放置在透明夾鏈袋中，如下圖（圖一）。夾鏈袋除了防水、防塵外，也有看起來較是人為自然使用之意。



圖一：隨身碟外觀樣式

3.3 檔案內容

每個隨身碟中階放置單一個名為「Info_2025-05.pdf」的 HTML 檔案。命名為仿造一般文件，以及加上日期提供時事感。HTML 檔案可以跨平台、跨裝置使用，檔案內容如下：

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <script>window.location.href =
```



```
"https://cycu.site/ {隨身碟編號} ";</script>
</head>
<body>
  <p>檔案預覽失敗，請點擊
  <a href="https://cycu.site/ {隨身碟編號} ">這裡</a>
  開啟完整檔案。</p>
</body>
</html>
```

{隨身碟編號} 以十位元數字與英文字母編碼構成，以便後台管理數據，使用簡單加密技術，防止受試者惡意進入其他隨身碟編號，影響實驗結果。

3.4 連線紀錄

使用中原大學 AI Console 架設伺服器系統。當有受試者點擊檔案後，會產生記錄檔，包含日期時間、隨身碟編號、IP 位址以及所使用的瀏覽器。

3.5 問卷表單

當受試者點擊檔案後，會出現「恭喜您成為受試者！」的字樣以及研究說明內容，接著顯示問卷表單。問題包含基本資料，如性別、年齡、職業等；以及隨身碟相關問題，如開啟動機、開啟裝置、預防措施等。詳細頁面見附錄一。

3.6 研究倫理

校園陌生隨身碟實驗已取得中原大學「學生事務處校安專責導師室」以及「軍訓室」的同意。

隨身碟內容為一個 HTML 檔案，不含任何惡意程式，或是任何主動收集個人資料的系統；僅在受試者親自開啟檔案，才會進行紀錄，不涉及任何個人識別，所有數據僅作為學術研究分析使用，符合現行規定與研究倫理原則。

3.7 資料分析方法

本研究使用定性資料與定量資料進行分析。定性資料包含問卷中的開放式問項，像是撿拾與開啟的意圖動機等。定量資料，使用隨身碟編號進行追蹤，像是開啟時間、地點等，為分析受試者行為之客觀指標。

肆、實驗與問卷結果

4.1 隨身碟行為數量統計

本研究團隊於 2025 年 5 月 19 日至 24 日於中原大學校園內進行隨身碟投放。行為紀錄從隨身碟投放當日起始日至 6 月 5 日。研究團隊準備共 125 隨身碟，由於損毀、實驗期限等限制，因此實際僅投放 62 個，有 47 個（75.81 %）被移動、撿拾，有 8 個（12.90 %）被開啟，有 4 個有填寫問卷（6.45 %）。隨身碟行為數量統計如下表（表二）：

表二：隨身碟行為統計表

	數量（個）	比例（%）
總投放	62	100
被移動、撿拾	47	75.81
被開啟	8	12.90
有填寫問卷	4	6.45

4.2 隨身碟行為地圖

根據中原大學官方校園地圖，將校園區分為三個區域：A 校區，行政與教學區域；B 校區，運動園區、宿舍、特殊功能教室；B 校區，宿舍、設備中心，詳見中原大學校園配置圖（附錄二）。本研究於三個校區皆有投放，統計如下表（表三）。

表三：隨身碟校區行為統計表

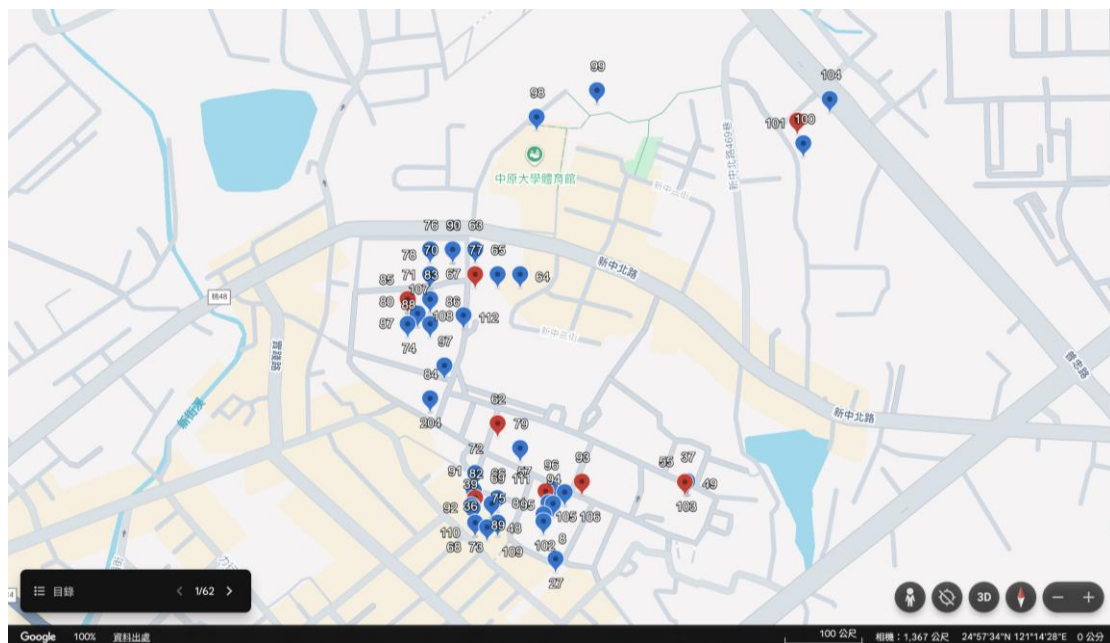
		數量（個）	區域比例（%）
校區 A	投放	57	100
	被開啟	7	12.28
校區 B	投放	2	100
	被開啟	0	0
校區 C	投放	3	100
	被開啟	1	33.33

本研究將投放地域區分為室內與室外進行統計，如下表（表四）。

表四：隨身碟地域行為統計表

		數量（個）	地域比例（%）
室內	投放	44	100
	被開啟	4	9.09
室外	投放	18	100
	被開啟	4	22.22

將隨身碟以座標方式記錄於 Google Earth 繪製校園實驗投放地圖（圖二），藍色標記為投放之隨身碟，紅色為被開啟之隨身碟。



圖二：隨身碟行為座標地圖

4.3 隨身碟開啟紀錄

在 8 個被開啟的隨身碟中，共有 5 個（62.5 %）的 IP 位址是 140.135 為開頭，即為中原大學 IP。訪問網頁 8 個均使用 Windows 作業系統，其中有 5 個（62.5 %）是使用 Chrome 系列瀏覽器，有三個是使用 Edge 系列瀏覽器（37.5 %）。隨身碟開啟紀錄整理見下表（表五）

表五：隨身碟開啟紀錄統計表

編號	訪問時間	IP 位址	作業系統	瀏覽器 (系列)
93	2025/5/22 05:37	2001:b011:6c0e:****:****:*** **.*.****.*.****	Windows	Chrome
103	2025/5/23 09:46	2001:b400:e23b:****:****:*** **.*.****.*.****	Windows	Chrome
82	2025/5/23 12:41	140.135.37.**	Windows	Chrome
62	2025/5/26 09:06	140.135.184.***	Windows	Edge
57	2025/5/26 17:27	140.135.140.**	Windows	Chrome
87	2025/5/27 09:38	140.135.40.***	Windows	Edge
101	2025/5/28 13:00	140.135.237.***	Windows	Chrome
77	2025/5/31 23:00	2a09:bac1:7400:***:***:***	Windows	Chrome

隨身碟最短經過 1 天 16 小時 21 分鐘後被開啟，而最久達 12 天 4 小時後才被撿拾訪問；從投放到開啟的時間平均為 5.44 天。

表六：隨身碟投放與開啟紀錄統計表

編號	投放時間	投放地點	投放 地域	投放 校區	被訪問所經 時間(天)
93	2025/5/20 13:16	電資學院外鐵椅子	室外	A	1.68
103	2025/5/21 15:06	莊敬大樓穿堂桌上	室內	A	1.78
82	2025/5/19 19:00	教學大樓 402 教室桌上	室內	A	3.74
62	2025/5/19 19:00	鐘塔草皮的白色餐桌	室外	A	6.59
57	2025/5/24 12:00	篤信大樓地下室教室	室內	A	2.23
87	2025/5/19 19:00	圖書館地下自習室電腦區	室內	A	7.61
101	2025/5/20 18:53	熱誠宿舍二樓空橋	室外	C	7.75
77	2025/5/19 19:00	全人村練舞區	室外	A	12.17

4.4 問卷紀錄

根據問卷內容（附錄一）我們收集共四位受試者的填答進行行為研究，以下呈現填答結果，包含基本資訊（表七）、隨身碟發現地點與開啟動機（表八）、隨身碟開啟顧慮、裝置與預防措施（表九）。

受試者有兩位教職員、一位學生，以及一位未知；根據年齡判斷，未知應為學生或是工讀生，推論受試者職員與學生各半。

表七：受試者問卷填答基本資訊

編號	性別	年齡	職業	單位／系級
62	男	51-60 歲	學校職員	軍訓室
57	非二元性別／不願透露	61 歲以上	學校職員	工業系辦
87	非二元性別／不願透露	18-24 歲	其他／不願透露	
77	女	18-24 歲	學生	我不要說

編號 62、編號 57 與編號 87 隨身碟，根據受試者所填答的發現地點以及單位，已與原投放位置有極大的差距。撿起、讀取隨身碟與開啟檔案的動機相同；有三位受試者是出於好奇，有一位是想找到失主。

表八：受試者問卷填答隨身碟發現地點與開啟動機

編號	發現地點	撿起、讀取動機	開啟檔案動機
62	維澈樓	基於助人意圖，確認隨身碟是否包含可協助尋找失主的線索	基於助人意圖，確認隨身碟是否包含可協助尋找失主的線索
57	206 飲水機櫃子旁	出於好奇心，探索隨身碟內可能包含的資訊	出於好奇心，探索隨身碟內可能包含的資訊
87	維澈樓 1F	出於好奇心，探索隨身碟內可能包含的資訊	出於好奇心，探索隨身碟內可能包含的資訊
77	在全人教育	這樣我就能知道是否有任何最深最黑暗的秘密	同樣的原因（同左）

編號 62、編號 57 與編號 87 隨身碟是透過學校 IP 位址訪問，根據使用裝置與單位，的確是如此；編號 62 所述之個人電腦，推論為學校辦公使用之電腦，連接校內網域。有三位對隨身碟讀取有顧慮，其中一位怕有色情內容；當看到檔案內容後，有兩位對開啟有顧慮，有兩位無。僅有一位在讀取前採取掃描病毒的預防措施。

表九：受試者問卷填答隨身碟開啟顧慮、裝置與預防措施

編號	是否顧慮讀取	是否顧慮開啟檔案	使用裝置	是否採取預防措施
62	是：怕中毒	是：不明檔案	個人電腦裝置	是：掃毒
57	是：怕有色情內容	否	學校實驗室或圖書館等公共裝置	否
87	否	否	學校實驗室或圖書館等公共裝置	否
77	是：當然有，也許像病毒？	是：同樣的原因（同左）	個人電腦裝置	否

4.5 群組及校版討論

於 5 月 22 日至 23 日期間，有人士在學校宿舍群組以及 Dcard 中原大學版張貼兩篇有關隨身碟失物招領的資訊，參見附錄三。

有學生留言「拜託誰可以插電腦看一下 我真的有夠好奇」、「慎防網路病毒」等，此研究實驗確實引起校內人員的關注。

4.6 系統缺失

隨身碟實驗紀錄之網站系統原架設於中原大學 GOC AI Console，在 5 月 27 日約 10 時 30 分因系統政策更新調整無法繼續提供服務，中斷實驗記錄。於同日約 18 時更改架設網站系統於 Google Cloud，重啟連線紀錄。此事件導致有約 7 小時 30 分鐘的隨身碟紀錄喪失。

伍、研究結論

5.1 隨身碟使用行為觀察

1. 拾取比例高

在 62 個隨身碟中，有 47 個（75.81 %）被移動、撿拾，與 Matthew Tischer（2015）研究之 98 %有降低的趨勢，但還是有十分高比例 [9] [10]。

2. 開啟比例低

在 62 個隨身碟中，有 8 個（12.90 %）被開啟，與 Zinaida Benenson 等人（2014）研究之 39 %、Isaac Yaw Ferguson（2017）研究之 50%以及 Matthew

Tischer (2015) 研究之 45%，有明顯的下降，顯示多數人在拾取後仍具備一定程度的風險意識或猶豫態度 [4] [5] [9] [10]。

3. 地域差異明顯

室外投放的隨身碟開啟比例 (22.22 %) 明顯高於室內 (9.09 %)，推測室外場域的隨身碟，較不為尋常，容易吸引大眾注意，引發大家的熱心與好奇心。

4. 校區影響行為

A、B、C 校區的投放比例差異大，B、C 校區樣本數偏少，無法得出有效的結論。

5.2 開啟行為分析

1. 開啟裝置以 Windows 作業系統及 Chrome 系列瀏覽器為主

所有開啟行為皆於 Windows 作業系統執行，瀏覽器以 Chrome 系列為主 (62.5%)，顯示 Windows 仍為校內與大眾主要的使用平台，並以 Chrome 系列為主要使用瀏覽器。

2. 多數開啟行為來自校內網路

共有 5 個隨身碟 (62.5 %) 之訪問來自中原大學 IP，顯示不少行為發生於校內環境設備。使用校內裝置所承擔的風險較低，大眾對於使用自己個人電腦裝置訪問陌生隨身碟仍保有一定警覺性。

3. 開啟時間間隔大

隨身碟自投放至開啟之時間最短為 1.68 天，最長超過 12 天，平均為 5.44 天，與 Matthew Tischer (2015) 之研究，從投放到開啟的時間平均為 6.9 小時，最快插入時間不到 6 分鐘，差異甚大 [9] [10]。顯示大眾對於使用陌生裝置之顧慮與考量有明顯的增加。

5.3 問卷調查結果

1. 開啟動機以好奇心為主

在四個有填寫問卷的受試者中，以好奇心為開啟動機占多數 (3 個)，少數出於助人意圖 (1 個)，推測可能與隨身碟無任何標籤有關，沒有資料或個人資

訊，大眾只因對其中內容好奇而打開隨身碟。

2. 風險認知存在但行動不足

多數受試者自述存在風險顧慮（如中毒、色情內容），但僅一人採取事前掃毒措施，顯示風險意識未能有效轉化為實際防範行動。

3. 不同背景皆有開啟行為

受試者包含職員與學生，顯示校園內各類人員均有潛在之資訊安全風險。

5.4 研究反思與未來展望

1. 樣本數需擴增

本次研究實驗僅使用 62 個隨身碟，樣本數相對有限，研究結果可能存在一定程度偏差。未來研究可擴大隨身碟投放數量，並設計更加多元的問卷內容、投放地點與隨身碟呈現形式，以提升統計效度、擴展樣本多樣性，並增進結果之普遍性與參考價值。

2. 系統中斷影響資料完整性

實驗期間伺服器系統一度中斷，部分行為資料可能遺漏，對實驗完整性有相當程度的影響。建議後續研究可採取備援機制，提升系統穩定性與資料保全性。

3. 強化風險教育

研究結果顯示，儘管大眾大部分皆具備風險意識，實際採取防範措施者比例仍偏低，且不少受試者最終仍「不敵好奇心」，選擇開啟未知隨身碟。值得注意的是，受試者中亦包含學校職員，若職員於校內網域環境中使用並開啟來路不明之隨身碟，將可能對校內資訊系統造成威脅。

未來應進一步強化資訊安全教育、社交工程認知、資訊素養能力，將風險意識轉化為具體行動，提升整體防範意識與行為落實度；尤其針對校內職員，須加強相關風險管理與行為規範。

參考文獻

中文參考文獻

- [1] 方仁威 (2016)。論社交工程安全威脅之研究。發展與前瞻學報，(11)，33-52。 [https://doi.org/10.6737/jdp.201603_\(11\).03](https://doi.org/10.6737/jdp.201603_(11).03)
- [2] 林方昌 (2024)。資通安全素養與認知對遵守資通安全政策行為之影響〔未出版之碩士論文〕。中原大學企業管理學系。
- [3] 唐善智 (2011)。資訊安全事件與資訊安全認知關係之研究—以社交工程為例〔未出版之碩士論文〕。中原大學資訊管理研究所。

英文參考文獻

- [4] Benenson, Z., Girard, A., Hintz, N., & Luder, A. (2014). Susceptibility to URL-based Internet attacks: Facebook vs. email. 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS).
- [5] Ferguson, I. Y. (2017). The Effectiveness of Social Engineering as a Cyber-Attacking Vector: People Do Use Unknown USB Drive, They Find. In.
- [6] Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. 2014 Information Security for South Africa.
- [7] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89. <https://www.mdpi.com/1999-5903/11/4/89>
- [8] Sèdes, F., & Degrace, J. (2024). Social Engineering and Security: from human vulnerabilities to malicious threats. 2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
- [9] Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users really do plug in USB drives they find. 2016 IEEE Symposium on Security and Privacy (SP).
- [10] Tischer, M. A. (2015). *Testing the malicious USB anecdote* University of Illinois at Urbana-Champaign].

生成式 AI 協作

- OpenAI (2025). *ChatGPT (GPT-4o)* [Large language model]. <https://chatgpt.com/>

附錄

附錄一：受試者頁面與表單問卷

恭喜您成為受試者！

- ※ 本研究旨在探討大眾對於「陌生隨身碟的使用行為及風險認知」。
- ※ 透過實地設置與問卷調查的方式，了解您在撿拾、插入及開啟未知隨身碟時的考量與行動。
- ※ 以下問卷資料僅作為學術研究分析使用，將保密處理，不涉及個人識別。
- ※ 本研究已向校安單位完成報備，相關作業均依校內規範進行。
- ※ 本研究由中原大學1132資訊素養概論第五研究團隊執行。
- ※ 若您對本研究有任何疑問，歡迎與我們聯絡；研究專案主持人alberthsu919@cycu.org.tw。
- ※ 按下「提交」即表示您已了解研究內容並同意參與本研究。

1. 您的性別：

- ☐ 男
- ☐ 女
- ☐ 非二元性別 / 不願透露

2. 您的年齡層：

- ☐ 17歲以下
- ☐ 18-24歲
- ☐ 25-30歲
- ☐ 31-40歲
- ☐ 41-50歲
- ☐ 51-60歲
- ☐ 61歲以上

- ☐ 不願透露

3. 您的職業：

- ☐ 學生
- ☐ 教師
- ☐ 學校職員
- ☐ 其他 / 不願透露

4. 您的服務單位 / 就讀系級：

例如：總務處、資訊二甲

5. 您在哪裡發現隨身碟？

例如：教學大樓505教室桌上

6. 為什麼您會撿起該隨身碟並將其插入電腦？

- ☐ 出於好奇心，探索隨身碟內可能包含的資訊
- ☐ 基於助人意圖，確認隨身碟是否包含可協助尋找失主的線索
- ☐ 其他

7. 為什麼您會開啟隨身碟中的檔案？

- ☐ 出於好奇心，探索隨身碟內可能包含的資訊
- ☐ 基於助人意圖，確認隨身碟是否包含可協助尋找失主的線索

☐ 其他

8. 您對插入該隨身碟是否有任何顧慮？

☐ 否

☐ 是

9. 您對開啟檔案是否有任何顧慮？

☐ 否

☐ 是

10. 您是使用哪一類型的裝置來開啟隨身碟？

☐ 個人電腦裝置（如筆電、桌機等）

☐ 個人行動裝置（如手機、平板等）

☐ 學校實驗室或圖書館等公共裝置

☐ 其他

11. 您在開啟該檔案前是否採取任何預防措施（如掃描病毒等）？

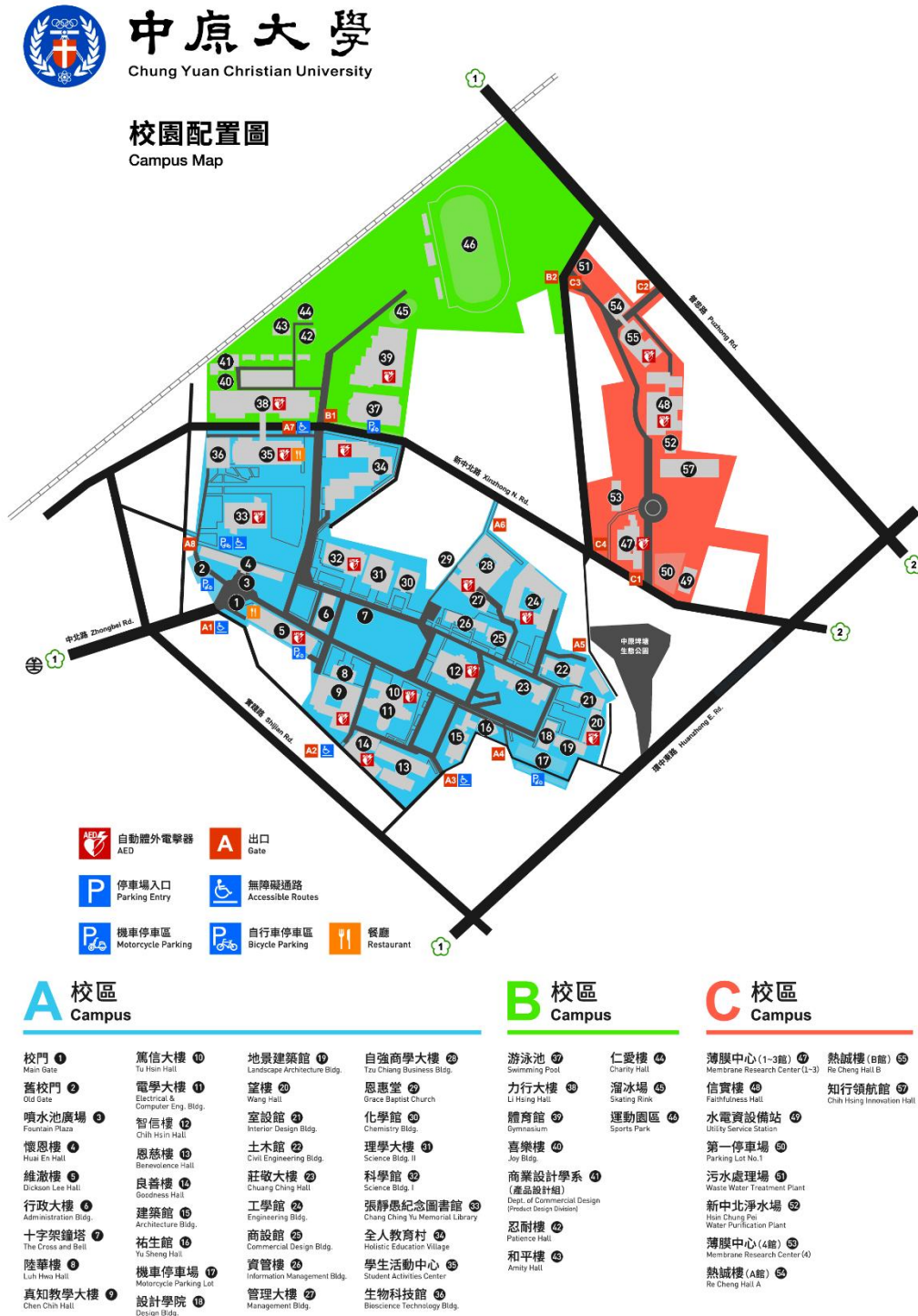
☐ 否

☐ 是

12. 其他想與本團隊說明的內容？

送出

附錄二：中原大學校園配置圖



附錄三：宿舍群組與 Dcard 中原大學版



