國立臺東大學資訊管理所碩士班

碩士論文

Department of Information Science and Management Systems National Taitung University

Proposal of Master Thesis

多因子認證保護帳號使用行為意圖影響因素之探討：計畫行為理論與保護動機理論之整合觀點

Exploring Factors Influencing Behavioral Intentions towards Multi-Factor Authentication: An Integrated Perspective of Theory of Planning Behavior and Protection Motivation Theory

學生：曾善勤 撰

Graduate Student: Shang-Chin Tseng

指導教授：陳宜樫 博士

Advisor: Yi-Cheng Chen, Ph.D.

中 華 民 國 一一三 年一月

January, 2024

國立臺東大學資訊管理所碩士班

碩士論文

Department of Information Science and Management Systems National Taitung University

Proposal of Master Thesis

多因子認證保護帳號使用行為意圖影響因素之探討：計畫行為理論與保護動機理論之整合觀點

Exploring Factors Influencing Behavioral Intentions towards Multi-Factor Authentication: An Integrated Perspective of Theory of Planning Behavior and Protection Motivation Theory

學生：曾善勤 撰

Graduate Student: Shang-Chin Tseng

指導教授：陳宜樫 博士

Advisor: Yi-Cheng Chen, Ph.D.

中 華 民 國 一一三 年一月

January, 2024

國立臺東大學
學位論文考試委員審定書

系所班：資訊管理學系

本班 曾善勤 君

所提之論文 多因子認證保護帳號使用行為意圖影響因素之探討：計畫行為理論與保護動機理論之整合觀點

業經本委員會通過合於 ☑ 碩士學位論文 ☐ 博士學位論文 條件

論文學位考試委員會：

（學位考試委員會召集人）

（指導教授）

論文類別（請勾選）：
☑學位論文
☐代替學位論文：
（☐藝術類 ☐應用科技類
☐體育運動類）
1.☐專業實務報告
2.☐技術報告
3.☐作品(連同「書面報告」)
4.☐成就證明(連同「書面報告」)

論文學位考試日期：113 年 1 月 11 日

國立臺東大學

附註：本表一式二份(正本)經學位考試委員會簽名後，分別送交系所辦公室及註冊組存查。

National Taitung University

國立臺東大學
學位論文網路公開授權書

重要事項說明：依著作權法第十五條第二項第三款規定，「依學位授予法撰寫之碩士、博士論文，著作人已取得學位者，推定著作人同意公開發表其著作」。本校圖書資訊館就紙本學位論文之閱覽服務依前開規定，採公開閱覽為原則。如論文涉及專利事項、機密或依法不得提供，需延後公開紙本論文者，請另行填寫本校「學位論文延後公開申請書」。(申請書得自本館網站下載)

本授權書所授權之 ☑**學位論文** ☐**書面報告** ☐**技術報告** ☐**專業實務報告** 為本人在

國立臺東大學 資訊管理 系(所) ______ 組 112 學年度

第 二 學期取得（☑碩士 ☐博士）學位之論文。

論文名稱：多因子認證保護帳號使用行為意圖影響因素之探討：計畫行為理論與保護動機理論之整合觀點

本人上列依學位授予法取得學位之論文電子全文(含書目、摘要、圖檔、影音資料、附件等，以下同)，依著作權法非專屬、無償授權予下列授權使用單位，得因教育、科學及研究等非營利用途，不限期間與次數重製，並得將電子全文收錄於數位資料庫，透過自有或委託代管之伺服器、網路系統或網際網路向授權使用單位圖書館館內及館外之使用者公開傳輸，提供該使用者為非營利目的之檢索、閱覽、下載及列印。

授權使用單位	電子全文於網路公開時程			
國立臺東大學	(依據 108 學年度第一學期第 3 次行政會議決議：研究生畢業論文延後公開上網時程，至多以三年為原則)			
	☑立即公開	☐一年後公開	☐二年後公開	☐三年後公開
國家圖書館	☑立即公開	☐一年後公開	☐二年後公開	☐三年後公開
	☐不同意公開			

本授權書所定授權，均為非專屬且非獨家授權之約定，本人仍得自行或授權任何第三人利用本著作。上述授權內容均無須訂立讓與及授權契約書。依本授權所為之收錄、重製、發行及學術研發利用均為無償。**<u>上述同意與不同意之欄位若未勾選，本人同意視同同意授權</u>。**

學　　號：10801306　(務必填寫)

研究生簽名：曾善勤　(親筆正楷)

指導教授簽名：　(親筆簽名)

日　　期：中華民國 113 年 1 月 24 日

本授權書(得自本校圖書資訊館網站下載)，請勿自行變更本授權書內容及格式，並以黑色字體撰寫後複印裝訂於審定書之次頁；授權書正本於畢業離校時，連同紙本論文一併繳交至圖書資訊館。

授權書版本: 2022/01/13

謝誌

有時候返歸臺東海岸住處的路上，沒有明燈、沒擦肩而過的路人、披星戴月的疲憊，途中沿著大學路與知本路呆望明月與漫天星，偶爾是東海岸專屬的日出昕曙，夜車旅途既孤獨又疲憊，但我仍很享受夜車時光，車殼提供無人打擾的安全感，幽暗車室中只有音樂、清唱、引擎、懸吊聲以及半放空的頭腦，不免尋思著人生意義：五年可以如何塑造一個人類？

從躊躇滿志幸福的天真青年變成冷淡務實的經商大叔，其中曲折的故事皆隨飯酒而去。其實寫論文不怎麼難，給任何人足夠的時間都能辦好任何事，但主要問題是心魔，每人都有各自的心魔，我的是從小到大的 issue，拖延與消極抵抗，有趣的是碩論正好都與之相違背，完成碩士學位更像是挑戰心魔以至於塑造人格的過程，畢竟資訊領域研究隨時都可能過時，但人格塑型是永久的。

很多人質疑碩士應該兩年畢業為何讀到四五年？對，我走了彎路，並且堅持全程走完不抄捷徑，感謝路途中遇到的所有人，無論好壞：謝謝兩年陪伴過程中有意或無意間教會我人生哲理的林小姐；謝謝我的朋友們，給予祝福鼓勵與意見；感謝正道行張頭家，感謝張信和老闆賞識並給予許多真知灼見，助我 men up 一步一步成為一位生意人；感謝陳宜樫指導教授支持以及提供寶貴的學術意見，謝謝老師不厭其煩地指教以及安排各項學術過程；謝謝各位學位審查委員的專業意見以及謝謝系辦阿姨協助通過畢業手續。最終，最最最感激我的生養母親，史偉珍，單親把一位熊孩子好手好腳地拉拔長大著實不易，尤其還是食量如熊比其他人大三倍的熊孩子，在不富裕的時空與際遇使我經濟無憂地完成高等學位。

要謝的太多，感謝天吧，謝謝這個世界線的一切量子震盪原子碰撞，巧合地生成出一位 27 歲碩士畢業身兼萬室屋老闆的曾善勤。

曾善勤 謹誌

國立台東大學資訊管理學系碩士班

中華民國一一四年一月

摘要

資料洩漏手法推陳出新，網路攻擊規模逐年增長，尤其 Covid-19 疫情造就遠距生活普及化使得資料外洩的風險急遽上升，是故加強資安技術、普及部署、深化資安素養有其必要性。多因子驗證乃最常見的資安加強手段之一，其早已行之有年，直觀、多樣化、高性價比等特性深受資訊敏感族群青睞；然而在網路犯罪如此猖獗的今日，多因子驗證在普羅大眾之中仍不見其普及化，遂為本研究欲詳加探討研究之主題。

本研究針對各大平台網路使用者對於多因子驗證的採用因素深入探討，根據多國各學術領域文獻資料收集、解析、彙整，以計畫行為理論為基礎，佐以保護動機理論建構出具有分析風險特色的計畫理論模型，藉以深入探究網路使用者對於資訊安全危機的認知程度，以及為了確保資訊安全而採用多因子驗證技術之關鍵影響因素。

通過多種不同管道發放問卷，本研究徵得 303 份有效樣本，依據性別、年齡、職業別、教育水平等特性分析可發現樣本族群相當分散，樣本數有限的狀態下造就本研究模型部分構面 R 平方值略低，若能擴增樣本數將能改善；而迴歸分析研究則顯示大多構面間假說呈現強顯著影響，其中甚有假說不成立但呈現超出預期之強烈顯著性，其餘則印證了社會科學領域先進 Hovland 等人所提出之威脅期望理論。

本研究統計分析結果顯示感知威脅可能性、反應有效性此兩自變數皆對行為意圖造成顯著影響，而感知威脅嚴重性則影響不明顯；研究中預期適應不良獎勵此構面對於態度、行為意圖兩構面將造成負面影響，然而其負向強顯著結果出乎預料，表示多因子驗證技術雖造成網路使用過程中多出額外手續，但絲毫不影響普羅大眾對多因子驗證的接受度。根據基本資料統計則另發現：「對多因子驗證技術的認識程度」與使用意圖具有高度相關，若在推廣過程中能將多因子驗證介紹得更詳細、簡顯易懂、更普及、勿一昧只針對威脅嚴重性宣導而是綜合各項構面而進行教育，可以預期將會有效地推廣多因子驗證此資安保護措施。

關鍵詞：資訊安全、多因子驗證、計畫行為理論、保護動機理論

Abstract

With new methods of data leakage, the scale of cyberattacks growing year by year, and the Covid-19 epidemic making remote living commonplace, the risk of data leakage has risen sharply, so there is a need to strengthen security technology, popularize its deployment, and deepen the quality of information security. Multi-factor authentication is one of the most common means of information security enhancement, which has been practiced for years, and its intuitive, diverse, and cost-effective features have been favored by information-sensitive groups; however, in today's world where cybercrime is so rampant, multi-factor authentication is still not popularized among the general public, which is why this study is intended to explore the topic of research in detail.

This study focuses on the in-depth exploration of the adoption factors of multi-factor authentication by Internet users on various platforms. Based on the collection, analysis, and compilation of literature from various academic fields in many countries, a theoretical model of the plan with risk analysis characteristics is constructed based on the theory of planned behavior and supported by the theory of protective motivation in order to deeply explore the level of Internet users' awareness of the crisis in information security and their adoption of multi-factor authentication technology in order to ensure the security of their information. The program's theoretical model with risk analysis features was constructed in order to deeply investigate the level of awareness of Internet users on information security crisis and the key influencing factors of the multi-factor authentication technique adopted to ensure information security.

Through various channels of questionnaire distribution, this study obtained 303 valid samples. According to the characteristics of gender, age, occupation, education level, etc., it can be found that the sample group is quite dispersed, and the limited number of samples has resulted in a slightly low R-square value for some of the components of the model, which will be improved if the number of samples can be increased; and the regression analysis study shows that most of the hypotheses among the components show a strong significant effect, and some of them are not valid but show more than expected effects. The regression analysis showed that most of the inter-factorial hypotheses showed strong significant effects, some of which were not valid but showed strong significance beyond expectations, and the rest of them confirmed the threat expectancy theory proposed by Hovland et al, a pioneer in the field of social sciences.

The statistical analysis of this study showed that the two independent variables of perceived threat likelihood and response validity had a significant effect on behavioral intention, while the effect of perceived threat severity was not significant. It was expected that the maladaptive reward component would have a negative effect on attitude and behavioral intention, but the negative result was unexpected, which indicated that the multifactor authentication technology caused additional procedures in the process of Internet use, but did not affect the general public. However, the negative result is unexpected, indicating that although multi-factor authentication technology causes additional procedures in the process of Internet use, it does not affect the acceptance of multi-factor authentication by the general public. Based on the basic statistics, it was also found that "awareness of multifactor authentication technology" was highly correlated with the intention to use it. If multifactor authentication can be introduced in a more detailed, easy-to-understand, and popularized manner during the promotion process, and if education is not focused on the severity of the threat, but rather on the integration of various components, it can be expected that multifactor authentication will be effectively promoted as a security protection measure.

Keywords: Information Security, Multi-factor authentication, Theory of Planned Behavior, Protection Motivation Theory

目錄

摘要 I

Abstract II

目錄 IV

表目錄 VI

圖目錄 VII

第一章 緒論 ..... - 1 -

1.1 研究背景與動機 ..... - 1 -

1.2 研究目的與研究對象 ..... - 5 -

1.3 研究流程與論文架構 ..... - 6 -

第二章 文獻探討 ..... - 8 -

2.1 資料外洩定義及近年趨勢 ..... - 8 -

2.2 零信任架構（Zero Trust Architecture, ZTA） ..... - 10 -

2.3 多因子驗證 ..... - 11 -

2.4 計畫行為理論 ..... - 14 -

2.5 保護動機理論 ..... - 18 -

第三章 研究方法 ..... - 20 -

3.1 研究架構與假設 ..... - 20 -

3.1.1 感知威脅期望 ..... - 22 -

3.1.2 反應有效性 ..... - 25 -

3.1.3 行為態度 ..... - 26 -

3.1.4 主觀規範 ..... - 27 -

3.1.5 知覺行為控制 - 28 -
3.1.6 適應不良獎勵 - 30 -
3.1.7 行為意圖 - 32 -
3.2 操作型定義 - 34 -
3.3 問卷設計 - 35 -
第四章 研究資料分析 - 39 -
4.1 受測者樣本描述 - 39 -
4.2 描述性統計分析 - 44 -
4.3 測量模型檢定分析 - 49 -
4.4 研究假說與模式驗證 - 51 -
第五章 結論與建議 - 56 -
5.1 研究結論 - 56 -
5.2 研究建議 - 59 -
5.3 研究限制與未來展望 - 60 -
參考文獻 - 61 -
中文部分 - 61 -
外文部分 - 63 -
網路文獻 - 71 -
附錄(本研究問卷問卷） - 75 -

圖目錄

圖 1.2019 至 2021 年網路攻擊趨勢統計 ..... - 2 -
圖 2.於私人帳號重複使用密碼習慣與雙因子驗證 ..... - 4 -
圖 3.研究流程 ..... - 7 -
圖 4.2012/1/1 至 2022/2/7 資料外洩統計 ..... - 8 -
圖 5.以貝式定理簡釋雙因子驗證降低受駭機率 ..... - 11 -
圖 6.理性行為理論(TRA)模型 ..... - 14 -
圖 7.計畫行為理論 ..... - 16 -
圖 8.新版計畫行為理論 ..... - 17 -
圖 9. 保護動機理論架構圖 ..... - 19 -
圖 10.初始研究架構圖 ..... - 21 -
圖 11.保護動機理論模式圖 ..... - 22 -
圖 12.威脅期望值理論決策流程圖 資料來源:作者自繪 ..... - 23 -
圖 13. 常用網路服務長條圖 ..... - 43 -
圖 14. 網路使用時數統計圓餅圖 ..... - 43 -
圖 15. 本研究模型統計路徑分析 ..... - 55 -
圖 16. 本研究修正模型 ..... - 58 -

表目錄

表 1. 驗證因素簡介表 ..... - 12 -
表 2.操作型定義彙整 ..... - 34 -
表 3.問卷的各構面之衡量題項 ..... - 36 -
表 4.受測者性別資料分析表 ..... - 39 -
表 5.受測者年齡資料分析表 ..... - 40 -
表 6.受測者教育程度資料分析表 ..... - 41 -
表 7.受測者職業別資料分析表 ..... - 42 -
表 8.敘述統計分析 ..... - 44 -
表 9.構面敘述統計分析 ..... - 45 -
表 10.反應有效性構面敘述統計分析 ..... - 45 -
表 11.態度構面分析 ..... - 46 -
表 12.主觀規範構面敘述統計分析 ..... - 46 -
表 13.適應不良獎勵敘述統計分析 ..... - 47 -
表 14.知覺行為控制敘述統計分析 ..... - 47 -
表 15.使用意圖敘述統計分析 ..... - 48 -
表 16.本研究模式變數之信度、效度整理表 ..... - 49 -
表 17.構面之相關係數與鑑別效度 ..... - 51 -
表 18.本研究假說檢定之整理表 ..... - 54 -

第一章 緒論

本研究旨在結合行為計畫理論與保護動機理論，以探討大眾對於多因子驗證的採用因素。本章分成四節，第一節為研究背景與動機；第二節為研究目的與研究對象；第三節為研究流程與論文架構。

1.1 研究背景與動機

自從人類祖先獲得溝通能力，訊息該如何傳遞、保密、破解便是無盡的盾矛攻防戰。遙想公元前一世紀羅馬共和時期的凱薩加密法(Suetonius, 110)，是相當直觀的加密技術，但在該年代可確保高度敏感的軍令無妨遭到竊窺甚至盜取，直至八百年後才由頻率分析法所輕易破解(Kahn, 1996)。恩尼格密碼機串流加密法耗費盟軍將近二十年(1926~1942)的功夫，在取得技術、密碼機、密碼本的同時，還得在加密員多次犯下錯誤的操作等多種條件之下才有機會破譯(COCHRAN, 1981)。冷戰時期兩大強國之間的軍備競賽與太空競賽之下，計算機科技與網路技術飛速見長，爾後演變為電腦時代乃至於資訊時代(NSF, 1995)，莫爾定律之下科技更迭，加密法與解密法之間的攻防步調亦加飛快，例如 MD5 問世十七年後家用電腦運算數秒即可破解(Tao, 2009)、SHA1 從誕生到被發現漏洞的時程減為十年(Schneier, 2005)。 一種加密法從問世到相應破解技術誕生由原先耗費八百年、三十年，十七年、十二年、最後短至十年，有逐漸縮短的趨勢，說明加密法在資安攻防戰中逐漸處於下風。

而「資訊安全」除了加密技術的演進外，資訊在輸送、保存等環節的安全與否還得仰賴使用者對於資訊科技的認知深度以及資安意識(Candrick, 2021)。資料如何輸入、存放在哪、如何存放、如何輸送、如何接收、如何輸出.....等層面皆有文章，從西元前上千年仰賴傳令跑腿乃演化至現代無線通訊技術，從「達文西密碼」般層層謎語加密乃遞嬗至現代利用每秒上億次電腦算力在多種演算法前仆後繼的演化之下加密技術愈趨複雜。然而，再強勁的加密技術恐仍敵不過使用者的大意疏忽，例如二次世界大戰時期德軍犯下多重錯誤導致滴水不漏的恩格爾加密法失

守(COCHRAN,1981)、人的天性本來就好逸惡勞，帳號密碼的命名大多傾向方便好記為主，現代電子產品使用者仍可能以單純數字組合或生日抑或單字作為密碼，以至於容易遭到瞎猜矇中，甚至會同一組帳號密碼重複使用在多個場合(Brown& Bracken, 2004; Gaw & Felten, 2006; Chun et al., 2018)，一旦其中一個場域遭到資料洩漏，其他平台的帳號也會跟著遭殃(Dastane, Bakon & Johari, 2020)；倘若再疏於防範木馬軟體、網路釣魚、側錄等惡意攻擊，再嚴密的加密技術都形如虛設(徐韻修，2018；iThome, 2021；Schulze, 2023)。

ATTACK VECTOR TRENDS	2021	2020	2019
Cyberattacks	1,613	878	928
Phishing/Smishing/BEC	537	383	490
Ransomware	321	158	83
Malware	139	104	112
Non-secured Cloud Environment	23	51	15
Credential Stuffing	14	17	3
Unpatched software flaw	4	3	3
Zero Day Attack	4	1	n/a
Other - not specified	436	161	222
NA	106	n/a	n/a
Human & System Errors	179	152	231
Failure to configure cloud security	54	57	56
Correspondence (email/letter)	66	55	89
Misconfigured firewall	13	4	4
Lost device or document	12	5	19
Other - not specified	34	31	63
Physical Attacks	51	78	118
Document Theft	9	15	19
Device Theft	17	30	57
Improper Disposal	5	11	14
Skimming Device	1	5	4
Other - not specified	19	17	24
Unknown	12	n/a	2

圖 1. 2019 至 2021 年嚴重網路攻擊事件次數統計

資料來源：ITRC 2021

自從 2019 年的全球大疫情 Covid-19 造就了大蕭條，逼得人們各自繭居並賴以網路維繫日常生活，根據 Deloitte 德勤瑞士風險諮詢總監 Cedric Nabe 報告指出：疫情期間因社會整體比以往更仰賴網路以維持運作，眾人必須遠距工作、交際、採購、辦事、交易等，然而家用級資安防護遠不及企業級因而造就其一破口；其二，在家工作受到的干擾變多，也導致網路使用者注意力受到分散因而疏漏應有的資安規範；其三，員工不依規範使用 VPN 虛擬專用網路也是重大風險之一；再者，

員工使用個人電子裝置存放或傳輸機密資料而非使用公務裝置，或使用公務裝置執行私人事務(Fortinet, 2023)，更添增了資安風險；然，駭客可以根據以上種種漏洞取得蛛絲馬跡，拼湊出某企員的完整身分資料並取得相關憑證，找出系統漏洞或頂冒著別人網路身分大肆為非作歹。根據行政院《110 年國家資通安全情勢報告》以及身分竊盜資源中心(ITRC)近三年來的年度數據洩露報告都指出：自從 Covid-19 疫情網路攻擊不管是次數、規模、層級都有惡化後居高不下的趨勢(行政院，2021；ITRC, 2020、2021、2022)，圖 1 所示為 ITRC 統計 2019 年、2020 年、2021 年的重大網路攻擊事件次數統計，可見網路攻擊次數有明顯增加趨勢。

自 Covid-19 疫情前，根據國內電腦週刊 iThome、獨立研究機構 Ponemon Institute、國外資安平台 Fortinet、Cybersecurity Insiders、全球領先科技電信公司 Verizon、國際會計顧問公司德勤 Deloitte Touche Tohmatsu 等機構的研究報告皆指出:資安威脅大多從內部可防可控。例如內部人員的不當操作、疏忽、受干擾、惡意、不良的密碼衛生習慣、欠缺資安意識等因素而承受網路釣魚、社交工程、Drive-by Compromise、字典攻擊.....等攻擊手法的騷擾(Mitnick,2001;Mouton & Leenen & Venter, 2016; De Backer, 2023; Ozkaya, 2018)，尤其 Covid-19 疫情促增網路使用量並連帶網路攻擊事件暴增(ITRC, 2021; Saleous et al., 2022)，根據 FBI 網路部門主管 Tonya Ugoretz 於 2020 年四月於網路討論會上指出「2020 初疫情期間，網路犯罪部門接到的投訴頻率竟然暴增達到平常的四倍(The Aspen Institute, 2020)」，其中大多來自於受害者警覺性不足以至於遭駭，畢竟人類。套句俏皮話：「就算配備再嚴密的門鎖，只要使用者沒把門鎖好就仍可能被闖空門！」

根據美國市場研究和分析公司哈里斯民意調查(Harris Poll)與 Google 合作的 3000 人規模問卷指出 65%受試者皆會同一密碼用於多組帳號，而其中把同一組密碼套用於名下所有帳號者竟有 13 個百分點之譜！再根據資安研究中心 Ponemon Institute 於 2020 年初出版的密碼與驗證安全行為報告，統計了 2,507 位資安人員與 563 位一般受訪者作為對照。如以下圖 2 柱狀圖所示，研究發現，雖然在「是否有套用二段試驗」題目中可發現，資安人員僅多出一般受試者 4 個百分點會套用二段式驗證；而在「私人帳戶重複使用密碼行為」方面，資安人員表達有重複使用密碼的答覆率高達半數之譜，僅少於一般受試者 4 個百分點，比例相去不遠，由此可

知無論從事身分，人性終究是懶惰的，而也因懶惰而可能造成疏忽乃至於意外(Whitney, 2019)。

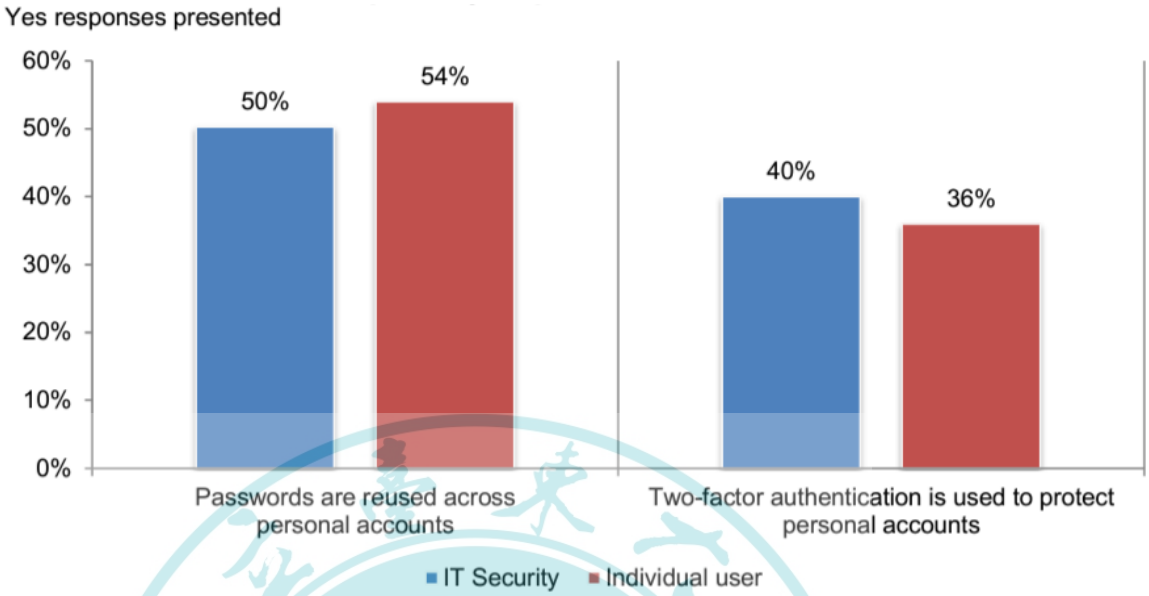

圖 2.於私人帳號重複使用密碼習慣與雙因子驗證－資安人員與一般受訪者作對照

資料來源：Ponemon Institute

是故，與其思索如何改進加密演算法、提升加密技術複雜度，不如探究並增進人員的資安意識顯然是直觀、實惠又有效的改進方案(Cho.et al., 2018；Herath and Rao, 2009)。若能輔以多因子驗證（Multi-Factor Verification）將能顯著的降低被入侵的風險，並大幅增加資訊安全度(Ometov et al., 2018; Wang et al., 2017; 朱惠中，2021; Li, 2022)，根據 Google1.5 億新帳號申請過程強制套用二段式驗證的案例則發現: 此舉可減少 50%的帳戶受害案件數(Fitzpatrick, 2022)；然而實際上根據大型社交平台 Twitter 和多份研究皆指出使用多因子驗證的用戶比率並不高，依各報告指出採用率最低至僅 2.5%(Twitter, 2021; Petsas et al., 2015; Glyer, 2022)，至於眾人皆曉的 Microsoft 則表示只有 22%用戶採用多因子驗證(Comeau , 2022)，另一方面解析受駭案例中高達 99%都未採用多因子驗證(Walker & Weinert, 2020)。便宜有效的防盜措施卻不普及實屬矛盾，值得研究探討其背後成因。

綜上所述，探討認知行為科學的主流是使用計畫行為理論(Theory of Planned Behavior)來解釋，而資安危害屬於風險，若能輔以防護動機理論(Protection Motivation Theory)此等恐懼訴求的理論佐以詮釋將會是有意思的研究角度。

1.2 研究目的與研究對象

歸納總結上節所述，告訴了我們兩件趨勢: 其一，僅仰賴複雜的加密技術仍不足以保護資料，人為因素佔有重大成分(Musthaler, 2006)；其二，單純的帳號密碼組合已不足以保證資訊安全，還需要參與更多驗證媒介以保證資訊安全性，例如多因子驗證(Multi-factor authentication)，而多因子驗證也的確在資安戰略上取得顯著成效，擋下資訊攻擊至少的成功率 7 成(Flynn, 2023)。

本研究欲探討。本研究以 Ajzen 於 1991 年提出的計畫行為理論(Theory of Planned Behavior) 為理論基礎，並將取自保護動機理論(Protection Motivation Theory)(Rogers, 1975)的變項置入其中，使之具備適應性反應的預測性。樣本界定為各大網路平台(如 Google、Apple、Facebook、Instagram…etc)使用者為主要研究對象，問卷抽樣對象不限於已知並已採用多因子驗證乃至於不知曉多因子驗證者。本研究主要研究目的簡述如下:

一、探討計畫行為理論如何與保護動機理論相互結合，並產出具備風險評估導向的研究模型。

二、以上述研究模型探討網路使用者對於採用多因子驗證的要素，哪些因素孰強孰弱方能根據研究結果提出結論與建議，以供後續研究之參照。

1.3 研究流程與論文架構

本研究的研究流程如圖 3 所示，為了達到研究目的，我們將研究分為五個章節。

第一章緒論將針對世界脈絡汲取出研究背景與動機，網羅國內外相關文獻、期刊、研究報告、報導等資料後指引出問題所在，以及歸納出最適當的解決方案。影響使用者對於採用多因子驗證之前置因素進行了解統整與分析，並根據統整後的文獻資料提出適切本研究的研究模型、架構與研究方法。

第二章文獻回顧以前章的論述一一詳解專有名詞。並逐一解說本研究即將採用的整合式模型中各個要素。本研究模型以 Ajzen 提出的計畫行為理論 (Theory of Planned Behavior)1988 年版本作為原型，並將 Rogers 提出的保護動機理論 (Protection Motivation Theory)中的恐懼訴求組件，例如：感知威脅嚴重性(Perceived Threat Severity) 、感知威脅可能性(Perceived Threat Vulnerability)、反應有效性(Response Validity)整合其中作為受試者感知威脅後影響計畫行為的自變數，並提出假說。

第三章研究方法將以前兩章的脈絡、文獻回顧統整出假說、研究架構、問項，方能提出問項定義以及問卷設計；再者決定資料分析方法及工具。

第四章資料處理與統計分析。隨著問卷設計與發放後，待問卷回收與彙整後，依循研究方法進行資料的統計分析，確認各迴歸路徑假說的確立與否。

第五章結論與建議。依照前章節的分析與假說確認給予結論與建議；評估本研究模型的預測能力、潛力與貢獻；並為未來欲鑽研相關題目的研究人員豎立基石、為資訊安全相關工作者指引建議、為資安政策工作者提供頭緒，資安路上有你有我共造福祉。

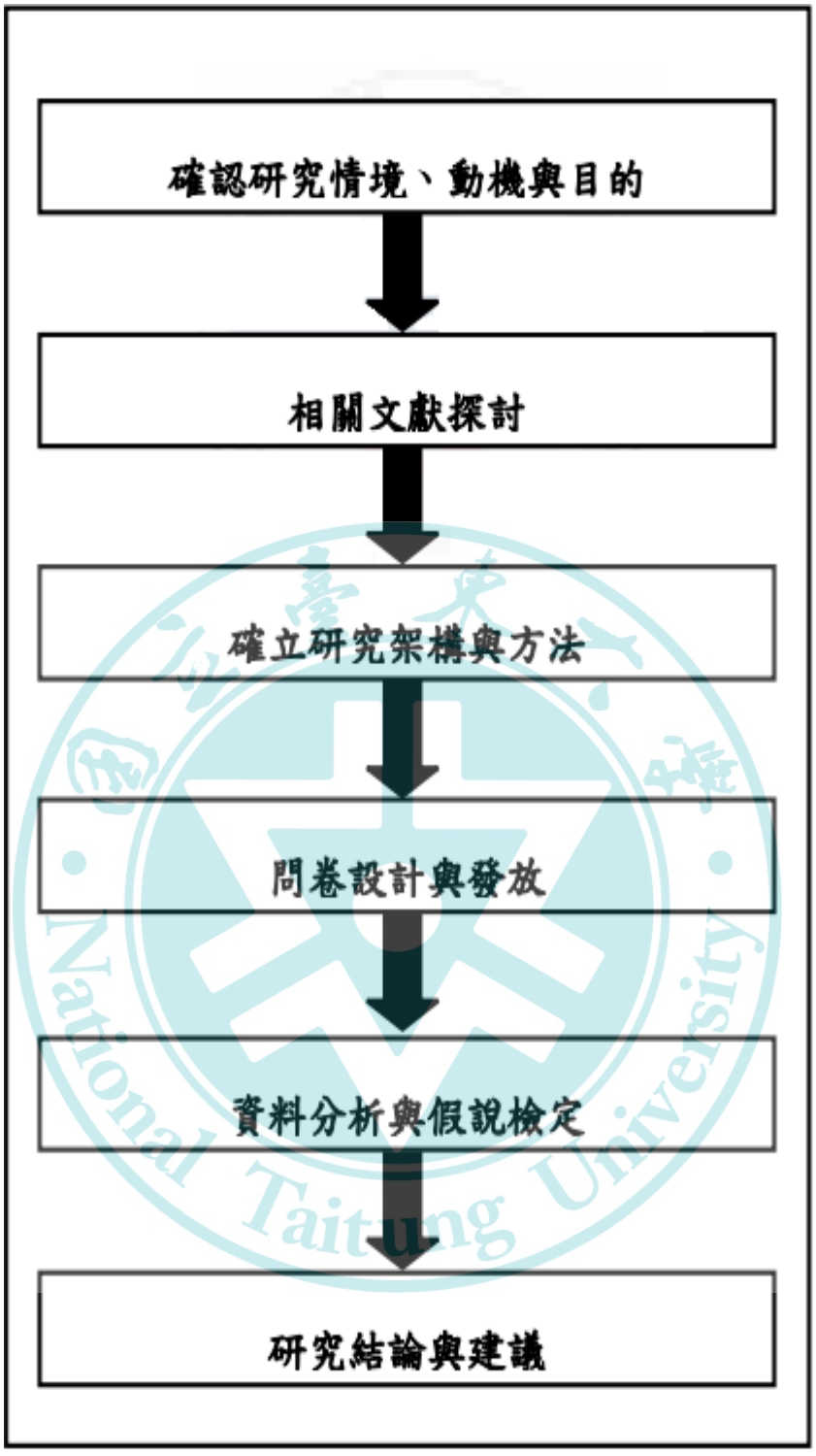

圖 3.研究流程

第二章 文獻探討

礙於篇幅限制，本文獻探討章節主要聚焦於本研究所鎖定的主題，故內容有一定指向性。透過相關文獻探討以瞭解各術語之定義、各構面之間的關聯、自變數與中介乃至於與依變數之間的相對待。本章分為5節，逐一詳解本研究的背景與研究工具。

2.1 資料外洩定義及近年趨勢

資料外洩定義為機敏資料遭到未經授權的存取、揭露、盜竊，可能遭到的機敏機料例如有個人姓名、生日、證件號、住址、電話、信用卡號、網路帳戶，以及商業資敏資料例如金流、商業機密、知識產權..... 等。(劍橋字典；ICO.；Verizon Business, 2021)資料外洩的元凶可以來自外部或內部人士、不可靠的程序、硬體設備或軟體；其媒介不限於電磁紀錄、攔截電磁波/電壓脈衝通訊、紙本、甚至於口語竊聽。(ACSC, n.d.)

資料外洩的手法從內部人員無意洩漏出去抑或惡意盜取、外部人員潛入或駭入都有可能。根據專門關注資料隱私權力問題的非營利組織Privacy Rights Clearinghouse的統計指出"主要的資料外洩手段來自外部駭客或惡意軟體，其次分別是意外披露(DISC)和欺詐(CARD)，內部攻擊(INSD)僅佔所有可識別的外洩事件5%，在所有外洩原因中排名第五"。

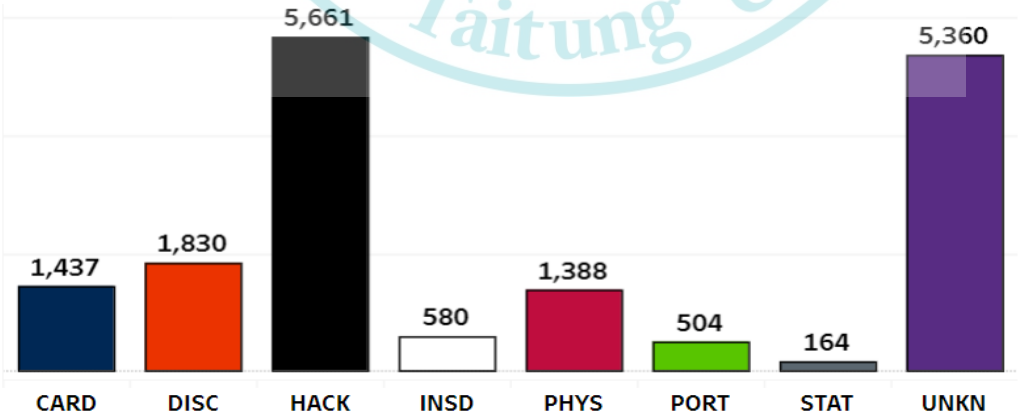

圖 4.2012/1/1 至 2022/2/7 資料外洩次數統計—以外洩原因分類
資料來源：Privacy Rights Clearinghouse

由此可知內部外洩發生率相當低，然而內部外洩有一舉端走整座資料庫的嚴重性(Ayereby, 2018)，例如健保署外洩11個情治系統的人員資料(林俊宏，2023)、戶政役全台個資外洩(鄭閔聲、史書華，2023)，更甚者如iRent以明碼保存58萬筆敏感個資並且資料庫不受密碼保護實屬離譜！為此問題，多國政府及私人機構大力提倡零信任架構（Zero Trust Architecture, ZTA）以絕類似情事發生(Whitehouse, 2021；美國國家安全局, 2021)。

2.2 零信任架構（Zero Trust Architecture, ZTA）

顧名思義，對任何人或封包甚至組織內成員都完全不信任，其架構核心理念基於「所有網路流量皆不受信任，因此資安人員必須驗證和保護所有資源，並限制、嚴格控制存取，還要檢查、記錄所有網路流量。(Kindervag, 2010b)」

早期網路防火牆屬「有邊界架構」，"外硬內軟"如同M&M巧克力豆，靠防火牆指望擋下來自外部的威脅，而牆內暢行無阻(Kindervag, 2010a)，然而一旦防火牆被突破將會是重大風險，經歷Covid-19改變了工作型態，更證實了傳統的防火牆邊界架構已不敷遠端化生活的防禦需求(Fan, 2023；翁浩正，2023)。再者，內部威脅也是重大的破防因素(陳育徽，2023)，因此絕不信任，一律驗證(WMware, n.d.)。此概念可追溯至John Kindervag於2010年著作《No more chewy centers: Introducing the zero trust model of information security》提出，2014年Google提出零信任設計與部署方法(Ward & Beyer, 2014)後，經過多年實踐，2020年更是推出BeyondCorp遠端存取服務，研究者於2018年有幸一覽國立臺東大學教育版Google雲端硬碟管理員介面，其管理員雖位於高級階層，但無法存取用戶在雲端硬碟中儲存的任何一筆資料，亦無從得知任一用戶帳戶個資，除了可從帳號推敲出學號/證號，任何資料業已去識別化。

美國國家標準技術研究所（NIST）及其他私人機構如 Gartner、Forrester、IDC 及 ESG 皆已提出定義零信任框架的基本原則，而本國、歐盟及各已開發國家皆也紛紛提出零信任架構轉型計劃(羅正漢，2023；行政院，2021；日本數位廳，202)，大型國際企業IBM也在資料洩漏財損報告《Cost of a Data BreachReport 2022》一書建議使用零信任架構以最小化資料洩漏所造成的財務損失。

零信任架構注重"驗證機制"，一如 Google Cloud 台灣技術副總經理林書平針對零信任架構的說明指出「讓正確的身分可以存取由正確程式碼授權的正確機器，並在正確時間與情境下，存取到正確的資料。」

由憑證確認使用者的存取權限尤為重要，而如前言所述，單純的帳號密碼組合已不可靠(Bonneau et al., 2015)，於是得佐以多道防護機制多管齊下，而多因子驗證正是合適解方(Saini, 2021)。

2.3 多因子驗證

「驗證(authentication)」是確認身分的必要手段，然而何謂「因子(factor)」呢?舉例來說，兩千年前泛用的「密語(cipher)」即是一種驗證因子(Churchhouse, 2002)，自60年代因終端機需要共享使用而發明「帳號密碼組合」其一驗證因子(Saini, 2021)，21世紀初的網際網路時代是大多讀者的少年或童年時期，常見的第二道認證因子大多是詢問個人私密問題例如「母親名字」、「生日」、「國小母校」.....等安全提問，於數學機率計算上確實能以貝式定理來證明(Papoulis & Unnikrishna Pillai, 2002；方景立，2016) ，假設一項因子的被破解機率為10%，兩件因子同時套用的機率則會驟降至1%(0.1×0.1=0.01)，因此同時將數個驗證因子串聯套用能降低被駭機率如圖5。

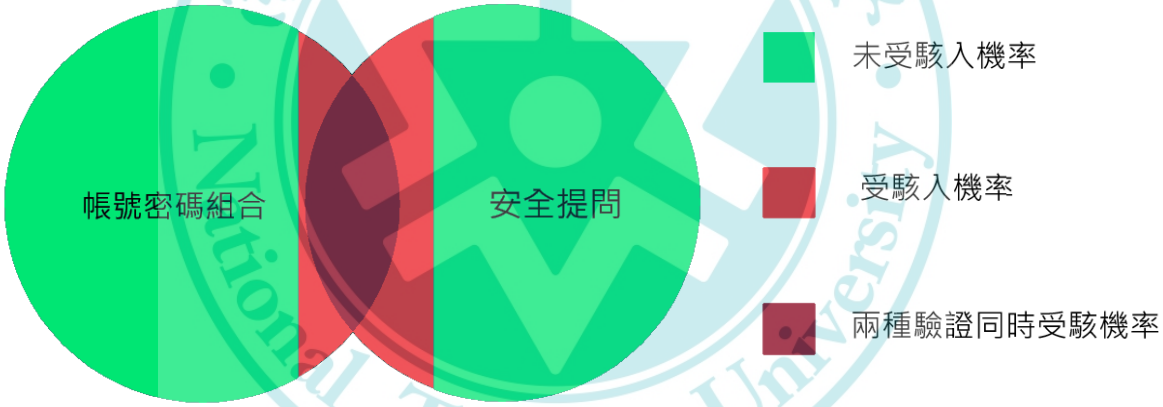

圖 5.以貝式定理簡釋雙因子驗證降低受駭機率

然而這套驗證組合完全將安全性託付於同個媒介－以兩項知識因子皆作用於鍵盤上，一但遭到鍵盤側錄將會門戶洞開，是故應該採用不同媒介的驗證因子才得以有效增強安全性(Ponnusamy et al., 2020)，以驗證媒介來分類可將驗證因子分為五大項(Rosencrance & Loshin & Cobb, 2020)，以下表1.為簡要整理:

表 1. 驗證因素簡介表

媒介種類	說明	範例
知識因子 (knowledge factor)	用戶證明知道某些秘密方能通過身份驗證	個人識別碼(PIN)、群組邀請碼、共享密鑰、圖形鎖、信用卡碼
擁有物因子 (possession factor)	持有特定物件以通過驗證	自然人憑證、FIDO、實體金鑰、手機認證、信用卡晶片、安全根
生物特徵因子 (biometric factor)	以使用者生理上的特徵作為驗證	指紋、虹膜、聲紋、面部辨識、擊鍵動態
位置因子 (location factor)	以使用者地理位置作為驗證	僅限用固定式裝置、GPS 定位、特定網域
時間因子 (time factor)	以特定時間作為驗證窗口	一次性密碼、限時驗證碼、特定存取時段

資料來源：Jacomme & Kremer, 2018；Van Tilborg & Jajodia, 2014；Meng-Yi Wu, 2020；FIDO Alliance, n.d.

理論上欲達到最嚴密的安全性，那以上所有驗證媒介種類都須至少套用一項驗證因子；然而實務上受成本考量與方便性的限制，大多驗證程序僅套用二到四項驗證因子，以大多數人的日常生活為例:

(1) ATM 領錢。此案例套用了三個因子

〔擁有物因子－信用卡晶片〕、〔知識因子－PIN〕、〔位置因子－固定式裝置 ATM〕

插入信用卡至特定 ATM，輸入密碼方能取錢。

(2) 網路信用卡付帳。至少套用了四個因子

〔知識因子－信用卡碼〕、〔擁有物因子－特定門號手機〕、〔生物特徵因子－指紋驗證〕、〔時間因子－一次性限時密碼〕

在網路付款的介面下，輸入信用卡號，傳送手機簡訊至特定門號的手機，內附一次性限時密碼，通常還會伴隨一次生物特徵驗證以證明是本人操作手機。

(3) LINE 電腦版登入。至少套用了三個因子

〔知識因子－電郵信箱與密碼〕、〔擁有物因子－已安裝 LINE 之手機驗證〕、〔時間因子－一次性限時密碼〕

輸入電郵信箱與密碼以登入，然而若要解密聊天室還需持有已登入該帳號的手機，輸入一次性限時密碼方能正常操作。

由此可見考量到成本、驗證準確度及速度、被駭風險、法規遵循、方便性等因素，將會影響各類使用情境將採用的驗證類別(李中仁，2018)。就原則而言，被駭風險越高，採用的驗證難度與成本也隨之提升(陳冠億，2020)，成本意味著代價，代價屬於損失的一種，而人天性就厭惡損失(Tversky & Kahneman, 1981)，可見人們對於多因子驗證的採用動機是理應存在阻力的，雖然多因子驗證可以大幅提升資訊安全性，然而也可能因為成本考量、信心因素、感知因素，例如個案認為太麻煩、覺得沒效、不會用、不懂、沒把握、覺得沒必要.....等原因導致許多人使用意圖不足不願意採用，遂為本研究探討主題。

2.4 計畫行為理論

計畫行為理論(Theory of Planned Behavior, TPB)係主要用以預測和瞭解人類的行為的理論框架，由Ajzen教授於1985年首度提出該決策模型，其理論基石可追溯至1975年Fishbein和Ajzen共同提出的著作《Belief, attitude, intention, and behavior: An introduction to theory and research.》 其著作定義出「態度」、「主觀規範」「信念」、「行為」、「意圖」等概念定義，為後續的學術發展奠定長遠基礎。

而後續1977年的著作《Attitude - behavior relations: A theoretical analysis and review of empirical research.》則以文獻與實證研究證明「態度」如何影響「意圖」連帶影響「行為」(Jones & Davis, 1965)，並解釋變數間產生相關性的原因，並可將其理論用於解釋其他概念之間的交互影響，再基於1968年Dulany的命題控制理論(Theory of Propositional Control)於是促生出了計畫行為理論的前身:理性行為理論(TRA, Theory of Reasoned Action)(Fishbein, 2008; Ajzan, 2012; Ajzen & Fishbein, 1980)。

理性行為理論(TRA)假設人類的行為是目標導向的(Heider, 1958; Lewin, 1951)，其決策過程具有理性、計畫、刻意等特點，而且在思考的過程當中會考慮行為的可能方案及各種期望的後果。(鍾易詩、翁士博，2014)

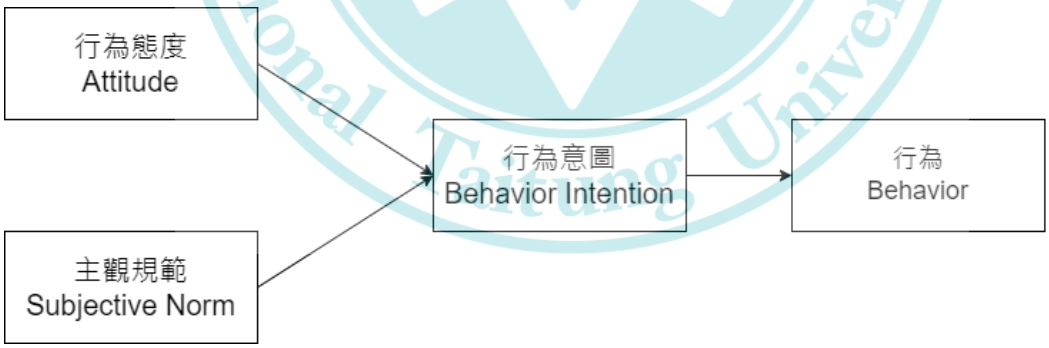

圖 6.理性行為理論(TRA)模型

資料來源:：Martin Fishbein & Icek Ajzen (1975)

在理性行為理論(TRA)模型中，「態度」、「主觀規範」兩項變數決定「行為意圖」至「行為」的綜合判斷路徑。而根據Sheeran & Paschal於2002年的綜合分析

指出，「行為意圖」和「行為」之間總體平均相關性高達0.53，也有越來越多證據表明「行為意圖」對「行為」有顯著的因果關係(Ajzen, 2020)。

以採用多因子驗證的情境下來舉例解釋：

- 「態度」(Attitudes)

  個人實行某特定行為的正向或負向的評價。

  「我認為多因子驗證好用/不好用。」

- 「主觀規範」(Subjective Norms)

  重要他人認為某人實行某特定行為的正向或負向的評價。

  「我的前輩/技術同事/親友/同儕認為多因子驗證好用/不好用。」

- 「行為意圖」(Behavioral Intention)

  個人想要採取某一特定行為的行動傾向。

  「我有多願意採取多因子驗證。」

- 「行動」(Behavior)

  個人採取某一特定行為。

  「受到先因素的影響，決定最後採用多因子驗證的意圖。」

個案舉例:

張大哥不了解何謂多因子驗證，對於是否該採用多因子驗證的態度舉旗不定；然而因為觀察他那就讀資管所的助理有在利用多因子驗證保護社群帳號並且推薦張大哥使用，於主觀規範上有顯著的正面評價，綜合考量之下正向影響了張大哥採用多因子驗證的行為意圖，於是最終 著手行動採用了多因子驗證以加強資訊安全。這段理性決策案例乍看之下合理，然而實際上理性行為理論的預測力差強人意(March, 1978; Coleman, 1990)，因為個體許多行為的實施需要具備一定的技能和知識，或者需要他人的合作；它可能需要克服諸如缺乏資金、時間或其他資源等障礙的能力。(Ajzan, 2020)

計畫行為理論(TPB)理論承襲了理性行為理論（TRA)之架構，並新增了「知覺行為控制 (Perceived behavioral control，PBC)」作為新變數。其中「對行為的態度」、「主觀規範」、「知覺行為控制」共同決定了「意圖」的強弱。

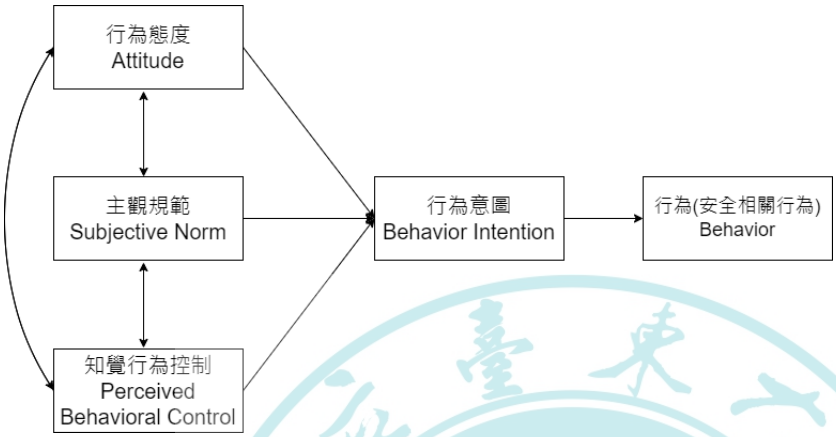

圖 7.計畫行為理論 資料來源: Icek Ajzen (1991)

- 「知覺行為控制」(Perceived Behavioral Control)

意指個人預期在採取某一特定的行為時，考量到成本、能力、名份、人脈、機會等各項資源，決定自己所感受到可以控制（或掌握）的程度。例如：張大哥意圖採用多因子驗證，但由於張大哥不熟悉資訊科技，不知如何啟用多因子驗證，家中也沒有能夠能協助指導的親友，於是在申請多因子驗證時頻頻卡關，就算申請成功後不曉得如何操作，於是無法登入帳號而感到困擾，因此拒絕使用多因子驗證。

由張大哥的案例可以窺見這就是所謂典型的「有心無力」、「道理我都知道，問題是辦不到」，也是原先理性行為理論(TRA)的最大盲點。僅因新增「知覺行為控制」一個決策因子即可以推翻原先理性行為理論的預測結果，當然這可能屬極端狀況。儘管知覺行為控制在部分研究領域、國家、人格、文化發揮的影響力不顯著，但仍能使得理論模型的整體預測結果更全面、更精準(Grandón et al., 2011；Engle et al., 2010)。

後續研究也發現「知覺行為控制」對於其他路徑有相當重要的調節作用，例如「知覺行為控制」的增強也會連帶增益「態度」至「意圖」的關聯強度、削弱

「主觀規範」至「意圖」之間的關聯強度(La Barbera & Ajzen, 2020)。由此可見「知覺行為控制」對於Ajzan與Fishbein的決策模型之完整性佔有重要地位，也使得計畫行為理論在社會科學類研究領域佔據一席之地。

Ajzen 於 2006 年提出更新版本，在原有變數之前新增了 3 項新變數，分別為：行為信念(Behavioral Beliefs)、規範信念(Normative Beliefs)、控制信念(Control Beliefs)。

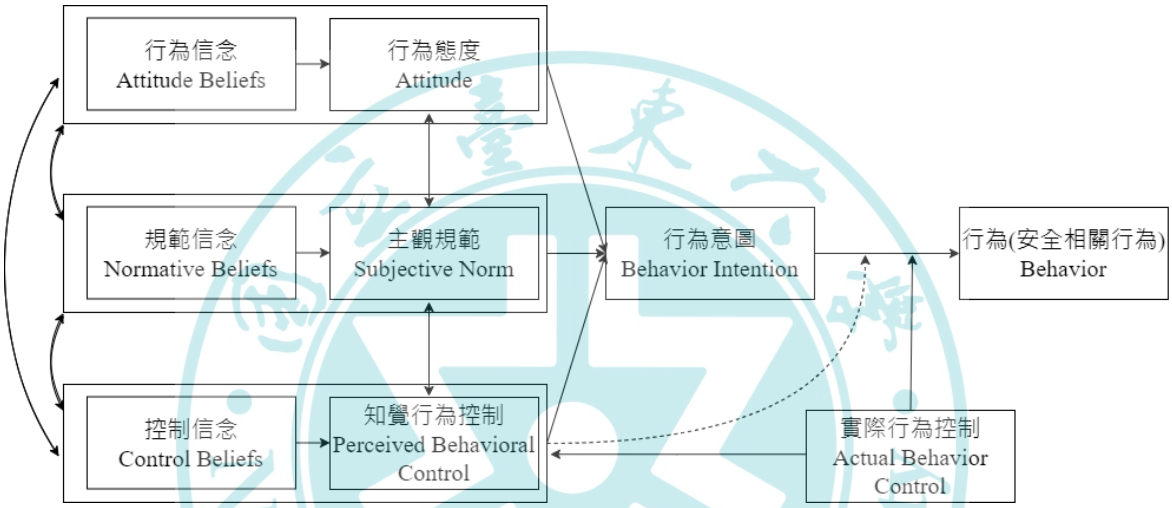

圖 8. 新版計畫行為理論 資料來源：Ajzen (2006)

- 「行為信念」(Behavioral Beliefs)

  對行為可能結果的信念以及對這些結果的評估

  「我認為這行為會有良好/不良後果」
- 「規範信念」(Normative Beliefs)

  對他人規範期望的信念以及遵守這些期望的動機

  「我覺得他人對這規範的看法重要/不重要」
- 「控制信念」(Control Beliefs)

  以及關於可能促進或阻礙行為表現的因素的存在以及這些因素的感知力量的信念

  「我認為自己能否輕易克服障礙」

2.5 保護動機理論

保護動機理論(Protection Motivation Theory,PMT)由Ronald W. Rogers 於1975年提出，後來Rogers 與 Prentice-Dunn (1997)陸續修訂，讓它能夠完整解釋個人在受到有害的威脅引起恐懼而產生保護自己的意圖(黃意雯，2022; Janmaimool, 2017）。

起初這套理論大多應用於促進健康、戒菸戒酒、生命安全行為、安全性行為、節省能源、保育瀕危生物等領域(Rogers & Cacioppo & Petty, 1983; Pagoto et al., 2004; Boer, 2005)。其有效的分析性及通用性很快地被應用至其他領域例如社會科學、認知科學、決策科學、心理學、資訊安全.....等領域廣泛應用的理論模型(Vance.et al.,2012)，其研究模型的主要特色是聚焦於恐懼性訴求(Fear Appeals)如何改變態度(Rogers, 1975; Maddux & Rogers, 1983)。

保護動機理論由九個因素構成，並以採用多因子驗證的情境下來舉例解釋：

- 「感知威脅嚴重性」(Perceived Threat Severity)

  個人感受到威脅所產生的傷害，其產生的嚴重程度。

  例：個案感受到資訊外洩有多嚴重、若發生將會造成多大損失。

- 「感知威脅脆弱性」(Perceived Threat Vulnerability)

  個人感受到威脅，並受到其傷害的可能性。

  例：個案感受到自己的資訊有多容易遭到外洩。

- 「適應不良獎勵」(Maladaptive Rewards)

  在威脅存在的情況下所能得到的獎勵。

  例：個案覺得在資安威脅情境下可以受到好處，例如詐領資安險、刻意讓資料外流散布以達成目的、自己本身就是駭客。

- 「害怕」(Fear)

  危險情境所產生的強烈的畏懼感。

  例：個案有多害怕威脅。

- 「反應效能」(Response Efficacy)

  個人對於採取某種保護行為是否可以減少威脅的認知。

  例：個案採取多因子驗證以防範資安威脅的能力。

- 「自我效能」(Self-efficacy)

  對於自己有能力採取保護行為的自信心。

  例：個案多有信心能應對資安威脅。

- 「反應成本」(Response Costs)

  採取保護行為所造成的相關成本，例如時間、金錢、精神等。

  例：個案為了防範資安威脅而採取多因子驗證所需的付出。

- 「保護動機」(Protection Motivation)

  為了使自身權益不受損害，而產生的心理傾向或內部驅力。

  例：個案有多願意採取多因子驗證。

- 「安全相關行為」(Security-related Behaviors)

  避免受到威脅、危險、危害、損失的行為。

  例：個案採取多因子驗證的投入程度。

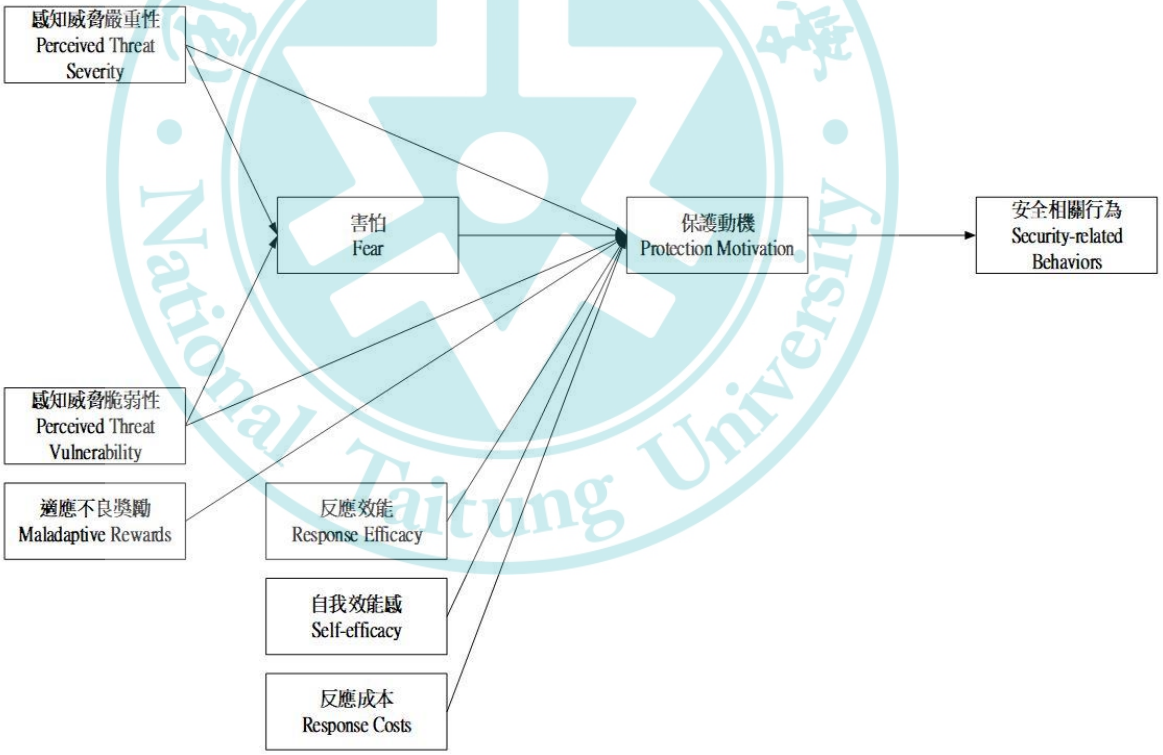

圖 9.保護動機理論架構圖

第三章 研究方法

根據第一章的緒論與第二章的相關文獻探討，整理脈絡後建構出本研究的研究架構，再進行問卷設計。本研究指基於保護動機理論中的疫情的認知影響感知威脅可能性與感知威脅嚴重性，整合基於計畫行為理論中的態度、主觀規範、知覺行為控制影響使用者行為意圖，使使用者行為意圖改變消費者行為，探討因素之間是否具有關聯性。

3.1 研究架構與假設

回顧文獻將保護動機理論(PMT)與計畫行為理論(TPB)兩相比對後可以發現：保護動機理論中的保護動機與安全相關行為與計畫行為理論的行為意圖和行動相呼應，各代表著個體的內隱信念以及外顯行為。而兩者明顯差異在於內隱信念的前置構面。

計畫行為理論(TPB)主重於解釋個體進行決策時對於自身以及別人眼光的心理衡量：

- 願不願意或看不看好？(態度)
- 別人怎麼看？(主觀規範)
- 能不能辦到？(知覺行為控制)

保護動機理論(PMT)主重於描述個體對於某種威脅的評估－反應過程：

- 這威脅多大、多嚴重？(感知威脅嚴重性)
- 被捲入這威脅的可能性多大？(感知威脅脆弱性)
- 在這場災害中有沒有機會獲益？(適應不良獎勵)
- 有多擔心受害？(害怕)
- 這招保護措施多有效？(反應效能)

- 使用這招保護措施要付多少代價？(反應成本)
- 有無信心好好地施展這招？(自我效能感)

本研究之首先目的是架構出計畫行為理論與保護動機理論相結合的研究模型，根據Icek Ajzen於1991年提出的計畫行為理論為基礎，再將保護動機理論(Rogers, 1975)的決策因子補充其中。「感知威脅脆弱性(Perceived Threat Vulnerability)」、「感知威脅嚴重性(Perceived Threat Severity)」、「反應有效性(Respond Vaildity)」、「適應不良獎勵(Maladaptive Rewards)」在原本的保護動機理論(PMT)可以解釋保護動機 (Protection Motivation)，在本研究中將會取用來補充解釋計畫行為理論(TPB)的「態度」、「主觀規範」、「知覺行為控制」、「行為意圖」，擴充出具有「評估特定危機並做出反應」的特性。

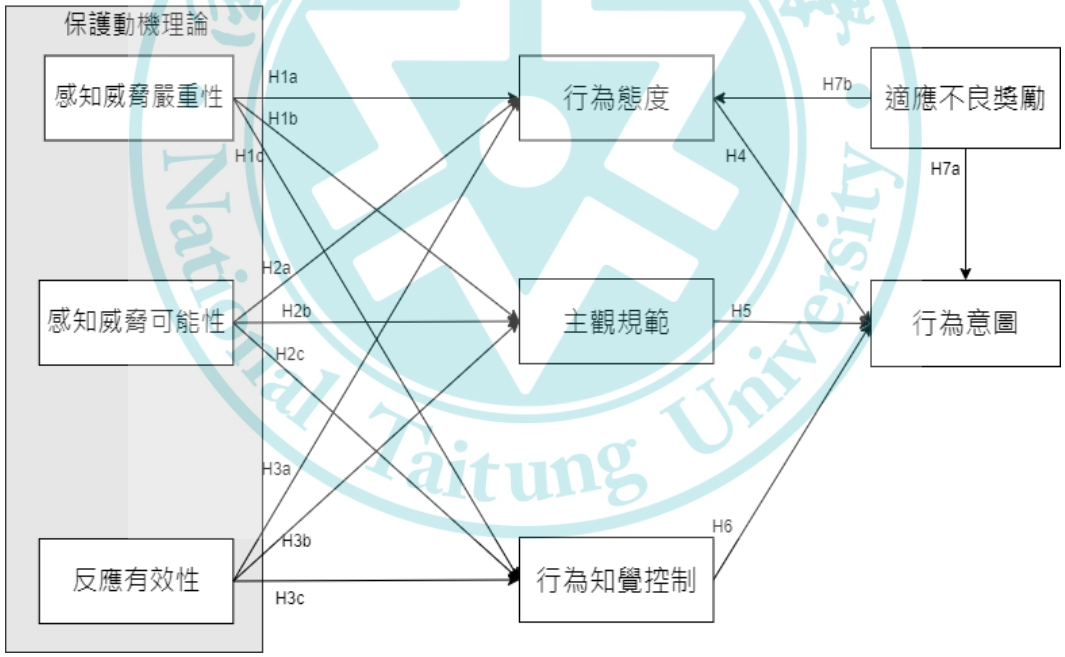

圖 10. 研究架構圖

3.1.1 感知威脅期望

在保護動機理論(PMT)的論述脈絡可知，恐懼是引起態度和行為改變的強大動力(Lennon, Rentfro & O'Leary, 2010)，面對威脅來臨時，首先須認知威脅方能分析並提出對策(林子婷，2011)。從Rogers於1975年提出的論文《A Protection Motivation Theory of Fear Appeals axnd Attitude Change1》可擷取出保護動機理論模式圖，Rogers認為"態度的改變(Attitude Change)"多寡取決於"認知調解過程(Cognitive Mediating Processes)"，而認知：調解過程中的考量因素來自於"恐懼訴求的構成要素(Components of a Fear Appeal)"。

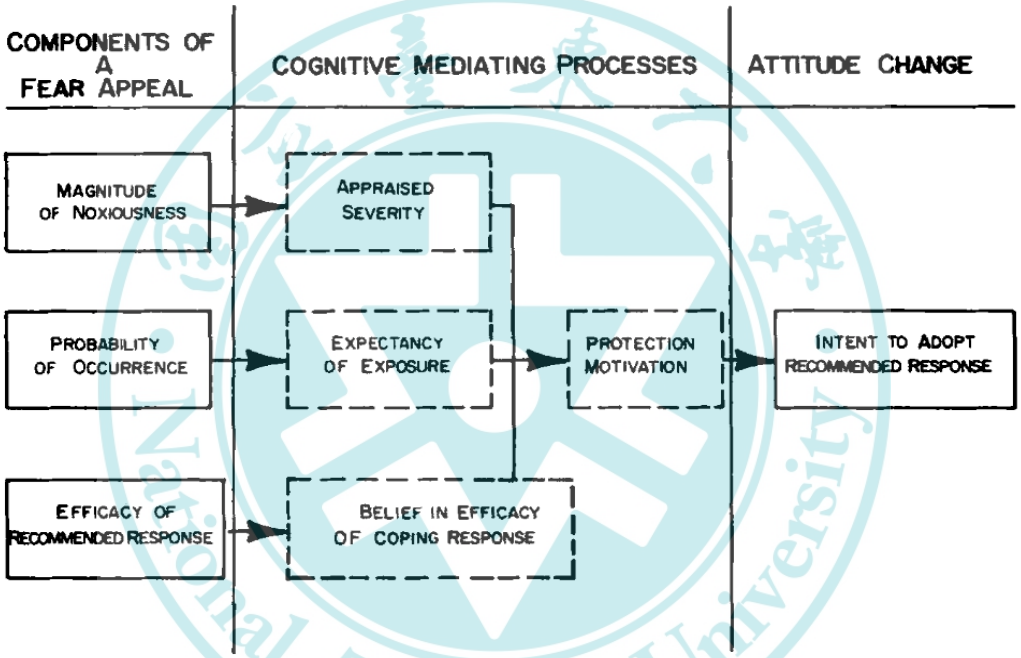

FIGURE 1
SCHEMA OF THE PROTECTION MOTIVATION THEORY

圖 11.保護動機理論模式圖

資料來源:Rogers, 1985

這項理論可以追溯至Rogers(1975)引用Hovland等人(1953)所著論文《Communication and Persuasion》其中提出的威脅期望值理論的概念，而此概念後來由五位不同領域的知名心理學家Atkinson、Edwards、Feather、Fishbein、Rosenberg皆引用過此威脅期望的概念以解釋決策選擇行為，並假設了其理論變數間的乘法關係。

其乘法函數認為由三項中介變數組成

<a變數> 所描述事件的危害程度(原文:the magnitude of noxiousness of a depicted event)；<b變數> 在不採取適應性行為或不改變現有行為傾向的情況下，事件發生的條件概率(原文:the conditional probability that the event will occur provided that no adaptive behavior is performed or there is no modification of an existing behavioral disposition)；<c變數> 可能減少或消除有害刺激的應對措施之可用性和有效性(原文:the availability and effectiveness of a coping response that might reduce or eliminate the noxious stimulus.)。

其定義與保護動機理論的三項前置變數此外，若三項變數之中其中一項為零，則不會激起保護動機(Rogers, 1975)。舉日常生活例子而言，火災是絕對的生命/財產危害情境<a變數+>，倘若查覺到了燃燒現象，小至點燃檀香大至神壇發爐，如果現場人員評估這燃燒現象不會失控<b變數->，則不激起保護動機；然而若現場人員評估這場火勢會失控蔓延<b變數+>，並且認為自己能應對<c變數+>，則會激起保護動機並做出滅火/逃避行為。但如果現場人員評估火勢會失控並迅速蔓延<b變數++>，且感知火勢既撲滅不了也腳麻跑不掉<c變數->，則可能待在原地接受命運。

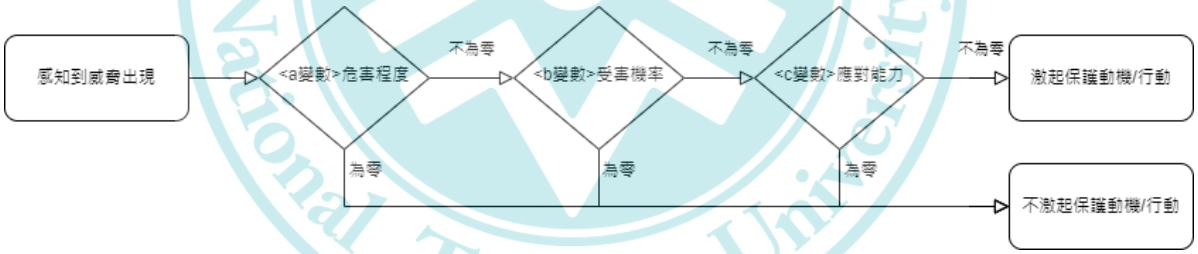

圖 12.威脅期望值理論決策流程圖

因此得以窺見從認知到評估的環節是整套決策流程的基石，Roger(1975)因此提出了基本假設「保護動機源於對所描述的事件有害且可能發生的認知評估」。若對威脅的認知不夠全面，在評估偏誤之下導致決策失誤，進而造成自身陷於險境(黃意雯，2022; Weman-Josefsson, 2021)。

威脅期望理論在本質上與保護動機理論相當近似。例如<a變數 危害程度>與保護動機理論的感知威脅嚴重性相吻合、<b變數 受害機率>與保護動機理論的感知威脅可能性定義相似、<c變數 應對能力>則與保護動機理論的感知反應有效性吻合。

鑒於以上Hovland的論述以及融合Rogers對於保護動機理論的理念架構。本研究認為恐懼訴求的構成要素(Components of Fear Appeal)包含感知威脅嚴重性、感知威脅可能性(近似於感知威脅脆弱性)，並且這兩項變數會對認知調解過程(包含行為態度、主觀規範、知覺行為控制)產生影響，進而影響行為意圖(保護動機)。

是故本研究提出以下假設:

H1a.感知威脅嚴重性對於行為態度有正向影響

H1b.感知威脅嚴重性對於主觀規範有正向影響

H1c.感知威脅嚴重性對於知覺行為控制有負向影響

H2a.感知威脅可能性對於行為態度有正向影響

H2b.感知威脅可能性對於主觀規範有正向影響

H2c.感知威脅可能性對於知覺行為控制有正向影響

3.1.2 反應有效性

誠如前節所述，Rogers(1975)認為認知調節過程是改變態度的前置過程，因而改變保護動機。改變態度有三項前置過程，其中兩項是前節所述的感知威脅可能性、感知威脅期望；而本節主題反應有效性是繼其危害評估流程的末項變數，也是保護動機理論原有的三項變數 反應效能 (Response Efficacy)、自我效能 (Self-efficacy)、反應成本 (Response Costs) 以及計劃型行為理論兩項關於行為控制的變數控制信念(Control Beliefs)、知覺行為控制 (Perceived Behavioral Control) 提綱挈領的涵意濃縮，並藉由中介變數間接影響行為意圖(保護動機)。

本主題在Hovland的威脅期望值理論裡屬於<c變數>，其代表了個體面對危害時的應對能力、行動有效性，並受到感知威脅可能性、感知威脅期望的前置影響，與計畫行為理論的知覺行為控制(Perceived Behavioral Control)用來預期個人在採取某一特定的行為時自己所感受到可以控制（或掌握）的程度之理念相吻合。Ajzen(2006)還補充表示，總括而論態度與主觀規範越正向，知覺行為控制就越強烈，進而強化個體的行為意圖。而且主觀規範與知覺行為控制三者之間還具有相互影響之關係(Ajzen,1985、1991; Ajzen and Madden, 1986)，並結合形成對某項行為之意向，其變數間的互動複雜程度與Hovland的威脅期望值理論相較更為精細。

因此本主題假設:

H3a.反應有效性對於行為態度有正向影響

H3b.反應有效性對於主觀規範有正向影響

H3c.反應有效性對於知覺行為控制有正向影響

3.1.3 行為態度

個體對於各種事物的看法、認知、好惡各有所不同，提綱挈領而論稱之為態度。在現實生活中隨處都是態度，各人對於任何人、事、物都有不同的態度，並且影響因素多樣且複雜，例如對工作的投入程度、對每天接觸到的廣告行銷有無感到興趣、對於政黨傾向乃至於對於總統／縣市長候選人的評價.....等等，皆是態度的展顯。諸多因素皆能左右一個人的態度，例如人格、耳濡目染、家族理念、教育、同儕、重要他人、師長、道德、社會觀感、社群規範、利害關係、利益、性別、身分地位、社會經驗、種族、偏見、歧視、媒體、視聽來源、場合、人際之間相對待、政治正確.....等因素，族繁不及備載。社會科學學術界其中一位知名學者 Richard T. LaPiere(1899–1986)一生做過多項關於態度的研究，像是在當年充滿種族歧視的美國測試各種情境之下，各家餐館在人前人後對待亞洲人的態度(LaPiere, 1934)，多項研究皆指出大多數人在公開場合會比私下場合更顯得寬宏大量，這就是態度受到歧視、場合、利害關係、社會觀感、政治正確等因素影響的體現。

至於Ajzen的計畫行為理論中，態度也受到諸多因素左右，例如主觀規範(SN)、知覺行為控制(PCB)皆能影響行為態度(At)，且三者會相互影響，最後，三者的綜合加權才是影響行為意圖(BI)，於是影響實際行為(B)。例如社會觀感、社群壓力也會影響個人的態度；個人的執行力以及實現可能性也會影響態度，這點也在數十年以來多項社會科學、心理學研究得到證實。本研究認為前述的感知威脅期望、反應有效性也能產生相似影響力，故有前述H1a、H2a、H3a假設，然而因受限於研究篇幅、本主題的探索特性、問卷長度、成本等因素，相較於Ajzen教授原本的路徑設定，本研究提出調整過的路徑如下：

H4.行為態度對於行為意圖有正向影響

3.1.4 主觀規範

人類身為群體動物，個人的思維或行為皆與社會環境環環相扣，我們每一個人日常的行為常受團體生活的影響，這是顯而易見的事實，而有時個人獨創新的行為模型受到社會廣泛採納時也可成為一種文化模型(龍冠海，1971)。

綜觀而論，社會文化與個人行為互為表裡，然而前者總是影響後者居多且力道更強(沙依仁，2007)。尤其作者與大多讀者所處的東方華人文化比其他文化更傾向於關係取向、社會取向、集體主義(王震武等人，2008；黃光國，1988；楊國樞，1992; Triandis. et al., 1988)，因此研究者推測本研究的主觀規範在亞洲文化圈的影響力將會較為明顯。

在Ajzen的計畫行為理論中，主觀規範也受到諸多因素左右，例如態度(At)、知覺行為控制(PCB)皆能與主觀規範(SN)相互影響，個體對於某件事的態度受到社會大眾的評價所左右(+/-)；然而倘若個體對於此事的態度相當強硬，則更傾向於不在意社會大眾的異樣眼光，因此削弱主觀規範(-)。社群壓力也會影響個體的行動力，因而增強或削弱知覺行為控制(+/-)；知覺行為控制較低落時，個體在信心低落狀態下會更傾向於徵求外在意見，因而增強主觀規範的影響力(+)；反之亦然(-)。

是故，因受限於研究篇幅、本主題的探索特性、問卷長度、成本等因素，相較於Ajzen教授原本的路徑設定，本研究提出調整過的路徑如下：

H5.主觀規範對於行為意圖有正向影響

3.1.5 知覺行為控制

知覺行為控制代表的是個體認為達成某件事物的難易程度(Ajzen, 1991)，也意味著個體執行該行為的信心以及掌握程度。「行為控制」意味著執行力，但未必然代表實際行動力，因為儘管有執行力，還需行動者本身的認知意識共同配合方能達成實際行動，認知意識的多寡就是「感知」。意識/認知未必能真實反映客觀實際的能力，因為可能低估亦可能高估，因此可能促進或阻礙行為表現的因素之個人能力評估。1995年Taylor 與 Todd 以計畫行為理論為基礎並參考 TAM 模型與創新特性相關文獻，共同提出解構式計畫行為理論(DTPB)其中能左右知覺行為控制的變數之一稱為自我效能(self efficacy)，自我效能早在1977年年由Albert Bandura提出，自我效能與個體本身擁有的能力無關，而是跟個體對於自身能否完成事項的評價(Bandura, 1986)，Strecher 等人1986年的研究更指出自我效能會影響行為的認知，也就是自信/信心，恰好正是保護動機理論中影響保護動機的自我效能感(self efficacy)變數。

影響信心的因素可分為外在/內在，內在控制因素力如個人的缺點、技術、能力或情緒等；外在控制因素力如外來資訊、機會、對他人的依賴性或障礙等（Notani, 1998）。這也印證了Ajzen的原先理論態度(At)、知覺行為控制(PCB)、主觀規範(SN)三者相互影響的模式，態度的正面或負面評價會影響行動力，也就是知覺行為控制；知覺行為控制的多寡亦能代表達成信心，信心多寡可以影響態度。外界的眼光、意見、主觀規範能影響信心、控制信念因而左右知覺行為控制；知覺行為控制程度高昂/低落時，亦能抑制/提升主觀規範的影響力。

執行特定行為時，信心尤關重要，若無把握執行，大多意圖都將因害怕失敗而淪為只空想而不施行的白日夢。知覺行為控制(PCB)在三者自變數之中常被認為預測行為(B)的強力變數，其與實際行為的關聯較為強烈(蔡志敏，2014; Compeau & Higgins, 1995;)，因而在計畫行為理論(TPB)或解構式計畫行為理論(DTPB)的理論框架中，只要掌握知覺行為控制(PBC)與行為意圖(BI)往往可以一葉知秋：知覺行為控制(PCB)與意圖(BI)的乘積相近於實際行為(B) PCB × BI = B

然而因受限於研究篇幅、本主題的探索特性、問卷長度、成本等因素，相較於Ajzen教授原本的路徑設定，本研究提出調整過的路徑如下：

H6.主觀規範對於行為意圖有正向影響

3.1.6 適應不良獎勵

這是來自於保護動機理論的構面，在大多有害情境之下此變數乍看違反直覺，實則少部分人因為個人因素不願採取措施、或只注重短期益處而忽略更嚴重的長期害處、甚至可能在特定情境之下可以因災害而受益，因而寧願不採取保護措施或願意任其發展，於是減低保護行為意圖(Hagan, 2020; Vance,et al., 2012)。

為了方便讀者理解，在此以近年全球流行病 Covid-19 舉例，Covid-19 疫情造成了生命健康損失、醫療系統告急、企業停頓、部分公司倒閉、員工因此失業、活動停擺，因而全球供應鏈失調，連帶影響全球政經局勢。

然而少部分人不打算改變現狀，例如：

1. 單純不願意戴口罩者。覺得戴上口罩難以呼吸又麻煩，乾脆不戴口罩方便呼吸又能省錢，因而不採取保護措施。
2. 數位政策推動者。因為 Covid-19 造就許多領域必須面臨數位化、遠距化，原本窒礙難行的數位化轉換變得更方便推動了。
3. 電資從業者。疫情造就大量的數位化市場需求，電信業、電腦資訊業因而從中獲得紅利。
4. 醫療相關業者。醫療需求大量湧入，顯而易見。
5. 倦怠生活者。原本就厭倦了忙碌的疫前生活，無暇在家陪親友，依自己的步調過活。疫情來臨終於有機會可以喘息。
6. 電商業者。實體經濟停擺，順帶而來的是虛擬經濟成長。
7. 物流運輸業者。疫情導致電商物流、搬遷、宅配等需求暴增。
8. 健康醫療險詐保者。趁疫情來襲從中獲取保險賠償。
9. 駭客。大量事務遠距化、數位化，許多公家或私人單位都防駭措施不夠完善，駭客因而能趁隙而入。等族繁不及備載.....

在危機重重日漸嚴峻的的資安環境從中擁有適應不良獎勵的情境預測可能有下:

1. 不願採用多因子驗證者。可能單純不懂、不會操作、嫌麻煩、認為沒必要，因此不採用多因子驗證反而省心省錢。

2. 驗證機制從業者。大家採用多因子驗證將能創造相關市場需求，例如密碼管理服務、驗證金鑰保管、實體金鑰銷售。
3. 資安險詐保者。已投保資安險。任資訊遭駭竊而獲取保險賠償。
4. 駭客。受僱參與資安攻防、產生練習累積經驗的機會、或其本人就是資安危機亂源。

而本研究聚焦於探究多因子驗證的採用動機，舉例2.驗證機制從業者屬於多因子驗證廣用化的受益者，顯然無理由有適應不良獎勵，故在本研究將把此族群排除在外。

是故，本主題假設：

H7a.適應不良獎勵對於行為意圖有負向影響

H7b.適應不良獎勵對於態度有負向影響

3.1.7 行為意圖

促成一項行動或現象有其脈絡，動機是促成目的或行為的原因；意圖則促成特定目的或行為。意圖、動機兩者皆是構成行為的要素，兩者定義上最大不同之處在於"特定性"，有時兩者對於行為的影響力重疊而無法區分。(黃惠婷，2008)

淺顯比喻，就如研究者本人有次在牛排館享用海鮮特餐，友人認為跑到牛排館吃海鮮餐點不甚合理而提出質疑，研究者當下行為的緣由可以分成多個層面解釋：

1. 研究者本人偏愛吃海鮮勝於牛排。喜吃海鮮是動機；當下為了打算滿足口腹之慾而點海鮮是意圖。(行為態度)
2. 研究者日常飲食不常出現海鮮，缺乏攝取鋅，擔心缺乏鋅而可能影響與伴侶的互動因而想補充鋅是動機；因為想補充鋅而點海鮮是為意圖。(感知威脅嚴重性、感知威脅可能性、主觀規範)
3. 海鮮比牛排更容易斷開、進食，因而可以在同一時間內更快吃完並享用自助吧附加服務。海鮮較方便進食、想吃自助吧此兩原因都是動機；因為想盡快完食主餐並享用附加服務而點海鮮是意圖。(反應有效性、知覺行為控制)
4. 海鮮餐和牛排餐的價格與 CP 值皆旗鼓相當，免除了成本/預算/CP 值的抉擇考量。(知覺行為控制)
5. 上述原因和機會成本考量等因素綜合疊加之下，在研究者心中更加合理化點海鮮餐的行為。綜合因素影響態度因而轉化為行為意圖，最後造就實際行為。

以上理由皆有其最佳替代方案。缺鋅可以吃營養品以補充鋅、愛吃海鮮可以光臨日本料理館、要方便進食可改吃流質食物；但由於在特定的人、事、時、地、物等脈絡下才發展出特定行為意圖或特定行為，遂有探究價值。

將保護動機理論與計畫行為理論兩相比較，保護動機理論較為追究引起事件發生的助力－動機；而計畫行為理論較聚焦於施展行為時的成因或想法－意圖。按照以相同的邏輯來檢視先前「張大哥採取多因子驗證」個案的決策過程（詳見第二章第四節－計畫行為理論），可得出各條路徑中各個因素影響的解釋：

1. 張大哥原本不了解何謂多因子驗證，對於是否該採用多因子驗證毫無意見態度；但因為親友帳號遭駭並被施展一連串不當操作，例如詐團利用受害者帳號四處發送木馬連結以及借款，張大哥擔心自己也會受害，詢問旗下就讀資管所擁有電資能力的員工，在該員工的指導下得知多因子驗證能有效保護資料，因而想採用多因子驗證。

   「從原本毫無態度-，瞭解到問題嚴重性後激發感知威脅嚴重性、感知威脅可能性，一言概之也就是感知威脅期望，並且在相關技術人員的指示下加強了主觀規範，因而提升採用措施的態度+。 因為怕自己也受害是為保護動機；有了保護動機而產生保護行為意圖」

2. 張大哥原本對於多因子驗證有相當正面的態度以及充足動機，但既不知如何控制這套驗證機制，家中也無親友懂得操作，因此張大哥喪失了採用意圖，也因此無法完成採用多因子驗證的行為。

   「對於保護措施有正面態度也有動機，然而因為知覺行為控制不足而作罷，喪失意圖」

3. 多日後張大哥再度請教該資管所畢業員工，協助施作並且教導操作，一舉解決了原本的瓶頸並成功採用多因子驗證。

   「在現有人脈資源協助下克服知覺行為控制不足的障礙，並將成功將整個路徑打通至行為，個案圓滿完結」

由意圖或動機的分析用以解釋或預測實際行為是絕大多數社會科學研究的主要目的，其之間的關聯已被許多研究確認為正相關(Venkatesh & Davis, 2000; Venkatesh, Morris, & Ackerman, 2000)。

研究者認為動機與意圖兩者密不可分，既有先來後到的因果關係，其兩種模型的成因以及影響力也有一定程度相似性，若能整併將有可能形成更為精密的決策模型，遂為本研究將要的研究方法/研究模型。綜觀名詞定義以及涵義層級，在動機與行為意圖間則一作為變數命名，本研究認為採用行為意圖較為恰當，其層級較高且涵義較具備指向性可以解釋特定行為。

3.2 操作型定義

本章節探討本研究架構的主要衡量的 9 項變數，並根據國內外學者所發表的相關研究萃取出各項操作型定義，藉以觀摩並設計出本研究之操作型定義，有利於後續問卷設計，整理如下表 2.：

表 2.操作型定義彙整

變數	操作型定義	參考文獻
感知威脅嚴重性	受試者對於網路侵駭的危害認知程度。	Rogers.et al. (1975,1983); Herath and Rao (2009);
感知威脅可能性	受試者認為受到網路侵駭的可能性。	Rogers.et al. (1975,1983); Herath and Rao (2009);
反應有效性	受試者認為多因子驗證能達到預期效果。	Rogers.et al. (1975,1983); Taylor and Todd(1995); Herath and Rao (2009);
態度	受試者對於多因子驗證的評價。	Fishbein and Ajzen (1975,1977); Herath and Rao (2009)
主觀規範	受試者認為其他人對於多因子驗證的評價。	Rogers.et al. (1975,1983); Taylor and Todd(1995)
知覺行為控制	受試者認為能否操作多因子驗證。	Bandura (1977,1986); Strecher. et al.(1986); Notani(1998); Taylor and Todd(1995); La Barbera and Ajzen(2020)
適應不良獎勵	受試者是否認為不使用多因子驗證反而比較好。	Rogers.et al. (1975,1983); Vance,et al.(2012); Hagan (2020)
行為意圖	受試者有多願意執行此行為。	Fishbein and Ajzen (1975); Ajzen(1989,1991,)

3.3 問卷設計

本研究採用的問卷題項採自於國內、國外相關領域之文獻，統整並邀請資訊管理領域學者審閱問卷格式、架構、用語、問項設計是否符合規範，經由前測分析並修正後再發行正式問卷。

本研究問卷分為三頁，第一頁為基本資料，第二頁為多因子驗證之介紹頁面，第三頁為各構面正式問項。由於「多因子驗證」此詞彙於多數人的認知中屬陌生詞彙，以防受試者不知道何謂多因子驗證因而無從作答，在基本資料的最後一題安排項目為「您知道多因子驗證或是二段式驗證嗎?」題目，若受測者填答「不知道」或「聽說過」即代表受測者對於多因子驗證並不熟悉，下一步將會傳送至第二頁多因子驗證之介紹頁面撥放時長2分鐘的講解短影片，此短片由Duo公司製作，並由研究者翻譯、追加繁體中文字幕而成。觀賞短影片之後方能填寫正式問卷；而此題若填答「充分理解」、「偶爾使用(一週至少一次)」、「經常使用(一週五次以上)」者即代表受測者對於多因子驗證已有一定認識，於是下一步將會跳過第二頁而直接在第三頁填寫正式題項。

正式題項各構面之量化題型採用李克特五點尺度量表 (Likert scale) 衡量，分數由低至高分別為非常不同意（1 分）、不同意（2 分）、普通（3 分）、同意（4 分）、非常同意（5 分）。

問卷中會適當安插反向題，反向題之語意邏輯順當，然而計分方式與其他題目相左，藉以偵測並去除惡意填卷或隨意填答的樣本。

表 3.問卷的各構面之衡量題項

研究構念	量表題項	參考文獻
感知威脅嚴重性	如果您的資料外洩將會造成嚴重的財物損失。 如果您的帳號被駭將會是個嚴重問題。 如果您所屬的單位資料外洩將會是個嚴重問題。 整體而言，您覺得資料外洩會造成嚴重的資安威脅。	Vance,et al.(2012); Johnston & Warkentin, (2010); Herath and Rao (2009);
感知威脅可能性	您認為您的網路帳號可能被侵駭。 您會覺得資料外洩或駭客入侵事件是很常見的。 您會覺得您的資料或帳號有可能被外洩或受到駭客入侵。 您認為周遭親友有可能被侵駭。	Herath and Rao (2009); Liang & Xue, (2010); Ogbanufe, O. (2023);
反應有效性	遵守資安規範可以減少被駭可能性。 您會遵守資安規範以有效減少被駭可能性。 您會使用多因子驗證以有效降低資料外洩的可能。 您會認為採用多因子驗證能有效反應資安防護需求。	Vance.et al.,(2012); Liang & Xue, (2010); Ogbanufe, O. (2023);
態度	您會認為採用多因子驗證可以有效預防資安威脅。 您會覺得採用多因子驗證是個好主意。 您會覺得多因子驗證是個很重要的防駭技術。 您會認為在特定資安預防情境應該強制使用多因子驗證。 您會認為多因子驗證應該要更普及。	Dugo (2007); Sommestad et al.(2014); Guo et al. (2011); Sommestad et al.(2014) ;

表 4.問卷的各構面之衡量題項(續)

研究構念	量表題項	參考文獻
主觀規範	您親朋好友會認為您應採用多因子驗證。 您資訊專長朋友會建議您採用多因子驗證。 您的長官或同事會建議您採用多因子驗證。 您周遭的利害關係人會認為您應採用多因子驗證。 您會認為各類公民營組織或個人都應採用多因子驗證。	Guo et al. (2011) ; Sommestad et al.(2014) ;
知覺行為控制	您會認為遇到資安侵駭事件時，您可以從容應對。 您會認為自身的資訊技術有信心。 如果遭遇資訊領域的問題，您知道從哪找資源。 如果您無法成功採用多因子驗證，有人可以幫忙達成。	Liang & Xue, (2010); Ogbanufe, O. (2023);
適應不良獎勵	您寧願不採用多因子驗證。 您認為不要使用多因子驗證比較省事 強制採用多因子驗證的話對您造成困擾 多因子驗證在世界上不存在的話對您比較有益處 您不希望各公家及私人團體倡議採用多因子驗證	Vance,et al.(2012);
行為意圖	在未來，您有意願要採用多因子驗證。 您有意願為個人資訊安全的需要採用多因子驗證。 您有意願推薦周遭親友採用多因子驗證。 您願意花費更多時間採用多因子驗證以增進資安等級。 您願意花費更多金錢採用多因子驗證以增進資安防護。	Liang & Xue, (2010); Ogbanufe, O. (2023);

3.4 問卷發放

為增加樣本多樣性，本研究透過多種管道與手法散佈問卷，分為線上發放與線下發放、特定親友散佈與陌生非特定散佈.....等。例如投放在Facebook問卷發放社團、Dcard匿名貼文、Line群組、研究者的人際圈、研究者親朋好友之人際圈(滾雪球式抽樣)、街頭訪問、研究者的客戶.....等，因此在觀察基本統計資料時可注意到受測者之間年齡、從事職業、學歷等個人背景差異甚鉅。

第四章 研究資料分析

4.1 受測者樣本描述

本研究是以網路使用者為研究母群體，故特意排除紙本問卷發放管道，經由網路平台上散佈短網址以及人潮密集處擺放QR Code發放以進行實證調查。本研究收到305份樣本，刪除掉隨意亂填、觸發反向題的無效問卷2份後，有效問卷303份。茲將本研究的受測者基本資料與使用者行為之次數分配統計分析結果說明如下。

(一) 依填答者性別

在本研究回收樣本中，生理女性作答者多於生理男性作答者，女性作答者有177人，佔58.4%，男性使用填答者有126人，佔41.6%。

表 5.受測者性別資料分析表

項目	人數	百分比
男生	126	41.6
女生	177	58.4
總和	303	100.0

(二)　依填答者年齡

在本研究回收問卷樣本中，18-25歲的作答者有93人為最多，佔30.7%；45-55歲的作答者次之，有76人，佔25.4%；55~65歲的作答者再次之，計有52人，佔17.2%；另外，與25~35歲則有41人，佔13.5%；35~45歲作答者有32人，佔10.2%；18歲以下的使用填答者人數5人，佔1.7%；65歲以上4人佔1.3%。

表 6.受測者年齡資料分析表

項目	人數	百分比
18 歲以下	5	1.7
18~25 歲	93	30.7
25-35 歲	41	13.5
35-45 歲	32	10.2
45~55 歲	76	25.4
55~65 歲	52	17.2
65 歲以上	4	1.3
總和	303	100.0

(三)　依填答者教育程度

在本研究樣本中，以一般大學的作答者為最多，有95人，佔31.4%；其次為研究所作答者，有73人，佔24.1%；高中/高職學歷的作答人數位居第三，有57人，佔18.9%；第四大為大專的作答者人數為52，佔17.2%；科技大學作答者佔第五大24人，佔7.9%；最後是國中或以下人口僅2人佔0.7%。

表 7.受測者教育程度資料分析表

項目	人數	百分比
國中(含)以下	2	0.7
高中(職)	57	18.9
一般大學	95	31.4
科技大學	24	7.9
大專	52	17.2
研究所	73	24.1
總和	392	100.0

(四)　依填答者職業別

本研究的回收問卷樣本當中，分別列了9個主要職業別選項，如下表將分析數據排列，從列表中，我們可瞭解到採集到的樣本以作答者為最多，有82人，佔27.1%；服務業的填答者次之，有54人，佔17.8%；第三大為軍公教的作答者，有40人，佔13.2%；第四大為製造業作答者有34人，佔11.2%；由數據顯示其他產業、自由業、金融業、資訊科技業、醫療業從業者分別佔了9.6%(29人)、6.6%(20人)、5.9%(18人) 、4.6%(14人)、4.0%(12人)。

表 8.受測者職業別資料分析表

項目	人數	百分比
學生	82	27.1
軍公教	40	13.2
製造業	34	11.2
資訊科技業	14	4.6
服務業	54	17.8
金融業	18	5.9
自由業	20	9.6
醫療業	12	4.0
其他	29	9.6
總和	392	100.0

(五)　依填答者常用網路服務

因本研究主重於多因子驗證之研究，網路使用者的常用網路服務/常用網路平台也是值得探討的研究因子。本問項採複選作答，根據統計大眾最常使用的網路服務為社群軟體例如Facebook、Instagram、Twitter、VK、Dcard…..等，總共261人，佔總人口86.1%；第二名為影片平台例如YouTube、Netflix、Disney+、Amazon Prime……等，總共232人，佔總人口76.6%；第三名為帳號同步化平台例如Google、Apple ID、Samsung帳號、小米帳戶、Yahoo …..等總共160人，佔總人口52.8%；第四名為金流服務例如網路ATM、電子支付、網路銀行、網路證券交易……等，總共129人，佔總人口42.6%；第五名為網路休閒類 (線上遊戲、網路購

物、網路論壇.....等) 總共125人，佔總人口41.3%；最後則是通訊軟體例如Line、WeChat、Telegram、Discord.....等，總共113人，佔總人口37.3%；

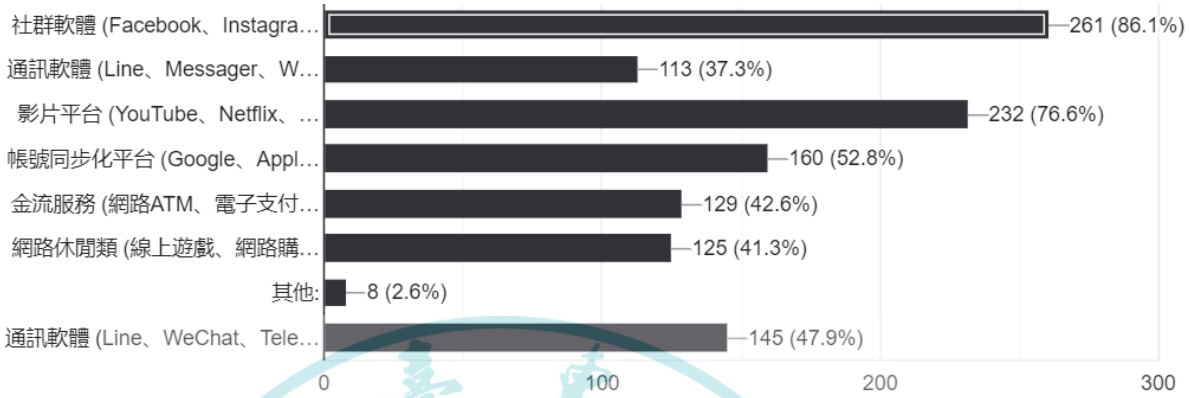

圖 13. 常用網路服務長條圖

(六)　依作答者平均每日使用網路之時數

在本研究樣本中，平均每日使用網路長達5小時以上的填答者高達47.9%(145人)；3至5小時的填答者佔17.3%(87人)；1至3小時者佔21.8%(66人)，小於1小時者僅5人，佔1.7%。

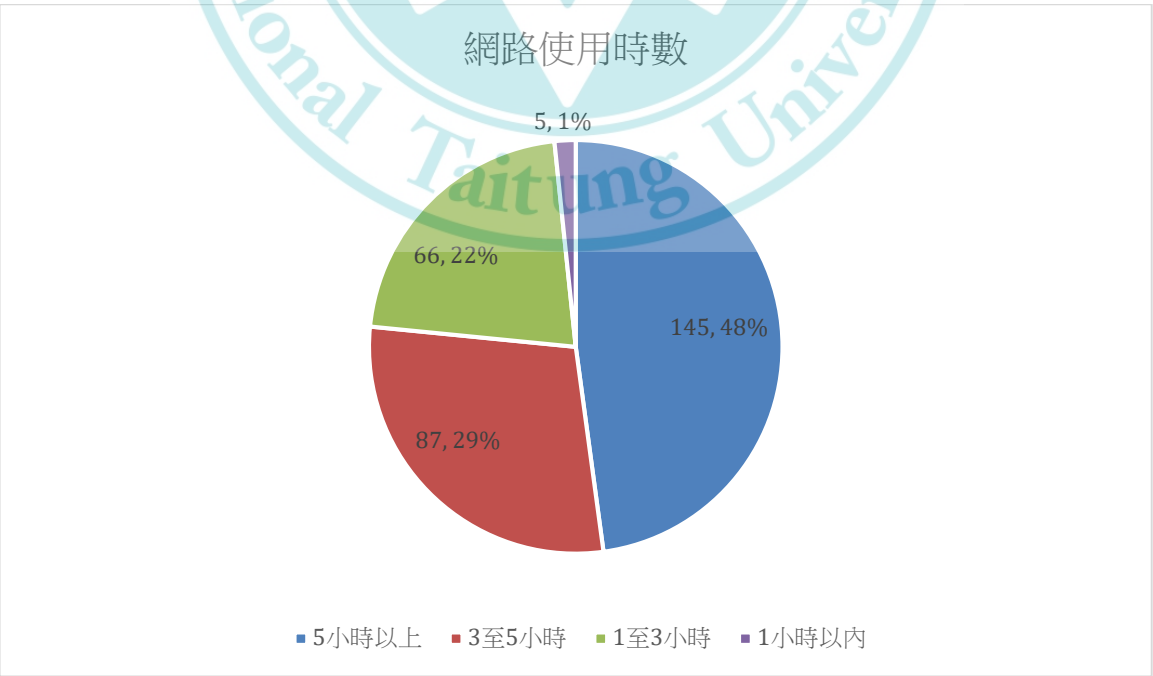

圖 14. 網路使用時數統計圓餅圖

4.2 描述性統計分析

本節根據採集樣本所得結果分析，以平均數、標準差等資料來瞭解本研究各構面感知威脅嚴重性、感知威脅可能性、反應有效性、態度、主觀規範、知覺行為控制、適應不良獎勵、行為意圖的相關問卷題項等八個構面的敘述性統計分析結果說明如下：

(一) 感知威脅嚴重性構面

關於感知威脅嚴重性構面上，相關問卷題項的得分平均數介於4.637至4.723分之間，填答者同意程度高於五點量表普通程度3，而中位數高達5分同意程度，得分屬於高程度的感知威脅嚴重性，表示大眾對於資安危害的嚴重性是感到認同的，分析結果如下表8所示。

表 9.敘述統計分析

	感知威脅嚴重性題項	平均數	標準差
PTS 1.	您會覺得如果資料外洩會造成嚴重的財務損失。	4.512	0.770
PTS 2.	您會覺得如果您的帳號被駭將會是個嚴重問題。	4.723	0.615
PTS 3.	您會覺得如果您所屬的單位資料外洩將會是個問題。	4.637	0.749
PTS 4.	整體而言，您覺得資料外洩會造成嚴重的資安威脅。	4.719	0.606

(二) 感知威脅可能性構面

在對於感知威脅可能性方面，相關問卷題項的得分平均數介於3.719至4.023分之間，題項的得分平均均高於3.5，題項同意程度介於3分普通和4分同意之間，中位數皆為4分，得分屬於中上同意程度的感知威脅可能性，表示大多數受試者對於資安威脅的發生可能性是感到認同的，分析結果如下表9所示。

表 10.構面敘述統計分析

感知威脅可能性題項		平均數	標準差
PTP 1.	您會覺得資料外洩或駭客入侵事件是很常見的。	4.023	1.016
PTP 2.	您會覺得您的網路帳號可能有被侵駭過了。	3.719	1.136
PTP 3.	您會覺得您周遭親友的資料、帳號仍可能受駭。	4.020	0.981
PTP 4.	您會覺得您的資料或帳號有可能被外洩或受到駭客入侵。	3.993	0.995

(三) 反應有效性構面

關於問卷受試者在反應有效性方面，分析結果顯示相關題項的得分平均數介於4.145至4.317分之間，題項同意程度介於4分同意和5分非常同意之間，得分屬於高程度的認知有用，表示使用者對於資安規範、多因子驗證的防駭有效性大部分是認同的，分析結果如下表10所示。

表 11.反應有效性構面敘述統計分析

反應有效性題項		平均數	標準差
RV 1.	您會認為遵守資安規範可有效減少被駭可能性。	4.145	0.971
RV 2.	您會遵守資安規範以有效減少被駭可能性。	4.241	0.911
RV 3.	您會使用多因子驗證以有效降低資料外洩的可能。	4.317	0.840
RV 4.	您會認為採用多因子驗證能有效反應資安防護需求。	4.297	0.827

(四) 態度構面

關於問卷受試者態度方面，相關題項的得分平均數介於4.31至4.419分之間，填答者同意程度高於五點量表同意程度4，介於4分同意和5分非常同意之間，其中4題中位數高達5分，剩餘4分，表示大部分使用者對於多因子驗證用以保護資安之情境抱持正面的態度，而且在使用者間具有相當的一致性，分析結果如下表11所示。

表 12.態度構面分析

	態度題項	平均數	標準差
A 1.	您會認為採用多因子驗證可以有效預防資安威脅。	4.310	0.764
A 2.	您會認為採用多因子驗證是個好主意。	4.366	0.745
A 3.	您會認為多因子驗證是個很重要的防駭技術。	4.333	0.790
A 4.	您會認為多因子驗證應該要更普及。	4.419	0.775
A 5.	您會認為在特定資安預防情境應該強制使用多因子驗證。	4.386	0.804

(五) . 主觀規範構面

關於問卷受試者對於他人眼光的主觀認知而感受到的規範效果，相關題項的得分平均數介於3.65至4.238分之間，高於本研究五點量表之3分普通和4分同意，得分亦屬於中上程度的認知有用，表示大多數受試者對於他人眼光的主觀認知具有一定的約束程度，分析結果如下表12所示。

表 13.主觀規範構面敘述統計分析

	主觀規範效果題項	平均數	標準差
SN 1.	您親朋好友會認為您應採用多因子驗證	3.660	1.028
SN 2.	您的長官或同事會建議您採用多因子驗證	3.650	1.029
SN 3.	您資訊專長朋友會建議您採用多因子驗證。	4.053	1.010
SN 4.	您周遭的利害關係人會認為您應採用多因子驗證。	3.855	1.021
SN 5.	您會認為各類公民營組織或個人都應採用多因子驗證	4.238	0.942

(六) 適應不良獎勵構面

關於問卷受試者在適應不良獎勵方面，相關題項的得分平均數介於2.172至2.809分之間，注意！這題型屬於負向題，分數越高代表越不願意採用多因子驗證，反之亦然。本構面各問項分數平均與中位數皆低於或等於本研究李克特五點量表尺度平均數3，得分程度介於3分普通幾近於2分不同意，得分符合預期，表示受試者普遍對於多因子驗證的排斥程度偏低，值得注意的是，本構面各題項標準差高

達1.26，若以柱狀圖表示會發現多個題項呈現鐘型分布或左偏分布且柱狀圖鋒度較緩，甚至有其中兩題並非典型的鐘形常態分佈或J型分布，而是1分與3分得分最高的U型分布曲線，推測大多數受試者其實認為採用多因子驗證有一定複雜性而感到困擾，然而終究會因為多因子驗證所帶來的益處而選擇與其共存，分析結果如下表13所示。

表 14.適應不良獎勵敘述統計分析

適應不良獎勵程度題項		平均數	標準差
MR 1.	您認為不採用多因子驗證比較省事	2.809	1.260
MR 2.	您寧願不採用多因子驗證	2.241	1.128
MR 3.	多因子驗證在世界上不存在的話對您比較有益處	2.172	1.119
MR 4.	強制採用多因子驗證的話對您造成困擾	2.647	1.212
MR 5.	您不希望各公家及私人團體倡議採用多因子驗證	2.340	1.169

(七)　知覺行為控制構面

關於問卷受試者在自身評估資安能力方面，相關題項的得分平均數介於2.855至3.373分之間，落在本研究李克特五點量表尺度平均數3分普通程度左右，顯示大部分受試者對於自身資安能力評估並無特別自信或自卑，另一角度解讀也可能來自於大眾對於資安領域的一知半解，例如在不確定如何衡量資安能力的情形下選擇作答普通3分最為保險，分析結果如下表14所示。

表 15.知覺行為控制敘述統計分析

知覺行為控制題項		平均數	標準差
PCB 1.	您會認為遇到資安侵駭事件時，您可以從容應對。	3.007	1.172
PCB 2.	您會認為自身的資訊技術有信心。	2.855	1.148
PCB 3.	如果遭遇資訊領域的問題，您知道從哪找資源。	3.208	1.199
PCB 4.	如果您無法成功採用多因子驗證，有人可以幫忙達成。	3.373	1.133

(八)　使用意圖構面

關於問卷受試者在使用多因子驗證的意圖方面，相關題項的得分平均數介於3.693至4.168分之間，高於本研究李克特五點量表尺度平均數3，顯示大部分受試者皆有願意採用多因子驗證甚至會投入更多資源的意圖，而且此滿意度具有相當高的一致性，分析結果如下表15所示。

表 16.使用意圖敘述統計分析

使用意圖題項		平均數	標準差
BI 1.	在未來，您有意願要採用多因子驗證。	4.050	0.927
BI 2.	您有意願為個人資訊安全的需要採用多因子驗證。	4.168	0.883
BI 3.	您有意願推薦周遭親友採用多因子驗證。	3.990	0.997
BI 4.	您願意花費更多時間採用多因子驗證以增進資安等級。	4.046	0.943
BI 5.	您願意花費更多金錢採用多因子驗證以增進資安防護。	3.693	1.097

4.3 測量模型檢定分析

本研究採用 SmartPLS 4 版用於檢測結構模型路徑之顯著程度。針對多因子驗證採用行為之重要影響因素之問卷，電子問卷共回收有效問卷 303 份，剔除填答不完全的問卷 2 份，可用率達 99%。根據 Fornell & Larcker(1981)提出，收斂效度採用 PLS 最小偏平方法之驗證性因素分析作為衡量依據，其中平均變異萃取量(average variance extracted; AVE)應大於 0.5，而個別構念之組合信度(CR)應大於 0.70，即達接受之收斂效度。當個別變項對於測量構念之因素荷負量(loading)夠高時(>0.707)，同樣亦達成收斂效度的要求(Straub, Marie and Gefen, 2004)。本研究針對測量工具於相關構念的區別效度進行考驗，以嚴謹驗證本研究概念架構所建立之主要研究變項之整體構念效度。所有構念的相關面向組成信度門檻值皆高於 0.70 以上，，因此各構念面向之內部一致性均符合標準。測量性質統計分析結果如表 16 所示。

表 17.本研究模式變數之信度、效度整理表

構面名稱	題項	因素負荷量	平均數	標準差
感知威脅嚴重性(PTS)	PTS 01.	0.757	4.512	0.770
	PTS 02.	0.890	4.723	0.615
	PTS 03.	0.835	4.637	0.749
	PTS 04.	0.838	4.719	0.606
感知威脅可能性(PTP)	PTP 01.	0.719	4.023	1.016
	PTP 02.	0.772	3.719	1.136
	PTP 03.	0.830	4.020	0.981
	PTP 04.	0.880	3.993	0.995
反應有效性(RV)	RV 01.	0.712	4.145	0.971
	RV 02.	0.750	4.241	0.911
	RV 03.	0.881	4.317	0.840
	RV 04.	0.876	4.297	0.827
態度(ATT)	ATT 01.	0.873	4.310	0.764
	ATT 02.	0.844	4.366	0.745
	ATT 03.	0.894	4.333	0.790
	ATT 04.	0.879	4.419	0.775
	ATT 05.	0.830	4.386	0.804

表 18.本研究模式變數之信度、效度整理表(續)

構面名稱	題項	因素負荷量	平均數	標準差
主觀規範(SN)	SN 01.	0.809	3.660	1.028
	SN 02.	0.837	3.650	1.029
	SN 03.	0.831	4.053	1.010
	SN 04.	0.844	3.855	1.021
	SN 05.	0.797	4.238	0.942
適應不良獎勵(MR)	MR 01.	0.703	2.809	1.260
	MR 02.	0.905	2.241	1.128
	MR 03.	0.849	2.172	1.119
	MR 04.	0.852	2.647	1.212
	MR 05.	0.878	2.340	1.169
知覺行為控制(PCB)	PCB 01.	0.802	3.007	1.172
	PCB 02.	0.806	2.855	1.148
	PCB 03.	0.842	3.208	1.199
	PCB 04.	0.759	3.373	1.133
行為意圖(BI)	BI 01.	0.908	4.050	0.927
	BI 02.	0.913	4.168	0.883
	BI 03.	0.906	3.990	0.997
	BI 04.	0.921	4.046	0.943
	BI 05.	0.788	3.693	1.097

本研究針對測量工具於相關構念的區別效度進行考驗，以嚴謹驗證本研究概念架構所建立之主要研究變項之整體構念效度。構念區別效度之檢驗主要在檢定測量之潛在變數對於不同的構念之間的鑑別程度。每個變項與測量同一構念的其他變項之相關程度，應該要高於與測量不同構念變項的相關係數。Chin, 1998 提出為了通過區別效度的檢驗，個別構念抽取之平均變異萃取量(AVE)的平方根，應大於該構念與模型中其他構念的共變關係。表 17 為各構面之間的相關係數矩陣，對角線所列之數值即該構念 AVE 平方根；任兩個構念之間的相關係數皆小於該構念

之測量變項的 AVE 平方根。顯示測量模型中各構念的變項確實彼此相異，本研究所設計的問卷具有足夠的區別效度。

表 19.構面之相關係數與鑑別效度

構面	1.	2.	3.	4.	5.	6.	7.	8.
1.感知威脅嚴重性	0.831							
2.感知威脅可能性	0.256	0.803						
3.反應有效性	0.381	0.242	0.808					
4.態度	0.343	0.3	0.78	0.864				
5.主觀規範	0.225	0.265	0.583	0.661	0.824			
6.意圖	0.262	0.251	0.573	0.644	0.602	0.889		
7.適應不良獎勵	-0.192	-0.012	-0.328	-0.427	-0.208	-0.473	0.84	
8.知覺行為控制	-0.059	-0.145	-0.169	-0.119	-0.241	-0.193	-0.171	0.803
平均變異萃取量(AVE)	0.691	0.644	0.653	0.747	0.679	0.79	0.706	0.645
組合信度(CR)	0.851	0.816	0.831	0.915	0.883	0.933	0.895	0.818

*對角線數值為潛在構面的平均萃取變異量(AVE)之平方根。

4.4 研究假說與模式驗證

本研究路徑係數分析採用SmartPLS 4版軟體，根據上述兩章節將本研究個別問項、構面進行信效度分析，由得到具體數據中即可確定各個構面間具有一定程度的信度與效度，因此便可再進一步對各個構面、變數間進行實質關係的檢測。本研究採用拔靴法(BootStrapping)計算研究構念的路徑係數，經由樣本的重新取樣的程序進行顯著性檢驗當t值大於1.96時，則p值小於0.05，表示已達顯著標準(以*表示)；當t值大於2.58時，則p值小於0.01，表示為次要顯著(以**表示) (Bollen and Stine, 1992)。

在研究概念架構之結構模式與主要假說的驗證檢核部分，本研究所提出的主要假設均獲得顯著性支持，進行之結構性分析結果其模型路徑參數，其結構模

式路徑分析之結果如圖 15.之SmartPLS路徑分析.所示，由其檢定結果分析，本研究歸結相關研究結果如下：

(1) H1a：感知威脅嚴重性構面對於行為態度構面無顯著的正向影響，由圖 15.之SmartPLS路徑分析結果可知，感知威脅嚴重性與行為態度之間的假說影響關係係數為0.014，t值為0.344小於1.96，未達到顯著性，所以假說H1a不成立。

(2) H1b：感知威脅嚴重性對主觀規範構面無顯著的正向影響，由圖 15.之SmartPLS路徑分析結果可知，資訊系統成功與期望確認程度之間的假說影響關係係數為-0.022，t值為0.451，未達到顯著性，所以假說H1b不成立。

(3) H1c：感知威脅嚴重性構面對知覺行為控制構面有負向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，感知威脅嚴重性與知覺行為控制之間的假說影響關係係數為-0.171，t值為3.006大於2.58，達到p小於0.01之顯著性，所以支持假說H1c成立。

(4) H2a：感知威脅可能性構面對態度構面有正向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，感知威脅可能性構面與態度構面之間的假說影響關係係數為0.128，t值為3.572大於3.28，達到p小於0.001之強顯著性，所以支持假說H2a成立。

(5) H2b：感知威脅可能性構面對主觀規範構面有正向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，感知威脅可能性構面與主觀規範構面之間的假說影響關係係數為0.136，t值為2.397大於1.96，達到p小於0.05之顯著性，所以支持假說H2b成立。

(6) H2c：感知威脅可能性構面對知覺行為控制構面有正向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，感知威脅可能性構面與主觀規範構面之間的假說影響關係係數為0.148，t值為2.280大於1.96，達到p小於0.05之顯著性，所以支持假說H2c成立。

(7) H3a：反應有效性構面對態度構面有正向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，反應有效性構面與態度構面之間的假說影響關係係數為0.678，t值為16.189大於3.28，達到p小於0.001之強顯著性，所以支持假說H3a成立。

(8) H3b：反應有效性構面對主觀規範構面有正向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，反應有效性構面與態度構面之間的假說影響關係係數為0.558，t值為10.394大於3.28，達到p小於0.001之強顯著性，所以支持假說H3b成立。

(9) H3c：反應有效性構面對知覺行為控制構面有正向顯著的影響，由圖 15.之SmartPLS路徑分析結果可知，反應有效性構面與態度構面之間的假說影響關係係數為0.198，t值為2.961大於2.58，達到p小於0.01之顯著性，所以支持假說H3c成立。

(10) H4：行為態度構面對於行為意圖構面有正向影響，由圖 15.之SmartPLS路徑分析結果可知，行為態度構面與行為意圖構面之間的假說影響關係係數為0.290，t值為4.872大於3.28，達到p小於0.001之強顯著性，所以支持假說H4成立。

(11) H5：主觀規範構面對於行為意圖構面有正向影響，由圖 15.之SmartPLS路徑分析結果可知，主觀規範構面與行為意圖構面之間的假說影響關係係數為0.312，t值為5.753大於3.28，達到p小於0.001之強顯著性，所以支持假說H5成立。

(12) H6. 知覺行為控制構面對於行為意圖構面有正向影響，由圖 15.之SmartPLS路徑分析結果可知，知覺行為控制構面與行為意圖構面假說影響關係係數為0.139，t值為3.193大於2.58，達到p小於0.01之顯著性，所以支持假說H6成立。

(13) H7a.適應不良獎勵構面對於行為意圖構面沒有負向影響，由圖 15.之SmartPLS路徑分析結果可知，知覺行為控制構面與行為意圖構面假說影響關係係數為-0.308，t值為5.826大於3.28，達到p小於0.001之強顯著性；然而本題型原設計為反向題，分數越大更說明大眾認為多因子驗證不理想因而萌生捨棄意圖，統計分析中可發現大眾填寫適應不良獎勵構面之題項普遍低分，路徑係數為負，所以假說H7a不成立。

(14) H7b. 適應不良獎勵構面對於態度構面沒有負向影響，由圖 15.之SmartPLS路徑分析結果可知，知覺行為控制構面與行為意圖構面假說影響關係係數為-0.200，t值為5.644大於3.28，達到p小於0.001之強顯著性；然而本題型原設計為反向題，分數越大更說明大眾認為多因子驗證不理想因而萌生捨棄意圖，統計分析中可發現大眾填寫適應不良獎勵構面之題項普遍低分，路徑係數為負，所以假說H7b不成立。

根據以上數據，本研究做出以下假說整理表18所示。

表 20.本研究假說檢定之整理表

	研究假說	路徑係數	t 值	是否成立
H1a	感知威脅嚴重性對於行為態度有正向影響	0.014	0.344	否
H1b	感知威脅嚴重性對於主觀規範有正向影響	-0.022	0.451	否
H1c	感知威脅嚴重性對於知覺行為控制有負向影響	-0.171**	3.006	是
H2a	感知威脅可能性對於行為態度有正向影響	0.128**	3.572	是
H2b	感知威脅可能性對於主觀規範有正向影響	0.136*	2.397	是
H2c	感知威脅可能性對於知覺行為控制有正向影響	0.148*	2.280	是
H3a	反應有效性對於行為態度有正向影響	0.678**	16.189	是
H3b	反應有效性對於主觀規範有正向影響	0.558**	10.394	是
H3c	反應有效性對於知覺行為控制有負向影響	0.198**	2.961	是
H4	行為態度對於行為意圖有正向影響	0.290**	4.872	是
H5	主觀規範對於行為意圖有正向影響	0.312**	5.753	是
H6	知覺行為控制對於行為意圖有正向影響	0.139**	3.193	是
H7a	適應不良獎勵對於行為意圖有負向影響	-0.308**	5.826	否
H7b	適應不良獎勵對於行為態度有負向影響	-0.200**	5.644	否

*p 小於 0.05; **p 小於 0.01

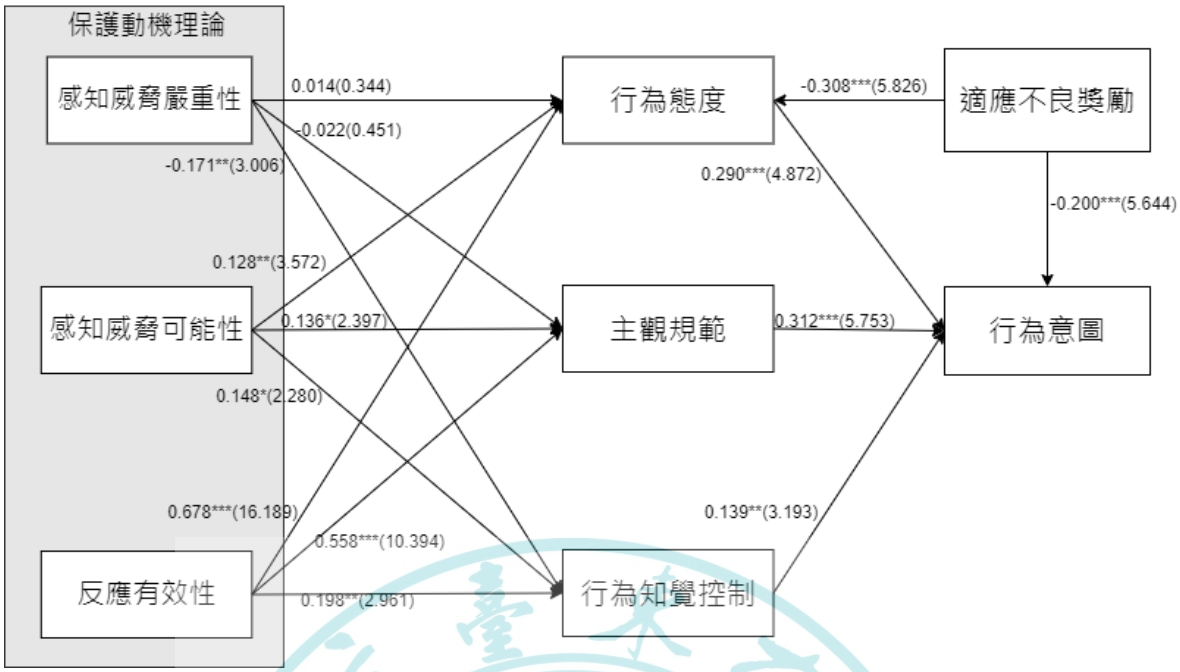

圖 15. 本研究模型統計路徑分析

第五章 結論與建議

本研究主要計畫行為理論結合保護動機理論之角度出發，探討平民大眾對於多因子驗證的採用因素。藉由相關研究文獻，據以發展混合模型藉以完備單項模型的預測力；研究者並藉由最小偏平方法，針對研究假說與概念架構進行驗證並檢核之。本章共分為四個節，第一節主要針對本研究的驗證結果進行說明與探討，為各構面之研究結論；第二節為本研究整理看法，歸納出研究之建議；第三節主要為說明本研究之限制；第四節針對未來的研究發展，整理未來展望。

5.1 研究結論

一、研究樣本資料分析

由第四章樣本資料之描述性分析中，可探究到本研究的樣本對象基本資料例如年齡、職業別、學歷等項目分布的相當分散，因此樣本數量顯得至關重要，若在樣本量有限條件下將會使得模型預測例受限。

二、感知威脅嚴重性相關假說的因果影響

本研究於研究假說構面中提出「感知威脅嚴重性對於行為態度有正向影響」、「感知威脅嚴重性對於主觀規範有正向影響」，然而實證統計研究發現此兩假說並不成立。

可見僅僅感知威脅嚴重性並不足以喚起足夠強烈的保護動機以及行為意圖，根據多件有關保護動機理論的文獻中也提及「感知威脅嚴重性對於行動意願的影響可能有限」(Fischer-Preßler et al.,2022; Ferrer et al.,2018; Plotnikoff & Higginbotham, 2002)，如同研究者先前於第二章第二節提到的保護動機啟動機制，在當事人接收到危害訊息後，還需感知到災害可能落在自己身上時才激起保護欲。另者可歸因於現代生活資訊超載而導致大眾反應鈍化(Sunstein, 2020)。

三、反應有效性的對於行為態度的強因果影響

本研究分析結果顯示，反應有效性構面對行為態度構面有強烈正向顯著的影響。根據PLS之統計分析結果顯示，反應有效性與行為態度之間的的路徑t值高達16.189，P值小於0.001，存在強烈顯著的正向影響關係。問卷回饋彙整成圖表後可以看出大多數作答者對於反應有效性抱有強烈認同感，構面中各題都皆呈現明顯右偏J型分布，可推論當大眾對於資安措施抱持認同感，並認為其足以保護資料安全時可以顯著增進施行資安措施的態度。

四、反應有效性的對於主觀規範的強因果影響

本研究分析結果顯示，反應有效性構面對主觀規範構面有強烈正向顯著的影響。根據PLS之統計分析結果顯示，反應有效性與行為態度之間的的路徑T值高達10.394，P值小於0.001，存在強烈顯著的正向影響關係。問卷回饋彙整成圖表後可以看出大多數作答者對於反應有效性各題目抱有強烈認同感，構面中各題都皆呈現明顯右偏J型分布，可見當大眾對於資安措施抱持認同感時，並且認為其足以保護資料安全時可以顯著增強對於主觀規範的態度。

五、適應不良獎勵對於行為態度的強顯著影響

根據本研究結果顯示，適應不良獎勵構面對行為態度構面有強顯著關係，適應不良獎勵構面對行為態度構面之路徑係數-0.308，T值高達5.644，p值小於0.001。存在強顯著的影響關係。此構面原設計為負面影響，並在問卷設計為反向題型，若得分數越高越代表受試者對多因子驗證抱持排斥態度。

然而本研究統計分析發現本構面平均分數偏低，意味著雖然多因子驗證額外多加了驗證措施，其額外繁瑣過程雖然會使人們需要額外多花心力設置與解鎖，並且增加了登入難度，但並未因此惡化大眾對於多因子驗證之態度。

六、適應不良獎勵對於使用意圖的強顯著影響

根據本研究結果顯示，適應不良獎勵構面對使用意圖構面有強顯著關係，適應不良獎勵構面對行為態度構面之路徑係數-0.200，T值高達5.826，p值小於0.001。存在強顯著的影響關係。此構面原設計為負面影響，並在問卷設計為反向題型，若得分數越高越代表受試者對多因子驗證抱持排斥態度。

然而本研究統計分析發現本構面平均分數偏低，意味著雖然多因子驗證額外多加了驗證措施，其額外繁瑣過程雖然會使人們需要額外多花心力設置並解鎖，但並未因此降低採用多因子驗證之意圖。

七、感知威脅嚴重性對其他構面的顯著影響，成為二階變項的潛力

儘管研究統計顯示感知威脅嚴重性構面對於態度構面與主觀規範構面不成立顯著關係。然而當研究者嘗試統計感知威脅嚴重性構面與感知威脅可能性構面以及反應有效性構面，分別測得路徑係數0.192**(t=2.938)以及0.381**(t=7.115)皆是強顯著影響，意味著感知威脅嚴重性構面應當是感知威脅可能性構面以及反應有效性構面。此實務研究也印證了Hovland於1953年提出的威脅期望理論，感知威脅嚴重性構面之於感知威脅可能性構面以及反應有效性構面之間具有先後順序之決定性關係。

八、拔除無效路徑，提出修正後模型

本研究所提出模型融合了計畫行為理論之觀點以及保護動機理論之動機起因，根據實證統計研究刪除不成立假說後，修正後新模型如下：

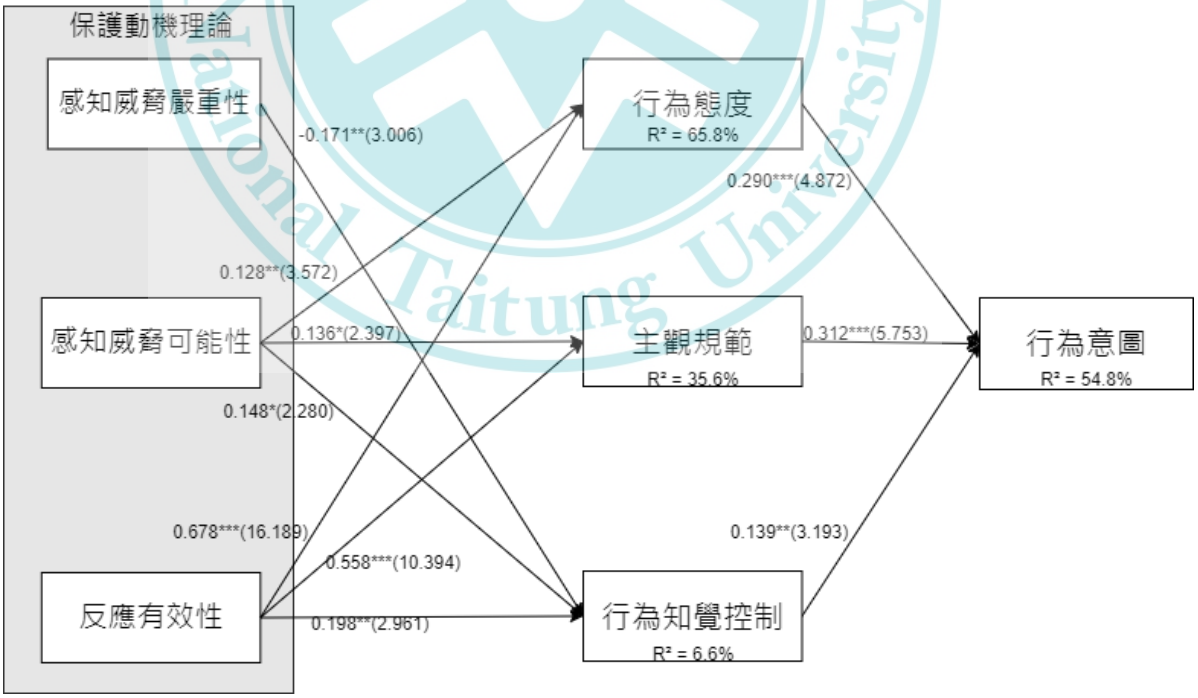

圖 166. 本研究修正模型

5.2 研究建議

本研究主要探討多因子驗證的採用因素以計畫行為理論結合保護動機理論實現，經過發現統計14項假說之中H1a、H1b兩項假說不顯著，並且感知威脅嚴重性與感知威脅可能性以及反應有效性組成強顯著，建議未來研究者將感知威脅嚴重性設定為感知威脅可能性構面或反應有效性構面之前置變數。

根據上一節第五、第六項的分析，適應不良獎勵構面對於行為態度構面、使用意圖構面並未造成顯著負面影響，意味著大眾對於採用多因子驗證所額外帶來的繁瑣程序並不在意。建議後續研究者可以試著改變問法以探討大眾不願採用多因子驗證的隱藏因素。

針對資安政策推廣者建言，研究者根據本研究撰寫歷程認為並非社會大眾不願採用多因子驗證，反而社會大眾在知曉細節之下願意花費更多時間與金錢強化資安並採用該防駭技術，然而因不知曉其技術或不甚瞭解而失之交臂。在問卷第二頁當受試者觀賞完多因子驗證介紹短片後安排一項問題關於「對於多因子驗證之了解程度」，此題採李克特5點量表，完全不懂1分至完全瞭解5分，發現其問項與反應有效性、態度呈現高度相關，T值分別為5.167和3.836，這兩個構面在本研究模型中佔有舉足輕重的角色，最終能顯著影響使用意圖，說明了認知程度之於最終行為意圖具有強烈影響力。而問卷第一頁末題問及「對多因子驗證/二段式驗證之瞭解程度」呈現超過半數民眾對此名詞表示陌生，實乃資安教育之重大漏洞。

而推廣保護意識時，無論是資訊安全抑或是交通安全、健康教育、理財規劃等領域，都需切記「勿一昧地強調危害程度」，因為多項研究文獻、本研究、保護動機理論的援引論文皆表示「單就感知威脅嚴重性對於保護動機的影響力有限」(Fischer-Preßler et al.,2022; Ferrer et al.,2018; Plotnikoff & Higginbotham, 2002; Hovland et al.,1953)。若要達到引起恐懼感而強化保護意識還須提供面臨危害可能性以及有效合理的保護措施。

若要推廣多因子驗證使之普及藉以強化全民資安，其基本教育工作尚有一大段里程，尤其是35歲以上壯年族群或長青族群，其族群對於資訊科技尚為陌生，也是社會中堅分子、處於一生中累積最多資產乃至於準備養老的年紀，近年臺灣國內智慧型犯罪橫行(法務部,2023;警政統計查詢網,2023; 唐筱恬,2023)，尤其壯年、

長青族群因對網路科技不熟悉乃網路犯罪高風險受害族群，一旦受害對其未來退休養老生活規劃影響甚鉅，資安教育刻不容緩。

5.3 研究限制與未來展望

人非聖賢，孰能無過。雖然本研究過程中對概念架構、研究方法、文獻探討、實證調查、回收問卷、資料統計分析等項目力求完美，在有限的財力、物力、人力等現實限制之下終究有不周到之處。探討本研究模型部分構面R平方值過低可能導致模型適配度不足問題，雖國際科學期刊也偶有R平方值不足10%之情事，然力求R平方值提高以提升模型適配度乃天經地義，現有樣本取自多樣化發放管道，因此樣本人口特性如職業別、教育水平、年齡層等因子呈現高相異度而導致樣本族群分散，若能增加採集樣本量可望提升R平方值。礙於篇幅與時間等因素，本研究僅提出部分人口變數對於各構面之影響，例如年齡之於資安知識、資安知識之於態度與反應有效性.....等，若尚有餘裕，例如職業別之於反應有效性與態度與知覺控制行為、年齡與學經歷之於知覺控制行為.....等不同因子交叉比對將可能淘出違反直覺的隱藏規律。

參考文獻

中文部分

1. 110 年國家資通安全情勢報告（110 年版）【資料檔】。台北市：行政院
2. Fan,P.(2023 年 5 月 11 日)。身份認證威脅防禦與實例分享。「CYBERSEC 2023 臺灣資安大會」現場演講，台北南港展覽二館。
3. 國家資通安全發展方案(110 年至 113 年)（110 年版）【資料檔】行政院國家資通安全會報 。台北市：行政院
4. 徐韻修（2019）。資安監控中心為基礎之網路資訊系統縱深防禦架構之研究。〔碩士論文。國防大學〕臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/gtymh2。
5. 方景立（2016）。具情境感知結合貝氏定理的適應性身分驗證技術。〔碩士論文。國立高雄應用科技大學〕臺灣博碩士論文知識加值系統。https://hdl.handle.net/11296/m2ad6f。
6. 朱惠中 (2021,NOV.)。 疫情改變工作環境，防資安破口於未然。CI 學堂 No.36(57-63)
7. 林子婷（2011）。影響民眾對節能減碳政策支持度之因素。〔碩士論文。國立中山大學〕臺灣博碩士論文知識加值系統。 https://hdl.handle.net/11296/xscsnr。
8. 沙依仁(民 96)。人類行為與社會環境(修訂版)。台北：五南圖書出版。
9. 王震武, 林文瑛, 林烘煜, 張郁雯, 陳學志(2008)。心理學(二版)。台北：學富文化。ISBN：9789866624094
10. 翁浩正(2023 年 5 月 11 日)。攻擊者視野中的零信任架構。「CYBERSEC 2023 臺灣資安大會」現場演講，台北南港展覽二館。
11. 蔡志敏（2014）。資訊科技教育政策接受模式之建立 －以教師 e 化教學自我效能及教師 使用新科技之態度為例。〔博士論文。國立臺灣師範大學〕臺灣博碩士論文知識加值系統。 https://hdl.handle.net/11296/ffe323。
12. 鍾易詩、翁士博(2014) 年輕機車駕駛超速行為分析：習慣與計畫行為模式。 運輸學刊 ，26(4)，467-495

13. 陳育徽(2023年5月11日)。去邊界化，端點防護非比尋常。「CYBERSEC 2023臺灣資安大會」現場演講，台北南港展覽二館。
14. 黃惠婷，意圖與動機-評最高法院九十六年台上字第五九八號判決，月旦法學雜誌，154期，頁252-260，2008年3月。
15. 黃意雯（2022）。COVID-19 疫情下消費者移轉至線上飲食外送平台的行為研究—整合保護動機理論與計畫行為理論的觀點。〔碩士論文。國立高雄科技大學〕臺灣博碩士論文知識加值系統。 https://hdl.handle.net/11296/wx2whk。
16. 龍冠海(民60)。社會學　(五版)。台北：三民書局。

外文部分

1. Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In Action control: From cognition to behavior (pp. 11-39). Berlin, Heidelberg: Springer Berlin Heidelberg.
2. Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.
3. Ajzen, I. (2006). Behavioral interventions based on the theory of planned behavior.
4. Ajzen, I. (2011) The theory of planned behaviour: Reactions and reflections. Psychology & Health, 26:9, 1113-1127, DOI: 10.1080/08870446.2011.613995
5. Ajzen, I. (2012). Martin Fishbein's Legacy: The Reasoned Action Approach. Annals of The American Academy of Political and Social Science - ANN AMER ACAD POLIT SOC SCI. 640. 11-27. 10.1177/0002716211423363.
6. Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. Human Behavior and Emerging Technologies, 2(4), 314-324.
7. Ajzen, I. and Madden, T. J.(1986). Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral-control, Journal ofExperimental Social Psychology, Vol.22(5), 453-474.
8. Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. Psychological bulletin, 84(5), 888.
9. Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: PrenticeóHall.
10. Atkinson, J. W. (1958). Motives in fantasy, action, and society: A method of assessment and study. Princeton, N.J.: Van Nostrand
11. Ayereby, M. P. M. (2018). Overcoming data breaches and human factors in minimizing threats to cyber-security ecosystems (Doctoral dissertation, Walden University).
12. Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191
13. Bandura, A. (1986). Social foundations of thought and action. Englewood Cliffs, NJ, 1986(23-28).
14. Boer, H.; Mashamba, M. T. (2005). "Psychosocial correlates of HIV protection motivation among black adolescents in Venda, South Africa". AIDS Education and

Prevention 17 (6): 590–602. doi:10.1521/aeap.2005.17.6.590. PMID 16398579.https://dx.doi.org/10.1521%2Faeap.2005.17.6.590

15. Bollen, K. A., & Stine, R. A. (1992). Bootstrapping Goodness-of-Fit Measures in Structural Equation Models. Sociological Methods & Research, 21, 205-229. https://doi.org/10.1177/0049124192021002004
16. Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. Communications of the ACM, 58(7), 78–87. doi10.11452699390
17. Brown A. S & E Bracken (2004) Generating and remembering passwords. DOI: 10.1002/acp.1014
18. Candrick ,W.(2021) 3 Steps to Stop Employees From Taking Cyber Bait: How to turn employees into cybersecurity assets. Gartner
19. Chan, D. K., Zhang, C.-Q., & Weman-Josefsson, K. (2021). Why people failed to adhere to COVID-19 preventive behaviors? Perspectives from an integrated behavior change model. Infection Control & Hospital Epidemiology, 42(3), 375-376.
20. Cho, K., Kim, K. M., Kim, S., & Kim, H. K. (2018). Towards a better understanding of two-factor authentication adoption: A systematic literature review. Computers & Security, 78, 196-219.
21. Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. (2018). The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18). Association for Computing Machinery, New York, NY, USA, 196–203. https://doi.org/10.1145/3176258.3176332
22. Churchhouse, R., & Churchhouse, R. F. (2002). Codes and ciphers: Julius Caesar, the Enigma, and the Internet. Cambridge University Press.
23. COCHRAN, A. (1981). THE ENIGMA WAR-THE INSIDE STORY OF THE GERMAN ENIGMA CODES AND HOW THE ALLIES BROKE THEM-GARLINSKI, J.
24. Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test, MIS Quarterly 20, 189-211.
25. Contreras, J. L. (2013). Developing a framework to improve critical infrastructure cybersecurity (response to nist request for information docket no. 130208119-3119-01). Available at SSRN 2248658.

26. Dastane, O. & Bakon, K. & Johari, Z. (2020). The Effect of Bad Password Habits on Personal Data Breach. International Journal of Emerging Trends in Engineering Research. 8. 6950-6960. 10.30534/ijeter/2020/538102020.
27. Deloitte Touche Tohmatsu LLC (2022) Insider Threat Mitigation:A holistic & risk-based program Retrieved Apr 28, 2023 from https://www2.deloitte.com/in/en/pages/risk/articles/Insider-Threat-Mitigation-A-holistic-and-risk-based-program.html
28. Dugo, T. (2007). The insider threat to organizational information security: A structural model and empirical test (Doctoral dissertation).
29. Dulany, D. E. (1968). Awareness, rules, and propositional control: A confrontation with SR behavior theory.
30. Edwards, W. (1954). The theory of decision making. Psychological Bulletin, 51(4), 380–417. https://doi.org/10.1037/h0053870
31. Engle, R. L., Dimitriadi, N., Gavidia, J. V., Schlaegel, C., Delanoe, S., Alvarado, I., et al. (2010). Entrepreneurial intent: A twelve-country evaluation of Ajzen's model of planned behavior. International Journal of Entrepreneurial Behaviour & Research, 16(1), 35-57.
32. Feather, N. T. (1959). Subjective probability and decision under uncertainty. Psychological Review, 66(3), 150.
33. Ferrer, R. A., Klein, W. M., Avishai, A., Jones, K., Villegas, M., & Sheeran, P. (2018). When does risk perception predict protection motivation for health threats? A person-by-situation analysis. PloS one, 13(3), e0191994.
34. Fischer-Preßler, D., Bonaretti, D., & Fischbach, K. (2022). A protection-motivation perspective to explain intention to use and continue to use mobile warning systems. Business & Information Systems Engineering, 64(2), 167-182.
35. Fishbein, M. (1967). Attitude and the prediction of behavior. Readings in attitude theory and measurement.
36. Fishbein, M. (2008). Reasoned Action, Theory of. The International Encyclopedia of Communication. doi:10.1002/9781405186407.wbiecr017
37. Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behaviour: An introduction to theory and research. Addison-Wesley.
38. Fortinet, Inc.(2023) 2023 Work-from-Anywhere Global Study Retrieved Apr 30, 2023 Retrieved

https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-WFH-global-study.pdf

39. Gaw S & E. W. Felten(2006) Password management strategies for online accounts. https://doi.org/10.1145/1143120.1143127
40. Glyer,C.(2022) Cyber Signals.January-December 2021 Microsoft.
41. Grandón, E. E., Nasco, S. A., & Mykytyn Jr, P. P. (2011). Comparing theories to explain e-commerce adoption. Journal of Business research, 64(3), 292-298.
42. Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. Journal of Management Information Systems, 28(2), 203–236. doi:10.2753/mis0742-1222280208
43. H. Schulze(2023) 2023 Report Insider Threat.Retrieved Apr 30, 2023 from https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurucul/
44. Heider, F. (1958). The psychology of interpersonal relations. John Wiley & Sons Inc. https://doi.org/10.1037/10628-000
45. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of information systems, 18, 106-125.
46. Hovland, C., Janis, I., & Kelley, H. (1953). Communication and persuasion. New Haven, GT: Yale University Press.
47. IBM. (2022). Cost of a Data BreachReport 2022. Retrieved Jul 20, 2023, from https://www.ibm.com/downloads/cas/3R8N1DZJ
48. IDENTITY THEFT RESOURCE CENTER(2021, Jan 28) 2020 Data Breach Report
49. IDENTITY THEFT RESOURCE CENTER(2022, Jan 24) 2021 Data Breach Report
50. IDENTITY THEFT RESOURCE CENTER(2023, Jan 25) 2022 Data Breach Report
51. Jacomme, C., & Kremer, S. (2018). An Extensive Formal Analysis of Multi-factor Authentication Protocols. 2018 IEEE 31st Computer Security Foundations Symposium (CSF). doi:10.1109/csf.2018.00008
52. Janmaimool, P. (2017). Application of protection motivation theory to investigate sustainable waste management behaviors. Sustainability, 9(7), 1079
53. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS quarterly, 549-566.

54. Jones, E. E., & Davis, K. E. (1965). From acts to dispositions the attribution process in person perception. In Advances in experimental social psychology (Vol. 2, pp. 219-266). Academic Press.
55. Kahn, D. (1996). The Codebreakers: The comprehensive history of secret communication from ancient times to the internet. Simon and Schuster.
56. Kindervag, J. (2010b). Build security into your network's dna: The zero trust network architecture. Forrester Research Inc, 27.
57. Kindervag, J., & Balaouras, S. (2010a). No more chewy centers: Introducing the zero trust model of information security. Forrester Research, 3.
58. LaPiere, R. T. (1934). Attitudes vs. actions. Social forces, 13(2), 230-237.
59. Lennon, R., Rentfro, R., & O'Leary, B. (2010). SOCIAL MARKETING AND DISTRACTED DRIVING BEHAVIORS AMONG YOUNG ADULTS: THE EFFECTIVENESS OF FEAR APPEALS. Academy of Marketing Studies Journal, 14(2).
60. Lewin, K. (1938). The conceptual representation and measurement of psychological forces. Duke University. Contributions to Psychological Theory, 1, 4, 247.
61. Lewin, K. (1951). Field theory in social science: selected theoretical papers (Edited by Dorwin Cartwright.).
62. Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the association for information systems, 11(7), 1.
63. MacDonald, N., Orans, L., & Skorupa, J. (2018). Zero Trust Is an Initial Step on the Roadmap to CARTA. Gartner Research.
64. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of experimental social psychology, 19(5), 469-479. 10.1016/0022-1031(83)90023-9.
65. March, J. G. (1978). Bounded rationality, ambiguity, and the engineering of choice. The bell journal of economics, 587-608.
66. Mitnick, K.&Simon, W.(2003). The Art of Deception: Controlling the Human Element of Security.New York City, United States:John Wiley & Sons
67. Mouton, Francois & Leenen, Louise & Venter, H.s. (2016). Social engineering attack examples, templates and scenarios. Computers & Security. 59. 186 - 209.10.1016/j.cose.2016.03.004

68. Notani, A.S. (1998) Moderators of Perceived Behavioral Control's Predictiveness in the Theory of Planned Behavior: A Meta-Analysis. Journal of Consumer Psychology, 7, 247-241. https://doi.org/10.1207/s15327663jcp0703_02
69. Ogbanufe, O. (2023). Securing online accounts and assets: An examination of personal investments and protection motivation. International Journal of Information Management, 68, 102590.
70. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.
71. Ozkaya, E. (2018). Cyber Security Challenges in Social Media.Doctor of Information Technology. School of Computing and Mathematics. Charles Sturt University.
72. Pagoto, Sherry & McChargue, Dennis & Schneider, Kristin & Cook, Jessica. (2004). Sun Protection Motivational Stages and Behavior: Skin Cancer Risk Profiles. American journal of health behavior. 28. 531-41. 10.5993/AJHB.28.6.6.
73. Papoulis, A., & Unnikrishna Pillai, S. (2002). Probability, random variables and stochastic processes.
74. Petsas, Thanasis & Tsirantonakis, Giorgos & Athanasopoulos, Elias & Ioannidis, Sotiris. (2015). Two-factor authentication: is the world ready?. 1-7. 10.1145/2751323.2751327.
75. Plotnikoff, R.C., & Higginbotham, N. (2002). Protection Motivation Theory and exercise behaviour change for the prevention of heart disease in a high-risk, Australian representative community sample of adults. Psychology, Health & Medicine, 7, 87 - 98.
76. Ponemon Institute (2020)2020 State of Password and Authentication Security Behaviors Report. Retrieved Apr 30, 2023 from nass.org/sites/default/files/2020-04/Yubico%20Report%20Ponemon%202020%20State%20of%20Password%20and%20Authentication%20Security%20Behaviors.pdf
77. Ponnusamy, V., Rafique, K., Liang, L. X., Yichiet, A., & Lee, G. M. (2021). Two-Factor Human Authentication for Mobile Applications. In International Conference on Mobile Computing and Sustainable Informatics: ICMCSI 2020 (pp. 373-382). Springer International Publishing.
78. Reese, K. R. (2018). Evaluating the usability of two-factor authentication. Brigham Young University.

79. Rogers, R & Cacioppo, John & Petty, Richard. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation.
80. Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), Handbook of health behavior research 1: Personal and social determinants (pp. 113–132). Plenum Press.
81. Roncato,C.,Gruber, D. (2021). ESG Research Report: The State of Zero-trust Security Strategies2021 TechTarget.
82. Rosenberg, M. J. (1956). Cognitive structure and attitudinal affect. The Journal of abnormal and social psychology, 53(3), 367.
83. Rotter, J. B. (1954). Social learning and clinical psychology. Prentice-Hall, Inc. https://doi.org/10.1037/10788-000
84. Saini, M. S. (2021). Comparative Analysis of Top 5, 2-Factor Authentication Solutions.
85. Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digital Communications and Networks.
86. Schneier, Bruce.(2005, Feb 18) Schneier on Security: Cryptanalysis of SHA-1.
87. Sheeran, Paschal. (2002) Intention-behavior relations: A conceptual and empirical review. In European review of social psychology, eds. Wolfgang Stroebe and Miles Hewstone. Chichester, UK: Wiley
88. Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. Information Management & Computer Security, 22(1), 42–75. doi:10.1108/imcs-08-2012-0045
89. Stafford, V. A. (2020). Zero trust architecture. NIST Special Publication, 800, 207.
90. Strecher, V.J., DeVellis, B.M., Becker, M.H. and Rosenstock, I.M. (1986) The Role of Self-Efficacy in Achieving Health Behavior Change. Health Education Quarterly, 13, 73-91. https://doi.org/10.1177/109019818601300108
91. Suetonius T. G. (AD 121) Vita Divi Julii. 56.6
92. Sunstein, C. R. (2020). Too much information: understanding what you don't want to know. MIT Press.
93. Tao X, Dengguo F.(2009) How To Find Weak Input Differences For MD5 Collision Attacks.

94. Taylor S., & Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions.International Journal of Research in Marketing, 12(2), 137-156.
95. Tolman, E. C. (1932). Purposive behavior in animals and men. Century/Random House UK.
96. Triandis, H. C. (1988). Collectivism vs. Individualism: A Reconceptualisation of a Basic Concept in Cross-Cultural Psychology. In G. Verma, & C. Bagley (Eds.), Cross-Cultural Studies of Personality, Attitudes, and Cognition (pp. 60-95). London: Macmillan. https://doi.org/10.1007/978-1-349-08120-2_3
97. Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. science, 211(4481), 453-458.
98. Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). Encyclopedia of cryptography and security. Springer Science & Business Media.
99. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190–198. doi:10.1016/j.im.2012.04.002
100. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186-204.
101. Venkatesh, V., Morris, M. G., & Ackerman, P. L. (2000). A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. Organizational Behavior and Human Decision Processes, 83(1), 33-60
102. Verizon Business. (2021). 2021 Data Breach Investigations Report. Retrieved May 7, 2023 from https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report/
103. Verizon Communications Inc.(2022) 2022-data-breach-investigations-report-dbir Retrieved Apr 25, 2023 from https://www.verizon.com/business/resources/Tc0a/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
104. Wang, X., Jiang, Y., Liu, C., & Chen, Y. (2017). A Survey of Password Security Research. Journal of Computer and Communications, 5(11), 1-9.
105. Ward, R., & Beyer, B. (2014). Beyondcorp: A new approach to enterprise security.

106. ゼロトラストアーキテクチャ適用方針（令和４年）【資料檔】東京都：デジタル庁

網路文獻

1. Australian Cyber Security Centre,ACSC(n.d.)”Data Breach” Retrieved May 10, 2023,from https://www.cyber.gov.au/learn-basics/explore-basics/watch-out-threats/data-breach
2. Flynn, J.(2023) 17 ESSENTIAL MULTI-FACTOR AUTHENTICATION (MFA) STATISTICS [2023] Zippia Retrieved Jun 12, 2023,from https://www.zippia.com/advice/mfa-statistics/
3. Comeau,Z. (2022) Microsoft Says MFA Adoption Is Still Terribly Low. Commercial Integrator. Retrieved Jul 9, 2023, from https://www.commercialintegrator.com/networks/information_technology/microsoft-says-mfa-adoption-is-still-terribly-low/
4. Duo Security,Cisco. (2016) What is Two-Factor Authentication? (2FA). Retrieved Dec 19, 2023,from https://www.youtube.com/watch?v=0mvCeNsTa1g
5. FIDO Alliance (n.d.) User Authentication Specifications Overview. Retrieved Jun 6, 2023,from https://fidoalliance.org/specifications/
6. Fitzpatrick,J. (2022) Keeping you safe online with Google and beyond. Google SAFETY & SECURITY. Retrieved Jul 9, 2023, from https://blog.google/technology/safety-security/safer-internet-day-2022/
7. Galletto, N. & Powers, E. & Murphy, T.(2019)Cyber, cyber everywhere: Is your cyber strategy everywhere too? Retrieved May 7, 2023,from https://www2.deloitte.com/us/en/insights/topics/risk-management/cyber-security-threats.html
8. Harris Poll & Google (2019) Online Security Survey.Retrieved Jun 21, 2023, from https://services.google.com/fh/files/blogs/google_security_infographic.pdf
9. iThome（民 107 年 4 月 7 日）。【iThome 2018 企業資安大調查：資安事件衝擊篇】員工資安意識不足的威脅，比駭客更大 民 112 年 4 月 29 日取自 https://www.ithome.com.tw/article/122191

10. iThome（民 110 年 5 月 12 日）【iThome 2021 企業資安大調查：資安挑戰】今年臺灣企業最關心的資安威脅是什麼？ 民 112 年 4 月 29 日取自 https://www.ithome.com.tw/article/144236
11. Jason Smathers is charged with stealing his employer's subscriber list and selling it".Retrieved May 10, 2023,from https://money.cnn.com/2004/06/23/technology/aol_spam/
12. Meng-Yi Wu (2020) PUF-based HRoT Design, Function and Application. 2020 晶片安全論壇。PUFsecurity Corp. Retrieved Jun 5, 2023,from https://www.youtube.com/watch?v=YHoc91xi5ao&ab_channel=PUFsecurityCorp.
13. Musthaler, L. (2006). How social engineering sinks security. Network World, 23(39), 45.Retrieved May 4, 2023,from https://search.proquest.com/docview/215993673.
14. Nabe,C.(2020) Impact of COVID-19 on Cybersecurity
15. National Science Foundation.(n.d.) NSF and The Birth of the Internet 1960s. Retrieved Apr 15, 2023
16. Privacy Rights Clearinghouse(n.d.)"Data Breach Chronology"Retrieved May 10, 2023,from https://privacyrights.org/data-breaches, Retrieved Apr 22, 2023, fromhttps://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
17. Rosencrance,L.& Loshin,P.& Cobb,M.(2020)two-factor authentication (2FA) Retrieved May 27, 2023,from https://www.techtarget.com/searchsecurity/definition/two-factor-authentication
18. Twitter (2021) Account Security Twitter Transparency. Retrieved Jun 14, 2023,from https://transparency.twitter.com/en/reports/account-security.html#2021-jan-jun
19. Walker, L. & Weinert, A. (2020) Breaking Password Dependencies: Challenges in the Final Mile at Microsoft. RSA Conference. Retrieved Jul 10, 2023, from https://www.youtube.com/watch?v=B_mhJO2qHlQ
20. Whitney,L.(2019)More companies use multi-factor authentication, but security still weak from poor password habits. TechRepublic. Retrieved Jun 12, 2023,from https://www.techrepublic.com/article/more-companies-use-multi-factor-authentication-but-security-still-weak-from-poor-password-habits/
21. fromhttps://www.nsf.gov/news/special_reports/nsf-net/textonly/60s.jsp
22. CNN. (2004,Jun 23)"AOL worker arrested in spam scheme

23. Ugoretz, T. [The Aspen Institute] (2020,Apr17)“Fight Back: Stopping Cyber Criminals During a Pandemic”[Video].14:12~14:32 https://www.youtube.com/watch?v=19cfBGtIouc
24. Hagan, E. (2020,Jun. 4) On Adaptive and Maladaptive Patterns. convergence-and-integration-in-psychotherapy. Psychology Today. Retrieved Jul 10, 2023, from https://www.psychologytoday.com/intl/blog/convergence-and-integration-in-psychotherapy/202006/on-adaptive-and-maladaptive-patterns
25. The White House (2021,MAY 12)"Executive Order on Improving the Nation’s Cybersecurity" Retrieved May 10, 2023,from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
26. Li,A.(2022,Feb. 8) Google auto-enabled 2SV for over 150M people leading to 50% decrease in compromised accounts. 9 TO 5 Google. Retrieved Jun 12, 2023,from https://9to5google.com/2022/02/08/google-account-2sv/
27. Jones C. (2022, Nov 24) The Most Significant Password Breaches Of 2021 Retrieved Dec 8, 2022, from https://expertinsights.com/insights/the-most-significant-password-breaches/
28. NIST(2022,Dec 21) Implementing a Zero Trust Architecture (2nd Preliminary Draft)Retrieved May 17, 2023,from https://csrc.nist.gov/publications/detail/sp/1800-35/draft
29. De Backer,A.(2023,Mar. 24) Quelles sont les bonnes pratiques en matière d'hygiène des mots de passe à adopter en télétravail ? Retrieved May 5, 2023,from https://www.journaldunet.com/solutions/dsi/1520309-quelles-sont-les-bonnes-pratiques-en-matiere-d-hygiene-des-mots-de-passe-a-adopter-en-teletravail/
30. Cambridge Dictionary(n.d.) “data-breach”Retrieved May 7, 2023,from https://dictionary.cambridge.org/dictionary/english/data-breach
31. ICO.(n.d) "Personal data breaches" Retrieved May 7, 2023,from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches
32. VMware(n.d.)"Zero Trust Security" Retrieved May 14, 2023,from https://www.vmware.com/topics/glossary/content/zero-trust-security.html
33. 李中仁(民 107 年 5 月)以多因子驗證機制強化身分驗證之安全性。財金資訊季刊 / No.92 /財金資訊股份有限公司 民 112 年 5 月 28 日 檢自

https://www.fisc.com.tw/Upload/a19a130b-bb71-43e5-aaec-4c94a3765907/TC/9206.pdf

34. 林俊宏（民 112 年 1 月 22 日）【全文】11 情治系統個資全遭洩　健保署前主祕神祕帳戶爆鉅款匯入。 鏡週刊 民 112 年 5 月 10 日 檢自 https://www.mirrormedia.mg/story/20230117inv006/
35. 羅正漢（民 110 年 12 月 14 日）2021 政府機關資安現況揭露，近年三級事件通報人為疏失是主因 民 112 年 4 月 26 日 檢自 https://www.ithome.com.tw/news/148431
36. 羅正漢(民 112 年 1 月 16 日)【2023 資安趨勢 1：零信任、身分安全、可信任供應鏈】零信任網路安全步入廣泛實踐的道路。 iThome 民 112 年 5 月 17 日 檢自 https://www.ithome.com.tw/news/155119
37. 鄭閔聲、史書華 (民 112 年 3 月 7 日) 15 萬如何買下 2300 萬人？《天下》深入白帽駭客圈，還原個資賤售荒唐錄。 天下雜誌 民 112 年 5 月 10 日 檢自 https://www.cw.com.tw/article/5124927
38. 陳冠億(民 109 年 3 月 31 號)雙因子認證 / 多因子認證機制 - 加強身分驗證之安全性。 Kenny's technology blog 民 112 年 5 月 28 日 檢自 https://reurl.cc/ed6A3b
39. 唐筱恬(民 112 年 06 月 28 日)詐騙之島－現象篇》僅 6%國人沒接過騙人訊息，台灣為何慘淪詐騙之島？ 新傳媒。民 113 年 1 月 6 日 檢自 https://new7.storm.mg/article/4802546

附錄(本研究問卷問卷）

多因子驗證保護帳號行為動機探討之研究

感謝您撥空填寫這份問卷，本問卷目的旨在探討社會大眾對於資安技術的認知研究。問卷採匿名形式填寫，您在問卷中所提供的資訊，僅作為學術研究用途不會對外公開，敬請安心填寫。您的意見對我們非常重要，衷心期盼您依自己的實際感受填答。感謝您的熱情支持與協助！

敬祝 身體健康 萬事如意

國立台東大學 資訊管理所研究生：曾善勤 敬上

指導教授：陳宜樫 博士

多因子驗證是一種多層保障資料的方法(CISA)。常見的帳號密碼組合是為一道因子；若同時混用多項驗證手法例如指紋、IC卡、簡訊、電郵等驗證因子可以大幅減少資料被竊的機率。例如操作ATM時，輸入密碼是為一道驗證因子，插入帳戶專屬IC卡是為第二道驗證因子。

壹、受試者個人基本資料

1. 性別
□生理男 □生理女

2. 請問您的年齡？
□18歲以下 □18~25歲 □25~35歲 □35~45歲 □45~55歲 □55~65歲 □65歲以上

3.請問您的學經歷？
□國中 □高中 □大專 □一般大學 □科技大學 □研究所

4.您的工作狀態?
□待業 □兼職 □實習 □正職

5. 請問您從事的職業別:
□軍公教 □資訊科技業 □金融業 □製造業 □醫療業 □服務業 □自由業 □學生 □其他

6.您平均一天使用網路多久？
□半小時以內 □1至3小時 □3至5小時 □5小時以上

7.您知道多因子驗證或是二段式驗證嗎?
□不知道 □聽說過 □知道 □偶爾使用(一週至少1次) □經常使用(一週5次或以上)

8.您常使用的網路服務?(複選)
□ 社群軟體 (Facebook、Instagram、Twitter、VK、Dcard…..等)
□ 通訊軟體 (Line、WeChat、Telegram、Discord…..等)
□ 影片平台 (YouTube、Netflix、Disney+、Amazon Prime……等)
□ 帳號同步化平台 (Google、Apple ID、Samsung帳號、小米帳戶 、Yahoo …..等)
□ 金流服務 (網路ATM、電子支付、網路銀行、網路證券交易……等)
□ 網路休閒類 (線上遊戲、網路購物、網路論壇…….等)
□ 其他:_____

貳、正式問卷題目

A. 感知威脅嚴重性 主觀認為敏感資訊外洩的嚴重程度		非常不同意	不同意	尚可	同意	非常同意
1	您會覺得如果資料外洩會造成嚴重的財務損失。					
2	您會覺得如果資料外洩將會造成嚴重的非財務損失。					
3	您會覺得如果您的帳號被駭將會是個嚴重問題。					
4	您會覺得如果您所屬的單位資料外洩將會是個嚴重問題。					
5	整體而言，您覺得資料外洩會造成嚴重的資安威脅。					
B. 感知威脅可能性 主觀認為敏感資訊外洩的可能性		非常不同意	不同意	尚可	同意	非常同意
1	您會覺得資料外洩或駭客入侵事件是很常見的。					
2	您會覺得您的資料有可能已經外洩了。					
3	您會覺得您的網路帳號可能有被侵駭過了。					
4	您會覺得您周遭親友的資料、帳號仍可能受到侵駭。					
5	您會覺得您的資料或帳號有可能被外洩或受到駭客入侵。					
C. 反應有效性 主觀認為採取保護措施的效果		非常不同意	不同意	尚可	同意	非常同意
1	您會認為遵守資安規範可有效減少被駭可能性。					
2	您會遵守資安規範以有效減少被駭可能性。					
3	您會使用多因子驗證以有效減少被駭可能性。					
4	您會使用多因子驗證以有效降低資料外洩的可能。					
5	您會認為採用多因子驗證能有效反應資安防護的需求。					
D. 態度 主觀如何看待多因子驗證		非常不同意	不同意	尚可	同意	非常同意
1	您會認為採用多因子驗證可以有效預防資安威脅。					
2	您會認為採用多因子驗證是個好主意。					
3	您會認為多因子驗證是個很重要的防駭技術。					
4	您會認為多因子驗證應該要更普及。					
5	您會認為在特定資安預防情境應該強制使用多因子驗證。					

E. 主觀規範 重要他人對主觀認知的影響力		非常不同意	不同意	尚可	同意	非常同意
1	您親朋好友會認為您應採用多因子驗證。					
2	您的長官或同事會建議您採用多因子驗證。					
3	您資訊專長朋友會建議您採用多因子驗證。					
4	您周遭的利壞關係人會認為您應採用多因子驗證。					
5	您會認為各類公民營組織或個人都應採用多因子驗證。					
F. 知覺行為控制 主觀認為自身應付難題的能力		非常不同意	不同意	尚可	同意	非常同意
1	您會認為採用多因子驗證很容易。					
2	您會認為遇到資安侵駭事件時，您可以從容應對。					
3	您會認為自身的資訊技術有信心。					
4	如果遭遇資訊領域的問題，您知道從哪找資源。					
5	如果您無法成功採用多因子驗證，有人可以幫忙達成。					
G. 適應不良獎勵 不採用多因子驗證的潛在動機		非常不同意	不同意	尚可	同意	非常同意
1	您認為不採用多因子驗證比較省事					
2	您寧願不採用多因子驗證					
3	多因子驗證在世界上不存在的話對您比較有益處					
4	強制採用多因子驗證的話對您造成困擾					
5	您不希望各公家及私人團體倡議採用多因子驗證					
H. 行為意圖 採用多因子驗證的意圖		非常不同意	不同意	尚可	同意	非常同意
1	在未來，您有意願有採用多因子驗證。					
2	您有意願為個人資訊安全的需要採用多因子驗證。					
3	您有意願推薦周遭親友採用多因子驗證。					
4	您願意花費更多時間採用多因子驗證以增進資安等級。					
5	您願意花費更多金錢採用多因子驗證以增進資安防護。					

問卷到此結束!感謝撥冗回答!