東海大學企業管理學研究所

碩士學位論文

使用者違反資訊安全行為意圖之研究

A study on Individuals' Information Systems Security Violations

指導教授：張榮庭 博士

研 究 生：丁紫涵 撰

中華民國一〇二年七月

論文名稱： 使用者違反資訊安全行為意圖之研究
校所名稱：東海大學企管系碩士班
畢業時間：2013 年 7 月
研究生：丁紫涵　　**指導教授：**張榮庭 博士

中文摘要

隨著資訊科技的發展，網路為人們生活帶來方便與快速，但是也替人們帶來資訊安全帶來威脅。網路中的惡意軟體，如釣魚網站、釣魚信件與電腦病毒等迅速蔓延，嚴重的威脅到個人的資訊安全。在過去的研究中都以正向觀點探討個人遵循資訊安全之意圖，鮮少從反向觀點來探討使用者違反資訊安全行為之意圖。

本研究以個人涉險行為為研究的議題，探討知覺風險、知覺利益、信任與資訊安全認知對違反資訊安全行為意圖之影響，並且進一步探討個人的風險傾向對知覺風險的影響力。

本研究採問卷調查法，利用便利抽樣方式蒐集樣本資料，研究對象為學生與一般大眾。研究結果發現，知覺風險對違反資訊安全行為之意圖有負向影響;知覺利益對違反資訊安全行為之意圖有正向影響;信任對違反資訊安全行為之意圖有正向影響;資訊安全認知對違反資訊安全行為之意圖有負向影響，在違反資訊安全行為之意圖中，以對網站的信任最具影響力，且個人的風險傾向對知覺風險也具有影響力。

相較於過去研究聚焦於使用者遵循資訊安全行為的因素，本研究是以反向觀點，探討知覺風險、知覺利益、信任與資訊安全認知對違反資訊安全行為之意圖的影響。希望能幫助學術界與實務界，了解使用者違反資訊安全之意圖的因素。

關鍵字：違反資訊安全行為、知覺風險、知覺利益、信任、資訊安全認知、風險傾向

Title of Thesis：A study on Individuals' Information Systems Security Violations
Name of Institute：Depart of Business Administration, TUNGHAI UNIVERSITY
Graduation Time：07/2013
Student Name：Ding, Zih-Han **Advisor Name**：Dr. Chang, Jung-Ting

Abstract

With the development of technology, the Internet provides computer users convenience and mobility but it also poses challenges of information security. These malwares, such as spyware, phishing, computer virus, keystroke logging code etc., spread rapidly and severely threaten the individual's information security. Previous study of information security is to follow the point of view of information security to prevent people for breaches of information security behavior, but few studies in Information Systems Security field from reverse viewpoint to discuss what factors will be affected when a person make violations of the security.

This paper is concerned with individuals' risky behavior regarding information systems security violations and discusses factors about perceived risk, perceived benefit, trust, and information systems security awareness related to effect information systems security violations. And risk propensity is a predict variable of perceived risk. Data was collected from survey questionnaires by convenient sampling, and collect data from student and member of society. The results shows that perceived risk and information systems security awareness are negatively related to the intention to make violations of the security; perceived benefit and trust are positively related to the intention to make violations of the security. And individual with risk-preference will perceive less risk on an information security violation than one with risk-aversion. Overall speaking, the trust of website exerted greater effect on information security violation.

Keywords： Information Systems Security Violations; Perceived Risk; Perceived Benefit; Trust; Information Systems Security Awareness; Risk Propensity.

致謝

「人的潛力是無限的」、「老天爺只會給人過得去的難關」這兩句話讓我走過了我在研究所中的每一個難題。

這篇論文得以順利完成，首先感謝指導教授張榮庭老師細心叮嚀與督促以及吳祉芸老師的鼓勵與幫助，在這兩位老師用心的教導之下讓我在研究所時期猶如破繭而出不斷突破自我。也謝謝張老師給我出國參加國際會議的機會，讓我能夠到國外增廣見聞。此次的會議經驗對我來說相當重要，不僅讓我有機會可以站在國際會議的舞台上發表文章，也能藉此機會練習自己的英文口說能力。同時，也要感謝口委鄭菲菲教授、吳金山教授與應鳴雄教授，謝謝他們用心審閱我的論文，且在論文口試時不吝指正與建議，使得我的論文能夠更臻完備。

在學期間感謝我的好友妮子、小濱以及施佳妤，因為妳們在我需要幫助時會適時伸出援手，在我低潮時給我滿滿的關心讓我在研究所生活中多了許多的歡笑與溫暖的回憶。謝謝我同門的好友素帆，因為妳的陪伴與貼心讓我在研究的道路上不孤單，也謝謝我同門的欣愉學姊，因為妳的鼓勵讓我在我研究的道路上充滿力量。另外，我也謝謝我的寶貝朋友晴宜、沒毛、宜庭、黃大便、賀老大與肥龍，無論何時何地你們總是在我身旁默默的陪伴、幫助與鼓勵，給我源源不絕的力量朝我的目標走去。也謝謝我的家人，在背後默默支持著我，給我自由與空間讓我可以自由的翱翔與發展。最後我想說的是謝謝你阿毛，因為你給了我信心與勇氣同時也是我最大的精神支柱。因為有你們讓我像蝴蝶般的蛻變。

在充滿謎一樣的未來，我會帶著我在研究所學到的知識與智慧，蛻變成一個獨一無二的人。

丁紫涵 謹 識

於東海大學企業管理學系

2013年7月

目錄

表目錄

圖目錄

第壹章　緒論

隨著網際網路的發展與普及化，民眾的生活與網路已密不可分。近來，新的網路詐騙行為與網路釣魚層出不窮，網路使用者使用網路的不當行為，使個人暴露在潛在的資訊安全相關風險之下，為個人的資訊安全帶來重大的挑戰。接下來，會先介紹目前網路犯罪的情形以及本研究的研究背景與動機及研究目的。

第一節 研究背景與動機

隨著資訊科技進步迅速，網際網路的蓬勃發展，電腦與網際網路已成為每個人生活及工作上必備的工具。網際網路具低成本、便捷、多媒體資料傳輸以及豐富的資訊等多項特質，這些特質使得網際網路的運用範圍不斷擴大。現代人在生活中嚴重的依賴網路，每個人往往電腦開機就是瀏覽網頁、收發電子郵件、下載軟體及上 Facebook 或 Plurk 等社交網站，顯示使用者上網的活躍與頻繁，但這也使使用者暴露在潛在的資訊安全相關風險之下，為個人的資訊安全帶來重大的挑戰。

近年來，危害資訊安全事件例如釣魚網站(phishing website)、釣魚信件(phishing email)、網路詐騙(internet fraud)與網路病毒等層出不窮。《Economist》2007 年的報導中顯示，網路釣魚的攻擊造成重大的經濟損失，造成個人名譽及信用受損之外還包括企業形象與商譽的重大傷害，反網路釣魚工作小組(APWG)在 2008 年 3 月的調查統計，全球釣魚網站數量達到 24,908 個且全球的網路釣魚攻擊通報數量約 25,630 件，損失的金額高達 32 億美元。網路釣魚攻擊猖獗且手法不斷推成出新，資安業者發現愈來愈多的釣魚網站改採 IP 位址顯示，隱藏假冒的網域名稱進行詐騙。賽門鐵克(Symantec)在 2009 年 7 月的新垃圾郵件及網路釣魚報告顯示，以 IP 位址網域的網站主機位置來看，全球共有 1,503 個釣魚網站，分散於 92 個國家，台北市因擁有超過 100 個釣魚網站為全球釣魚主機來源城市第一名。

在過去美國政府對於網路釣魚事件頻頻發出警訊，將其列為未來最嚴重的網路犯罪型態，根據賽門鐵克(Symantec)在 2012 年 7 月的網路安全報告顯示，平均每 475.3 封郵

件中便有一封帶有某種類型的釣魚攻擊。由此可見，網路釣魚的攻擊所造成的資訊安全問題，對企業、組織以及個人造成一個很大的衝擊與危害。

以往釣魚郵件的詐騙類型，不外乎提供商業機會、健身及瘦身減肥騙局、免費贈品、投資機會、信用卡或旅遊獎品促銷等騙取使用者的個人資料例如身份證字號及信用卡號。近來釣魚郵件的詐騙，不再是廣告而是利用近來發燒議題如 2014 年世界盃足球賽或是以假借身分方式取得用戶的信任，進而使用戶自動提供個人資料，如信用卡資料、銀行帳戶或密碼以及身分證等，歹徒再利用這些竊取而來的資料從事不法行為。現代人的日常生活從購物、金融交易到商業買賣均離不開網路，因此對於這一類的犯罪，要更加提高警覺。

許多的資訊安全管理者、輔導人員時常告知使用者在使用網路資源時要注意的事項，以避免資訊安全相關風險的危害。Pattinson et al.,(2012) 的研究指出被告知的參與者管理釣魚郵件優於未被告知的參與者。但為什麼有些人願意承擔一個大的風險，開啟一封疑似是釣魚郵件的電子郵件呢？這可能是企業管理者或資安從業人員輔導業者極想得到的問題的答案。過去許多學者試圖找出影響使用者意圖遵循資訊安全政策的因素，了解使用者的從事網路活動的行為，以預防使用者意圖做出違反資訊安全的行為。本研究則是以反向觀點來看，藉由過去的學者研究，試圖找出是什麼因素使得使用者做出違反資訊安全行為，且這些因素是如何影響使用者意圖違反資訊安全行為。

因此，本研究提出一個違反資訊安全行為的模型，根據過去的文獻探討知覺風險(perceived risk)、知覺利益(perceived benefit)、信任(trust)與資訊安全認知(information systems security awareness)等四個因素對使用者違反資訊安全行為之意圖的影響，並以風險傾向(risk propensity)為知覺風險的預測變數。

第二節 研究目的

近年來，釣魚郵件詐騙的氾濫，使得使用者在從事網路活動時面臨資訊安全相關風險。無論科技如何進步，它主要的目的是要幫助人們可以正確、有效的使用資訊，雖然現今的資訊技術已經為使用者阻擋了大部分的威脅，但是使用者不遵循資訊安全的行為，依然會造成個人資訊安全上的漏洞。使用者了解資訊安全對個人的重要性，但在哪些因素影響下會使使用者做出違反資訊安全行為。根據過去學者的研究結果，本研究以知覺風險、知覺利益、信任與資訊安全認知等四個因素探討使用者違反資訊安全行為之意圖。並探討個人的風險傾向是否會影響知覺風險。

因此，本研究研究目的如下：

- 探討個人的知覺風險、知覺利益、對網站的信任、對朋友的信任與資訊安全認知對使用者違反資訊安全行為意圖之影響。
- 探討上述的影響因子，哪一個對使用者違反資訊安全行為之意圖最具影響力。
- 探討個人的風險傾向對知覺風險是否具有影響力，進而造成使用者違反資訊安全行為，並且探討知覺風險是否為風險傾向與違反資訊安全行為的中介變項。

第三節 研究流程

首先是闡述本研究的背景與動機，確認本研究的主要目的。依據本研究的目，蒐集國內外相關文獻，其範圍包含知覺風險、知覺利益、個人對朋友與網站的信任、個人對資訊安全認知及違反資訊安全行為之意圖等範疇。最後由相關文獻及彙整的理論基礎與知識，提出本研究的模式假設。研究模型的各項構面的操作性定義，參考各文獻的量表及專家意見設計問卷內容並以便利抽樣的方式展開樣本的收集。將回收的問卷加以整理後，利用統計方法與軟體工具進行分析，再針對分析後的資料結果提出合理的解釋，對本研究的假說進行檢定。最後針對資料分析的結果進行彙整，實證本研究的結果，並做出適當的結論與建議。研究流程如圖 1-1 所示：

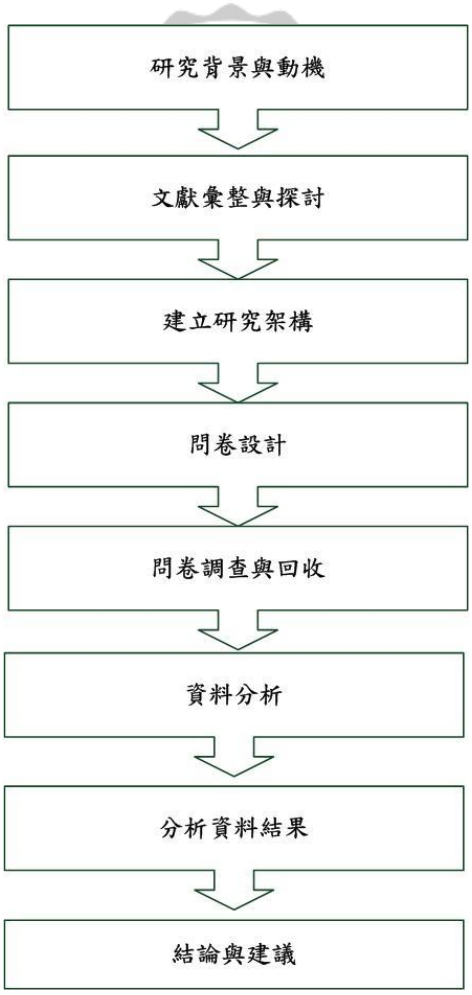

圖 1-1 研究流程

第貳章　文獻探討

本研究的主要目的是探討知覺風險、知覺利益、信任與資訊安全認知等四個因素對使用者違反資訊安全行為意圖之影響，並探討個人的風險傾向對知覺風險之影響。本章節將針對各個研究構面進行相關的文獻探討，以此做為本研究之研究架構基礎。

第一節 資訊系統安全(Information Systems Security)

「資訊」 (information)是由「資料」(data)所產生的，所謂資料指的是一種未經處理的原始文字(word)、數字(number)、符號(symbol)或圖形(graph)等，所表達的只是一種沒有評估價值的基本元素或項目。當資料經過處理(process)，如以特定方式有系統的整理、歸納及分析後，就成為了資訊(周宣光, 2001)。簡而言之，資訊是資料已被整理成對人而言是有意義且有用的格式。現在大部分資訊的收集、處理和存儲皆以電腦處理，並通過網絡傳輸到其他電腦上，資訊是以數位(digital)形式傳遞資料，因此容易被他人非法存取、竄改及偷竊。

資訊系統安全是為了保護資訊避免受多種威脅的攻擊。根據美國資訊安全詞彙(U.S. National Information Systems Security Glossary) 將資訊安全定義為保護資訊和資訊系統，使其免於遭受未經授權的存取、使用、揭露、瓦解、變更或毀損。資訊安全管理的目的在保護電腦資源，包括硬體、軟體、資料、程序及人員，以防止電腦資源被變更、破壞及未授權使用。資訊安全核心目標為必需能保護儲存於資訊系統中資料之機密性(confidentiality)、完整性(integrity)及可用性(availability)(Schneider and Therkalsen, 1990)。機密性為確保資料傳遞與儲存的私密性。完整性為避免非經授權的使用者或處理程序篡改資料。可用性為確保獲得授權的使用者在有需要時可以取得資訊資源。廣義而言，資訊安全就是保護任何與電腦有關事物之安全，應考量的範圍包含電腦軟、硬體、網路、及人員等二大類「技術」與「人」的因素，防止非法存取、竄改、偷竊和對資訊系統造成傷害的一些政策與程序，並藉由技術和工具來保護硬體、軟體、網路和資料，以提昇資料的安全性。電腦軟、硬體、資料及服務資訊等都是資訊系統應該要保護的主要元素，因為這些元素具有不同的資訊風險(Straub Jr and Nance, 1990)。資訊風險的定義為資訊系

統相關資產的弱點，當受到資訊威脅攻擊而造成資訊資產負面的衝擊。

資訊安全的威脅分類為設備故障、軟體故障、潛在的威脅、實體災難、人員錯誤、資料的濫(誤)用及資料遺失等威脅(Hutt,1995)。資訊威脅分為自然災害、技術問題及人為因素等三種來源(Posthumus and Von Solms, 2004)， White et al,, (1996)歸納所有資訊可能的威脅，分為來自「內部安全」即系統面的安全與「外部安全」即非系統面的安全。資訊安全外部的威脅包含天然災害等重大突發事件，外部的駭客及網路病毒等惡意程式的攻擊;內部的威脅包含電腦的相關硬體的損害、員工的破壞及內部網路病毒的傳播等。這些威脅嚴重衝擊到個人、組織和企業的資訊安全,個人或組織員工對資訊系統的濫用，直(間)接造成個人及企業組織嚴重的威脅與衝擊，並導致個人或企業組織的損失及傷害。

第二節 違反資訊安全行為之意圖(Intentions to make IS Violations)

(一) 違反資訊安全行為之意圖定義

過去的資訊安全相關的研究，大多專注在資訊安全的技術面，提出許多資訊安全的衡量標準與系統工具，但從使用者行為面的角度探討資訊安全相關的研究甚少。近來有學者發現個人或組織員工對資訊系統的濫(誤)用的行為，如員工的忽視(ignore)、錯誤(mistake)和惡意的(deliberate)行為會對資訊系統安全造成損害(Bulgurcu et al.,2010; Lee and Lee, 2002)，進而使個人與企業組織暴露在資訊安全相關風險之下。因此，了解使用者違反資訊安全行為之意圖可視為企業資訊安全管理者與資訊安全輔導業者主要關注問題之一。本研究歸納資訊安全行為的違反分為三種類型：個人涉險行為、違反道德但不違反法律以及非法行為。個人涉險行為指的是使用者在有意或無意的狀況下做出違反資訊安全的行為，使得自身暴露在資訊安全相關風險之下造成個人的損失，如使用者在不知名的網站上登入個人資料而導致個資外洩，對自身造成的損失；違反道德但不違反法律，如員工不遵守公司的資訊安全政策或對資訊系統的濫(誤)用，導致組織或公司的損失及傷害；非法行為如盜版及違法下載軟體等侵害到他人的著作權或著作財產權。

本研究以個人的涉險行做為研究的議題，以釣魚郵件為情境設計，了解為什麼使用者意圖做出違反資訊安全的行為。

（二）違反資訊安全行為之意圖構面

科技接受模式(Technology Acceptance Model, TAM)是由(Davis, 1989)所提出，用來建構一個資訊科技接受的行為模式，主要目的在於解釋和預測使用者對資訊系統的接受度。(Davis, 1989)認為信念(beliefs)會影響態度(attitude)，態度再進一步影響行為意圖(intention)，行為意圖對實際使用(actual system use)有顯著且正面的影響。科技接受模式的行為意圖與使用者違反資訊安全行為意圖是相似的，即當使用者從事某項網路活動，假設使用者先會有信念，綜合多個信念轉變為使用者的態度，最後才表現出行為意圖。如線上遊戲的玩家登入某網站就可獲取遊戲寶物，則對此網路活動的態度會趨於正向，縱使可能從事此網路活動可能是不安全的。故本研究以科技接受模式的行為意圖做為使用者違反資訊安全意圖的探討構面。

第三節 知覺風險(Perceived Risk)

（一）知覺風險定義

風險(Risk)的概念可以回溯到 1920 年，指的是在某一特定環境下，某一特定時間段內，某種損失發生的可能性。Mitchell(1999)認為風險是組織或個人發生損失的機率以及損失嚴重性二者的組合，風險強調發生機率，即任一事件的風險為事件的可能發生機率以及事件發生的後果之組合乘積。風險是潛在於一個選擇活動後導致一個損失的可能性與負面的結果。無論風險如何被定義，其核心含義為未來結果的不確定性與損失。

知覺風險的概念最早是由 Bauer(1960)所提出發展至今已被用來廣泛的討論消費者行為，認為消費者所採取購買行為都可能產生無法預期的結果，而且結果可能有些是負面的。消費者購買行為本身就是一種風險，因為消費者無法事先預測購買決策會帶來何種結果，這種無法預測結果的情形就代表風險的存在。

Cox(1967)將 Bauer 的知覺風險概念做更深入的推論，假設消費者購物是目標導向，認為消費者在每次購物時都會產生一個購買目標，當消費者認為購買結果可能不如購買

目標所預期，甚至出現不好結果時，便會產生知覺風險。因此 Cox(1967)提出構成知覺風險的兩種函數：

1. 消費者在進行消費行為前，感覺到會產生不良後果的可能性，意即消費者在購買前所承受的風險程度。

2. 當消費結果為不利時，消費者在個人主觀上所感覺的損失大小，也就是當風險產生時，每個人對於損失程度的感覺有所差異。

Cunningham(1967)是第一位提出雙因素測量模型，針對 Cox(1967)所提出的兩種函數分別給予定義：

1. 不確定性(uncertainty)：消費者對於某風險是否發生的可能性。

2. 結果(consequence)：當事件發生後所導致結果的嚴重性。

故消費者的知覺風險之衡量為不確定性與結果的嚴重性兩者之相乘。Cunningham (1967)亦指出知覺風險的大小對於不同的消費者、不同的環境下會不一樣，當消費者本身的不確定性和損失結果程度較高時，則消費者本身的知覺風險會提高。依據 Cunningham(1967)與 Cox (1967)對知覺風險定義，本研究將知覺風險定義為使用者知覺某一項資安行為發生損失的可能性與損失的嚴重性。

（二）知覺風險構面

過去研究顯示，許多學者為知覺風險具有多個構面。最早將知覺風險區分為不同構面的學者是 Roselius(1971)，主要區分為四種不同因素，包括時間損失(time loss)、危險損失(hazard loss)、自我損失(ego loss)與金錢損失(money loss)。

1. 時間損失(time loss)：購買的某項產品無法使用時，因調整、修理或替換所浪費的時間。

2. 危險損失(hazard loss)：購買的產品無法使用或品質不良時，而造成自身健康及安全上的損失。

3. 自我損失(ego loss)：當購買的產品有瑕疵時，消費者本身會認為因自己愚昧在意他人的看法而感覺自己是愚昧的。

4. 金錢損失(money loss)：當購買的產品是不良或無法使用，為了維修或替換產品而造成金錢上的損失。

Jacoby and Kaplan (1972)則認為知覺風險為以下六個構面財務風險(financial risk)、績效風險(performance risk)、身體風險(physical risk)、心理風險(psychological risk)與時間風險(time risk)及社會風險(social risk)，之後 Stone and Grønhaug (1993)針對財務、績效、身體、心理、時間與社會六種知覺風險構面進行研究後發現，這六種構面對於知覺風險的解釋力高達 88.8%。

由於 Stone and Grønhaug (1993)所提出的構面涵蓋範圍較廣，且解釋力較高。依照 Stone and Grønhaug (1993)的看法，分別解釋知覺風險的六個構面，說明如下：

1. 財務風險(financial risk)：產品無法正常使用或是不能使用，結果會使消費者有財務上的損失。
2. 績效風險(performance risk)：產品未如預期中表現的風險。
3. 身體風險(physical risk)：產品本身會對消費者帶來傷害的風險。
4. 心理風險(psychological risk)：產品或服務無法滿足消費者本身的觀點。
5. 時間風險(time risk)：產品使用或購買需要花費較多的時間而造成的風險。
6. 社會風險(social risk)：購買產品不被他人所認同。

雖然各學者在知覺風險的定義有些許差異，但以上這六種知覺風險的構面，被廣泛使用在衡量消費者購買行為所面臨的風險上。

消費者行為與科技的採納相似都是涉及風險的行為。過去有研究結合其他行為相關理論如科技接受模型、計畫性行為理論、理性行為理論等探討資訊系統管理者接受新科技之意圖，亦有研究顯示知覺風險對創新科技的接受行為具有顯著的負面影響(Swaminathan et al., 1999)。Featherman and Pavlou (2003)整合過去的研究並重新定義知覺風險的財務、功能、時間、心理、社會、隱私與加總風險等構面在預測 e-services 的採納(Chang, 2010)。定義如下：

1. 財務風險(financial risk)：採用的科技技術結果不如預期的能夠保護組織的資產免受威脅，所造成額外的金錢損失。

2. 功能風險(performance risk)：採用的科技技術故障，導致企業須花費更多的時間彌補。

3. 時間風險(time risk)：採用的科技技術需花費時間研究、以及學習如何使用此科技技術而造成時間上的浪費。

4. 心理風險(psychological risk)：採用的科技技術結果不如預期的目標，導致潛在的自尊損失(自我虧損)。

5. 社會風險(social risk)：採用的科技技術造成組織內潛在虧損狀態。

6. 隱私風險(privacy risk)：個人資訊的潛在損失。

7. 加總風險(overall risk)：當所有知覺風險面向一起被評估時，所感受到可能的風險總和。

前面四種風險發生時，管理者會知覺採用的科技技術所產生效益是不足的。上述的知覺風險被廣泛運用在預測 e-services 的採納。

在網路的環境下，使用者在從事某項網路活動時存在一定的風險，如線上提供個人資料、網路金融交易等(Levi and Koç, 2001; Tsai and Yeh, 2010; Youn, 2005)。因此，知覺風險可說是使用者在從事某項網路活動時，所認知到的風險的知覺而非實際存在的風險。假如使用者收到一封電子郵件時，知覺到此郵件是不安全的或開啟此郵件可能會導致電腦中毒或個人資料外洩，則使用者開啟此郵件的意願就會降低。因此，本研究以 Dowling and Staelin (1994)與 Peter(1979)所定義的知覺風險構面，以發生負向結果的機率與負面結果的嚴重性衡量本研究的構面。

第四節 知覺利益(Perceived Benefit)

（一）知覺利益定義

在過去的研究中各學者對於知覺利益有不同的看法。Gutman(1982)指出知覺利益被視為一種結果，此結果能增加個人的效用或有助於達到高層次目標的價值。消費者購買產品不僅在於其產品本身提供之功能可以滿足自身需求外，該產品所提供的附加功能與服務，亦為消費者追求的實質利益(Drennan et al., 2006)。Park et al.,(1986) 認為利益是指消費者關於產品及服務屬性的個人價值和意義的認知，即消費者認為該產品及服務能夠帶給自己的好處與意義。利益依其內含動機可區分為三個種類：功能性利益(functional benefits)、象徵性利益(symbolic benefits) 以及經驗性利益(experiential benefits)。其定義解釋如下：

1. 功能性利益：為產品和服務商品的內在優勢，可提供個體功能上的效用，即強調產品實用、好用等功能性機能。
2. 象徵性利益：指的是產品和服務商品的外部優勢為反應使用者意象，滿足消費者對於社會關係及自我實現的需求。如品牌代表社會地位、財富的炫耀或時尚的品味。
3. 經驗性利益：為同時反應產品相關屬性與非相關屬性，此類利益滿足消費者感官愉悅、新奇及認知性的情感需求。

過去的文獻中已有研究討論知覺利益在網路購物行為的影響力(Alba et al., 1997)。知覺利益在網路購物中的定義有別於傳統的產品取得的定義，因為傳統的產品取得的定義無法完全反應出購物體驗的意義(Bloch and Richins,1983)。Forsythe et al.,(2006)綜合過去學者的研究提出網路購物的兩種利益為功能性利益與非功能性利益。功能性利益包含購物方便性(purchase convenience)、產品選擇性(product selection);非功能性利益包含購物舒適性(product selection)、享樂性(hedonic)等四個構面來衡量網路購物知覺利益。

在消費者購買中，消費者知覺利益就是消費者針對外來的商品資訊所知覺到的價值(Sheth et al., 1999)。Lovelock (1983)認為知覺利益代表消費者個人心理主觀判斷在消費

時所獲得之益處，簡單來說就是某樣商品帶給消費者的好處。同樣的，使用者從事某項網路活動時，也是想從網路活動中獲得益處，例如下載音樂、影片、軟體或與朋友聊天聯繫感情等對網路的活動或資訊所知覺到的利益與意義。

故本研究將知覺利益定義為使用者在進行某項違反資訊安全行為時，心理主觀判斷獲得之益處與意義。

（二）知覺利益構面

Forsythe et al.,(2006) 整理各學者的研究並歸納出知覺利益的四個構面為購物方便性、產品選擇性、購物舒適性及享樂性。

1. 購物方便性：消費者可以隨時從辦公室或家中瀏覽上網購物，不受地點與時間的限制。因此，方便已經是成為網路購物者主要的理由。
2. 產品選擇性：網路商店擁有大量商品資訊，而且比購物型錄提供更好的知覺體驗並且提供更多產品資訊及價格比較可供購物者參考選擇。
3. 購物舒適性：網際網路可讓消費者瀏覽產品，提供廣泛的服務、搜集商品資訊、比較價格、購買產品以及下訂單或更改訂單，不需前往購物商場即可反應意見，也沒有商場的擁擠感覺。
4. 享樂性：可節省時間和金錢、擁有更多的選擇、不用排隊和沒有銷售人員推銷的壓力成為一個更加愉快的購物體驗。

利益知覺主要包括知覺品質(perceived quality)與知覺價值(perceived value)。消費者購買商品行為，知覺利益與知覺價值是相似的，同樣都是想從商品中獲得好處。故本研究以Petrick and Backman(2002)與Zeithaml (1988)提出的知覺價值的構面衡量，分別為產品品質(quality)、貨幣價值(monetary value)、行為價格(behavioral price)、情感性反應(emotional response)與聲譽(reputation)來衡量知覺利益的構面。

第五節 資訊安全認知(Information Systems Security Awareness)

（一）資訊安全認知定義

一般談到資訊安全會讓人聯想到其建立資訊安全周邊環境，如防火牆、認證授權管理、VPN 及入侵偵防系統等，鮮少人會去想到與人員的行為表現有關。一個缺乏資訊安全知識的人可能會做出違反資訊安全的行為，如將重要的資料寄給非授權的人、備忘錄放置網路留言版等，這些行為可能是有意或無意的但是都會導致負面的結果，如重要資訊外流、個人資料的外洩及電腦中毒等。

經濟合作及發展組織理事會(OECD)通過「資訊系統與網路安全準則」修訂，作為其會員國推動資訊安全相關政策、法令的參考準則，其中更對於人員的認知與責任賦予下列的意義：

1. 認知(awareness)：所有參與者均應認知到資訊系統與網路安全的必要性。
2. 責任(responsibility)：所有參與者均應對資訊系統與網路安全負責。

人員對資訊安全的認知能促使和激發人員關心安全相關議題並提醒他們安全實踐的重要。

資訊安全認知的概念是指電腦使用者對資訊的安全認知，其目的在於呈現資訊安全上簡單的重點(Spurling, 1995)，認知使個人對資訊的威脅、攻擊與弱點感到敏感，並可識別出所需保護的資料、資訊與處理的過程。使用者須了解資訊安全的重要性為何，單純的將注意力聚焦在安全上，其目的是讓個人認知到資訊安全相關的議題並作出相對的回應(Wilson and Hash, 2003)。使用者須對資訊安全具有簡單的知識或是對資訊安全主題有認知的概念，以了解資訊安全之利害關係，並將資訊安全知識應用在資訊安全領域上以減少資訊安全風險的發生。NIST提出與資訊系統相關的員工都必須熟悉的資訊安全基礎知識，且要能夠應用以保護資訊與系統(蕭瑞祥、許容豪, 2008)。資訊安全認知對個人與組織運作來說是重要的。

資訊安全認知在組織中扮演重要的角色，在過去的研究中已有大量的文獻在資訊安全認知的訓練，以加強員工遵守資訊安全政策(Bulgurcu et al.,2010; Kwak et al.,2011;

Puhakainen and Ahonen, 2006; Siponen, 2000)。因此，員工遵循資訊安全政策對一個組織運作的成功是重要的(Bulgurcu et al.,2010; Vardi and Weitz, 2003)。即員工的資訊安全認知為有效的資訊安全管理政策的一部分(Cavusoglu, Son, and Benbasat, 2009)，因為員工都了解到他們在資訊安全上的使命。員工對資訊安全認知的缺乏或濫用使組織暴露在資訊風險的威脅之下，並導致企業在信譽或財務上的損失。Bulgurcu et al.,(2010) 的研究中顯示，員工的資訊安全認知會正向影響員工遵循資訊安全政策。因此，提高員工的資訊安全認知對組織來說是必須的。

組織的資訊安全認知與網路使用者的資訊安全認知是相似的。使用者的資訊安全認知不足，導致使用者可能做出違反資訊安全的行為，使自身暴露在資訊相關風險之下。如，瀏覽不知名的網站或登入不知名的社群網站等，而導致電腦中毒或個人資料的外洩。因此，使用者需具備足夠的資訊安全認知，以避免自身暴露在資訊風險威脅下。資訊安全認知主要是要讓使用者瞭解，當資訊安全事件發生時對於組織的運作與相關人員所可能造成的影響，並讓使用者知道重要的資訊安全議題以及對應之道。故本研究將資訊安全認知定義為個人對資訊安全的概念。

（二）資訊安全認知構面

組織中員工資訊安全認知與網路使用者的資訊安全認知是相似的。在Bulgurcu et al., (2010)的研究中資訊安全認知被定義為員工的一般知識(general knowledge)，即此知識為資訊安全相關的認知與了解資訊安全相關議題與潛在的負向的結果。Wang et al.,(2009) 指出網路消費者具有豐富的網路知識與對網路知識的熟悉度，會了解如何避免網路中潛在的安全問題。故本研究參考Bulgurcu et al.,(2010)的研究中員工資訊安全認知的衡量構面以測得使用者對資訊安全認知的了解。在釣魚郵件的認知部分，本研究修改Wang et al., (2009)消費者對網路購物的了解與知識熟悉度的構面，欲以了解使用者是否熟悉釣魚郵件相關議題、釣魚郵件的結構特徵與負向結果等，探討使用者對釣魚郵件的認知。

第六節 信任(Trust)

（一）信任定義

信任是一種無形的存在，且信任一詞在不同領域有不同的定義。信任一詞源起於心理學之研究領域，後來被廣泛的運用於社會學、經濟學、管理學與組織行為等領域。在非網路環境裡，信任是以信任者與被信任者之關係的形式被討論著(Dunn, 2000)。McKnight et al.,(1998) 定義信任為信任者相信並且願意依賴另一方。簡單來說，信任就是人與人之間的連結。信任可說是個人主觀的心理狀態，對於某人或某物的真實性具有信心且依賴之，屬於一種正面的期待(Boon and Holmes, 1991)。

一般信任的定義如下表2-1：

表 2-1 信任的定義

學者	定義
Bhattacharya et al.,(1998)	信任是對正面結果的期望，在不確定性的狀態前提下，該期望可以從預期另一方的行動中獲得。
Lewis and Weigert(1985)	信任是一種狀態，對他人動機持有信心的正面期望，而他人的動機對自己而言，是存在某些程度上的風險。
Mayer et al.,(1995)	認為信任是樂意承受可能受傷的情況並且基於期待被信任的人將會執行對信任者特定重要的行為，而不是監督或是控制被信任對象的能力。
Carnevale and Wechsler (1992)	信任暗示著願意將自身置於風險、易受傷害的狀態，即使個人的所有物被使用，亦願奉獻。
Gefen(2002)	信任是對以前的互動做有利期望的一種信心。
Morgan and Hunt(1994)	信任是人與人之間一連串的互動中，所產生的信任與承諾。

上述學者對信任的定義有不同的看法，但皆有雙方關係中的不確定性與面對風險時正面的期望以及處於易受傷的狀態的共同點。

信任具有概念性層次(McAllister, 1995; Harrison et al., 2002)，可分為信任傾向(disposition to trust)、制度型信任(institution-based trust)、信任信念(trusting beliefs)、信任意圖(trusting intentions) 及信任行為(trust-related behavior)。

1. 信任傾向：在不同情境與所遇對象之中，願意展現依賴他人之傾向。換言之，為對人性的相信。
2. 制度型信任：個人以一種安全的感覺，在面臨具有風險的行為或情境時，感受到處於在情境上的有利條件。
3. 信任信念：個人以一種安全的感覺，相信對方存在有利於自己的特點；即對方願意且能夠為信任者的利益做事。
4. 信任意圖：個人願意去依賴對方，縱使可能存在無法控制以及承受負面的結果的前提下。
5. 信任行為：個人在面對被信任對象時自願依賴對方，縱使可能會遭受負面的結果。

信任區分為情感型信任(affect-based trust)與認知型信任(cognition-based trust)兩種類型(McAllister, 1995)。

1. 情感型信任：為因情感結合而產生對他方的信任，即於對某一個人的情感依附而願意信任對方。情感型信任其特點是需要先經過互動一段時間之後才可能發展，一旦雙方產生情感的連繫，彼此的信任關係就會更加穩固。情感型信任的研究大部分皆探討婚姻、朋友或家庭成員之間的人際關係(Miller and Rempel, 2004; Rempel et al.,1985)，人與人之間的關係會因情感交流會加深雙方的信任感，在持續的相處與合作中充分了解到對方的善意、可靠性與可信任性，就會逐漸對他產生某種依賴，這種依賴成會是互動的。因此，當使用者收到來以朋友名義寄來的電子郵件，因與朋友具有情感上的信賴，因而對此郵件較容易相信郵件的真實性或可靠性。
2. 認知型的信任：基於個人對他方可靠性和可依賴性的信念，即了解到有關某一個人可信任性證據之後，而產生信任對方的意願。以認知基礎的信任是基於在

某些方面和情況下選擇信任對方，而選擇是基於有構成值得信任事證的合理理由。不同於情感型信任，認知型信任的本質上客觀的以理性的觀點判斷個體或組織是可靠的(Hansen et al., 2002)，例如信任者信任被信任的人格特質、生活背景、專業知識及相關能力等條件。在網路環境下信任被視為成功關係的一個關鍵因素(Corritore et al., 2003)。(Corritore et al.,2003)也發現在特定相似的情況下，非網路信任的結論能夠適用於網路的信任。在電子商務與網路交易的環境中，消費者交易時必須承受比實體環境更高程度的風險，而認知型信任能夠降低交易的風險，減輕資訊的不對稱(Ba and Pavlou, 2002)進而提高消費者交易的意願。

本研究欲探討使用者違反資訊安全行為之意圖，以釣魚信件為例，其認知型信任的標的物為網站，即為對網站的信任，情感型信任的標的物為朋友即為對朋友的信任，以兩種不同的信任類型來探討使用者違反資訊安全行為之意圖。

（二）信任構面

信任可分為兩種類型，分別為情感型信任(affect-based trust)與認知型信任(cognition-based trust) (McAllister, 1995)。情感型信任為信任者對被信任者具有情感進而相信對方，情感型信任是透過人際交往、共同人格特徵和價值觀、內群體認同建立起來的信任，簡單來說為人際關係之間的情感。認知型信任是以信任者的個人經驗和以各種方法來了解被信任者的能力和可信度，如信任者信任被信任者的專業能力、知識及聲譽等。

在本研究中，以情感型信任(Chowdhury, 2005; McAllister, 1995)與認知型信任(Johnson and Grayson, 2005; McAllister, 1995)來探討使用者違反資訊安全的因素。情感型信任被定義為對朋友的信任，為人與個人感情因素、社交能力有關，容易與他人分享想法與經驗，而且當對方有問題時願意傾聽對方的需求，且在對方有困難時會主動幫助對方，即信任的標的物為人。當使用者收到以朋友名義寄來的一封電子郵件，因為情感信任的人基於對朋友的信賴而對此郵件具一定程度的信任。因此，許多駭客或詐騙者利用

使用者對與朋友的信任，騙取使用者的個人資料。認知型信任在本研究中被定義為對網站的信任，即標的物為網站。認知型信任的人會願意相信網站的可靠性及專業性，進而對網站產生一定的信任程度。

第七節 風險傾向(Risk Propensity)

(一) 風險傾向定義

風險傾向是個人特質的一部分，為個人承擔風險的意願，即個人追求或規避風險的意願(Sitkin and Weingart, 1995)。下表 2-2 為各學者對於風險傾向之定義：

表 2-2 風險傾向之定義

學者	定義
Litwin and Stringer(1968)	認為風險傾向是個人具有冒險及挑戰性的程度。
Kim(1992)	認為風險傾向是指個人的冒險傾向，當面臨不確定性的情境時，個人所選擇承擔危險或規避危險的意願，即個人傾向追求風險或規避風險的機率。
Robbins(2001)	認為風險傾向是指每個人碰運氣的意願不同，當面臨時個人選擇承擔危險或逃避危險的傾向。
黃洲煌(2000)	風險傾向指的是員工承擔風險的傾向。根據研究顯示，高風險傾向的人決策比較迅速，所用情報較少，而組織中的成員普遍規避風險。
Weber et al.,(2002)	個體差異性在不同領域和情形下會表現出不同的風險傾向。

綜合上述，風險傾向是指個人的冒險傾向，當面臨不確定性的情境時，個人所選擇承擔危險或規避危險的意願，即風險的處置。

宋明哲(2001)認為風險傾向的分類依據影響風險傾向的決策因子，可分為內在與外在因子。內在因子為決策者本身的個人因素，可分為決策的動機、決策者的個性、決策者的態度與決策者所承受的壓力與情緒，外在因子是指決策時存在的外在環境因子，包括文化環境、人口統計環境、社會經濟狀況與參考團體(reference group)。

隨著時間演進，風險傾向的概念可以定義為決策者個人特質。一般而言，風險傾向的概念可分為風險追求行為(risk-taking behavior)和風險規避行為(risk-aversive behavior)，可以用來分析當個人在面臨不確定的情況下,所做出的行為反應。風險傾向程度高的人，會為了追求最大的利益而從事可能產生風險的活動，此類型的人決策較為迅速且願意承擔較大的風險，即為風險追求者;反之，風險傾向程度低的人，則重視風險的最小化，並採取使損失發生機率等於零的措施以免除風險的威脅，此類型的人決策較慢，追求安全與穩定性，即為風險趨避者。MacCrimmon and Wehrung(1985)研究發現風險傾向可視為某一特定環境下的變數，意指在不同環境下個人的風險傾向是不可能一樣的。因此，在一個特定的風險情境下，預測個人的風險決策行為時，了解個人的風險傾向是需要的。故本研究以釣魚郵件為情境，探討個人的風險傾向對個人知覺風險是否具影響力。

(二)風險傾向構面

根據風險傾向不同的定義，各學者提出風險傾向的衡量方法雖然不同，但大多數是類似的，下表 2-3 為本研究整理近代風險傾向的量表：

表 2-3 風險傾向量表

量表名稱	衡量領域	評估方式
風險傾向量表 (Risk Propensity Scale ; RPS) Willman et al.,(2002)	娛樂、健康、職業、經濟、安全和社交風險	每一種範圍都有兩種反應量表，一為「現在」，另一為「過去」，受訪者在「1」(從不)到「5」(經常)中作出評價。每一種風險範圍的平均值在最後會被計算出來，值愈高，代表愈高的風險傾向。此測量工具較能區分現在和過去的風險習慣。
風險傾向問卷 (Risk Propensity Questionnaire；RPQ) Rohrmann (2002)	肉體、經濟、健康與社交	自我評估的分數範圍從「0」(極為低)到「10」(極為高)，顯示他們接受每種風險的個人可能性，並且與其他如朋友、同儕和同事等人在「0」(我非常不願意接受風險)到「10」之間做比較(我很願意接受風險)。最後，每個問卷中總分的平均會被紀錄下來以決定一個最後分數；分數愈高，則顯示這個人願意接受風險的傾向愈高。

特定領域風險態度量表(Domain-Specific Risk Attitude Scale；DOSPERT) Weber et al., (2002)	財務決策(投資與賭博)、健康/安全、娛樂、道德與社交決策	以「1」(一點都沒有風險)到「5」(風險非常大)來評量各風險領域的敘述到底有多冒險；分數愈高就顯示愈高的風險行為和認知。
商業風險傾向量表(Business Risk Propensity Scale；BRPS) Sitkin and Weingart (1995)	決策需仰賴他人的分析、決策面臨技術上複雜度、決策會造成高度衝擊、遺失資訊、失敗的可能	在「0」到「9」的量表上做出選擇，顯示他們在每種情境中會表現出來的傾向，所有的分數被加總，且得到一個總風險傾向數值。

上述的風險傾向量表橫跨不同領域範圍，但本研究以 Sitkin and Weingart (1995)與 Keil et al.,(2000)的對軟體專案風險的評估，即著重於當面臨一個風險已知的方案時，應採取何種風險處置以降低風險，發展本研究的風險傾向概念發展衡量問項。本研究的風險傾向是根據 Kogan and Wallach(1964)發展的選擇難題問卷量表(Choice Dilemma Questionnaire; CDQ)。選擇難題問卷量表是由描述風險(risky)與安全(safe)兩種情況的情境所組成的。受測者被要求在建議高風險的替代方案之前指出他們成功的最小可能性需求。半投射法(semi-projective)的目的是受測者被要求在敘述中的情境給別人建議。這種方法中假設受測者給予他人的意見即反映出個人的傾向。選擇難題問卷量表已普遍與成功的成為個人風險傾向的評量方式(Brockhaus, 1980; Fagley and Miller, 1990; Ghosh and Ray, 1992)。因此，本研究修改 Keil et al.,(2000)資訊安全專案情境中的選擇難題問卷量表，成為本研究測量使用者風險傾向的量表。

第參章　研究方法

第一節為本研究的研究假設，第二節為研究架構說明，第三節說明本研究的問卷如何設計以及各構面的概念型定義，第四節為說明本研究欲發放的問卷對象與使用何種統計分析方法分析資料。

第一節 研究假設

(一) 知覺風險與違反資訊安全之關聯

消費者購買行為與資訊安全行為相似都是涉及風險的行為(Levi and Koç, 2001; Tsai and Yeh, 2010; Youn, 2005)。在消費者購買行為中， Bauer(1960)與 Cox(1967)認為當消費者知覺到所購買的商品可能無法滿足其購買目標，或預料可能會產生不如預期的結果時，消費者便會知覺到某種程度的風險。且 Dowling and Staelin(1994)發現知覺風險會影響資訊搜尋的行為，因為買方與賣方往往存在著資訊不對稱的現象，當消費者知覺的風險愈高，便會花費更多的時間搜尋相關資訊以支援購買決策。許多研究指出風險是可以被知覺到的，知覺風險確實是會對購買行為產生某種程度上的影響(Hoover et al.,1978)且知覺風險會進而影響到消費者的傾向及購買意願(Shimp and Bearden, 1982)。因此，當消費者覺得該購物網站不安全，則知覺其結果可能是負向的，進而影響購買態度(Swaminathan et al., 1999);若消費者對於網路購物的知覺風險愈低，則購買態度會愈正向(Jarvenpaa et al., 1999)。使用者的資訊安全行為亦是如此，當使用者再使用網路資源或面對網路環境的不確定性時，所知覺到的風險程度較高時認為後果是負面的，則使用者的知覺風險也就會隨之提高，進而降低使用者違反資訊安全行為之意圖。故本研究得出研究假設：

H1：使用者的知覺風險與違反資訊安全之意圖呈負向關係。

（二） 知覺利益與違反資訊安全之關聯

利益是指消費者關於產品及服務屬性的個人價值和意義的認知，即消費者認為該產品及服務能夠帶給自己的好處與意義(Park et al., 1986)。知覺利益代表消費者個人心理主觀判斷在消費時所獲得之益處(Lovelock, 1983)，簡單來說就是某樣商品帶給消費者的好處。Zeithaml(1988)認為消費者的知覺價值會進一步產生購買意願，且消費者的購買行為通常取決於知覺其所獲得的價值與利益。根據Youn(2005)的研究顯示，個人知覺其利益程度較高時，讓使用者更願意在網站上提供個人資料。因此，當網路使用者知覺到某樣商品或從事某項網路活動，能夠帶給自己好處時，如登入某個網站即可下載所需軟體，則代表這樣商品或活動帶給使用者的知覺利益程度較高，使用者的使用態度會越趨於正向，進而影響使用意圖。故本研究得出研究假設：

H2：使用者的知覺利益與違反資訊安全之行為意圖呈正向關係。

（三） 資訊安全認知與違反資訊安全之關聯

在過去的研究中指出員工的資訊安全認知在資訊安全管理中是很重要的一部分(Cavusoglu et al., 2009)，且在 Bulgurcu et al.,(2010)提出員工願意遵守資訊安全政策(information security policy)，可增加組織之訊安全的關鍵要素。因此員工對資訊安全認知(information security awareness)的知識程度高低，就顯得很重要。資訊安全認知的概念是指電腦使用者對資訊的安全認知，其目的在於呈現資訊安全上簡單的重點(Spurling, 1995)，認知使個人對資訊的威脅、攻擊與弱點感到敏感，並可識別出所需保護的資料、資訊與處理的過程。因此，當網路使用者具有較高資訊安全認知，使其對資訊的威脅、攻擊與弱點感到敏感，了解違反資訊安全對自身的危害，因而較不輕易做出違反資訊安全的行為。故本研究得出研究假設：

H3：使用者的資訊安全認知與違反資訊安全之行為意圖呈負向關係。

（四） 信任與違反資訊安全之關聯

近年來，在網路環境下信任被視為成功關係的一個關鍵因素(Corritore et al., 2003)。Corritore et al.,(2003)發現在特定相似的情況下，非網路信任的結論能夠適用於網路的信任。網站本身是一種科技的應用，網路上的應用和人有密切的關係，因此網站信任為人與此科技的互動的重要因素。認知型信任的任會以個人經驗對於資訊內容的第一印象及認知所感受到被信任者的可信程度(Johnson and Grayson, 2005)。在本研究中，將認知型信任的標的物從信任他人的專業知識與能力，轉為信任網站的專業程度、商譽等。Johnson and Grayson(2005)與李碩育(2010)研究指出使用者在瀏覽網站或與網站互動時，依據該網站的評價，並產生依賴該網站的意願。情感型信任是基於情感上的信賴，換言之，情感型信任的人在瀏覽網站或與網站互動時，當看到網站是朋友推薦的或者電子郵件是朋友寄來的，因為與朋友具有情感上的聯繫而對該網站或信件所產生的感受，讓使用者依賴該網站或信件的意願。

故本研究得出研究假設：

H4：使用者對資訊安全行為相關的人、網站的信任程度與違反資訊安全之行為意圖呈正向關係。

（五） 風險傾向與知覺風險之關聯

風險傾向和知覺風險都顯著的影響決策行為，也有證據顯示風險傾向與知覺風險具有交互作用，風險傾向可能也會直接的影響知覺風險(Keil et al., 2000; Sitkin and Weingart, 1995)。例如，個人具有較高的風險承擔傾向，則此人可能傾向於低估所涉及的風險的情況。喜好風險的決策者更願認知別和權衡正向的結果，因而高估了獲利的機率。這種高估獲利的結果會使的個人的知覺風險降低;反之，趨避風險的決策者會權衡負向結果高於正向結果，因而提高個人的知覺風險(Keil et al., 2000)。

故本研究得出研究假設：

H5：風險趨避者知覺某一項違反資訊安全行為的風險程度會比風險愛好者高。

第二節 研究架構

圖 3-1 為本研究的整體架構，欲探討知覺風險、知覺利益、信任及認知對使用者違反資訊安全行為之意圖的影響，並預測風險傾向對於知覺風險具影響力。

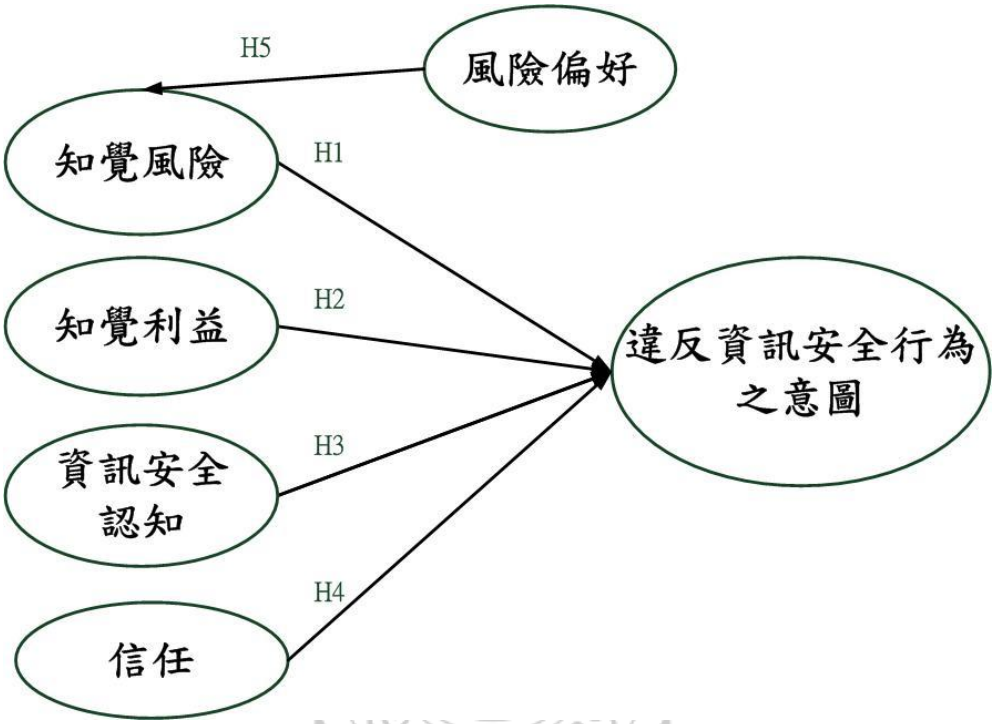

圖 3-1 研究架構

研究假設

H1：使用者的知覺風險與違反資訊安全之意圖呈負向關係。

H2：使用者的知覺利益與違反資訊安全之行為意圖呈正向關係。

H3：使用者的資訊安全認知與違反資訊安全之行為意圖呈負向關係。

H4：使用者對資訊安全行為相關的人、網站的信任程度與違反資訊安全之行為意圖呈正向關係。

H5：風險趨避者知覺某一項違反資訊安全行為的風險程度會比風險愛好者高。

第三節 問卷設計與操作性定義

本研究使用的衡量工具，為過去許多學者引用與驗證過之量表，問卷由六個構面所組成，包含知覺風險、知覺利益、信任、資訊安全認知、風險傾向、違反資訊安全行為之意圖以及個人資料等，下列為各部分操作型定義與衡量方式：

一、操作型定義

1. 違反資訊安全行為之意圖

根據 Davis(1989)所提出的科技接受模型中認為信念(beliefs)會影響態度(attitude)，態度再進一步影響行為意圖(intention)，行為意圖對實際使用(actual system use)有顯著且正面的影響，使用者違反資訊安全行為之意圖亦是如此，即當使用者收到一封郵件，假設使用者相信信件內的資訊對自己是有利的且相信信件內容的真實性，綜合這些信念轉變為使用者的態度，當使用者態度趨於正向，則會進一步影響違反資訊安全行為之意圖。本研究將此變數作為在知覺風險、知覺利益、信任與資訊安全認知這些因素的影響下，使用者點選郵件內的連結的意願有多大。

表 3-1 違反資訊安全行為之意圖操作化定義

構面	操作型定義	問項
違反資訊安全行為之意圖	使用者點選郵件內的連結的意願	我打算開啟此電子郵件中的連結。
		我將會開啟此電子郵件中的連結。

2. 知覺風險

知覺風險是使用者面對不確定性的情況下，主觀認知到的風險。本研究以知覺風險的定義作為衡量知覺風險的構面。在釣魚郵件情境中，此變數為網路使用者知覺此郵件為可能為釣魚郵件的機率的大小，與點下郵件中的連結後自身損失的嚴重性的大小(Dowling and Staelin, 1994; Peter, 1979)。

表 3-2 知覺風險操作化定義

構面	操作型定義	問項
知覺風險	使用者認為此信件為釣魚郵件的機率	我覺得此電子郵件為釣魚信件的機率是大的。
	使用者認為點下郵件中的連結後自身損失的嚴重性	我覺得點下此郵件中的連結後所造成個人資料外洩的損失是大的。

3. 知覺利益

知覺利益是使用者主觀認知到自己可以獲得的好處。因為商品的知覺利益與知覺價值相似，故本研究以知覺價值的構面做為知覺利益的衡量。本研究將此變數為個人知覺到某項商品所提供的特性可以帶給自己的好處與意義，包含產品品質、貨幣價值、行為價格、情感性反應與聲譽。在本研究的情境中以客製化的 XXX 品牌的郵差包做為使用者的知覺利益。

表 3-3 知覺利益操作化定義

構面	操作型定義	問項
知覺利益	使用者知覺到信件內產品所帶給自身的好處，包含產品品質、貨幣價值、行為價格、情感性反應與聲譽	整體而言，我覺得這個商品的品質是可信賴的。
		我覺得這個商品的實用性高。
		我覺得這個商品讓人覺得是值得的。
		我覺得這個商品可依照我的傾向來設計。
		我覺得這個商品品牌有好的聲譽。

4. 資訊安全認知

資訊安全認知的概念是指電腦使用者對資訊的安全認知，其目的在於呈現資訊安全上簡單的重點(Spurling, 1995)，認知使個人對資訊的威脅、攻擊與弱點感到敏感。本研究以使用者對資訊安全的認知程度與對釣魚郵件相關資訊的熟悉度作為此構面的操作變數。

表 3-4 資訊安全認知操作化定義

構面	操作型定義	問項
資訊安全認知	了解使用者對資訊安全的認知程度	整體來說，我了解違反資訊安全行為的相關威脅與可能的負面結果。
		對於潛在的資訊安全問題，我具有足夠的知識。
		我了解與資訊安全相關的議題及違反資訊安全的相關可能的風險。
	了解使用者對釣魚郵件的認知程度	我熟悉釣魚郵件的相關資訊。
		對於釣魚郵件的相關風險我具有足夠的知識。
		我了解釣魚郵件的結構特徵。
		我了解與釣魚郵件的相關議題。

5. 信任

本研究在信任的部分，因信任的標的物的不同將信任分為對朋友的信任與對網站的信任。在網站信任部分，本研究以 XXX 的網址可靠性與真實性以及網頁的聲譽與專業水準作為為使用者對網站的信任的操作變數。在朋友信任部分，操作變數為假設這封信是以朋友的名義寄來時，使用者因與朋友具情感上的連結而對此信件具有一定的信任程度。

表 3-5 信任操作化定義

構面	操作型定義	問項
朋友信任	使用者對寄電子信件來的朋友的情感上的聯繫	我能夠與這位朋友自由地分享想法、感受和期許。
		當我與這位朋友表達問題時，我相信對方願意傾聽。
		如果告訴這位朋友我的問題，我相信對方會給我有建設性的回應。
		我與這位朋友已建立深厚的關係。
		當我與這位朋友斷了聯繫時,我會感到失落。
網站信任	使用者評估信件內網址的可靠性與真實性	我相信這個網址。
		XXX 網站具備專業水準。
		我可以放心地點選這個網址。
		我相信點下這網址之後的結果不會造成困擾。

6. 風險傾向

喜好風險的決策者更願認知別和權衡正向的結果，因而高估了獲利的機率。這種高估獲利的結果會使的個人的知覺風險降低;反之,趨避風險的決策者會權衡負向結果高於正向結果，因而提高個人的知覺風險。故本研究以 Keil et al.,(2000)與 Sitkin and Weingart(1995)研究中對風險傾向的衡量個人的以了解使用者是風險喜好者還是風險趨避者，與使用 Kogan and Wallach(1964)所發展的 CDQ 量表，以情境題的方式評估當使用者面臨一個風險已知的方案時，會採取何種風險處置以降低風險。

表 3-6 風險傾向操作化定義

構面	操作型定義	問項
風險傾向	風險喜好者、風險趨避者與面臨一個風險已知的方案時，應採取何種風險處置以降低風險	我認為開啟此信件連結的風險(危險程度)高。
		我認為開啟此信件連結的風險(危險程度)低。
		情境題採用 CDQ 量表的問卷方式 在下列哪一種最高機率情況下，您會建議 A 先生不要點這封信件內的連結? □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 10%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 30%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 50%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 70%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 90%。 □ 無論機率為何,都不會建議 A 先生點這封信件內的連結。

二、衡量方式

使用者對違反資訊安全行為之意圖共有2題問項、使用者的知覺利益共有5題問項，使用者的信任部分分為對朋友的信任與對網站的信任，對朋友信任共 5 題問項，對網站信任共 4 題問項。使用者的知覺風險共有 2 題問項，分別問的是使用者知覺的負向結果

的機率與損失的嚴重性。使用者的資訊安全認知共 7 題分為對資訊安全的認知與釣魚郵件的認知。個人的風險傾向共 3 題，以了解使用者的風險傾向。

表 3- 7 違反資訊安全行為題項來源彙整表

構面	題數	參考量表	衡量
違反資訊安全行為之意圖	1~2	Lee (2009) Warshaw and Davis(1985)	李克特 7 點量表 1：非常不同意 7：非常同意
知覺利益	3~7	Petrick and Backman (2002) Zeithaml(1988)	
信任	8~12	Chowdhury(2005) McAllister(1995)	
	13~16	Chowdhury(2005) Johnson and Grayson(2005) McAllister(1995)	
知覺風險	17~18	(Dowling amd Staelin(1994) Peter(1979)	
資訊安全認知	19~21	Bulgurcu et al.,(2010)	
	22~25	Wang et al.,(2009)	
風險傾向	26~27	Keil et al.,(2000) Sitkin and Weingart(1995)	情境題 李克特 7 點量表 1：非常不同意 7：非常同意
	28		情境題採用 CDQ 量表的問卷方式，由機率高低來決定受測者的風險傾向

圖 3-17 為違反資訊安全行為題項來源彙整表，以李克特 7 點尺度量表，由「非常不同意」、「不同意」、「有點不同意」、「沒意見」、「有點同意」、「同意」、「非常同意」，依序給與 1~7 分，在違反資訊安全行為之意圖的構面中，分數越高代表受測者點選此郵件內的連結之意圖越高。在知覺利益的構面中，分數越高代表受測者知覺此商品能夠帶給他/她的利益越高。信任構面部分，對朋友信任構面當分數越高，則代表受測者越能夠與此朋友做情感上的連結;對網站信任構面當分數越高代表受測者相信網站程度越高。

知覺風險的構面中，在損失的嚴重性部分，分數越高則代表受測者認為點選此信件內的連結導致的損失的嚴重性是大的，在負向結果的機率部分，當分數越高則代表受測者認為此郵件為釣魚郵件的機率是大的。資訊安全認知構面，當分數越高則代表受測者對資訊安全的知識/認知程度越高。風險傾向構面中，認為開啟此信件連結的風險(危險程度)高，此問項分數越高代表受測者的風險傾向偏向風險趨避者;反之為風險喜好者，與面臨一個風險已知的方案時，應採取何種風險處置以降低風險。

三、個人基本資料

本問卷的個人基本資料是參考過去與資訊安全相關的文獻而來，包含受測者的性別、年齡、職業、教育程度與去年是否曾經收過釣魚郵件等五項，說明如下：

性別：分為男、女。

年齡：分別為 16-20 歲、21-25 歲、26-30 歲、31-35 歲、36-40 歲、41-45 歲、46-50 歲、51 歲以上。

職業：分為軍警、公教、服務業、金融保險、電子資訊、醫護、學生、製造業、研究員、其他。

教育程度：分別為國中(含)以下、高中(職)、專科、大學、碩士、博士。

去年是否曾經收過釣魚郵件：分為是、否。

第四節 研究對象與資料分析方法

一、研究對象

本研究的資料收集以問卷調查的方式，研究對象以東海大學學生與社會人士為主要對象。問卷發放方式以便利抽樣方式，透過紙本問卷與線上問卷兩種型式。問卷發放日期由 2013 年 5 月 5 日開始，至 2013 年 5 月 26 日為止，為期三周。

本研究共回收 288 份問卷，扣除無效問卷 6 份，有效問卷 282 份。

二、資料分析方法

本研究使用 SPSS 17.0 for Windows 為分析工具，透過敘述統計分析、信度分析、相關分析、階層迴歸分析等統計方法，進行研究假設的驗證並呈現研究結果：

(一)敘述統計分析

經由敘述統計分析基本的人口統計分布，了解受測者的基本資料以次數分配與百分比來說明分布狀況;了解各構面的行量狀況，以平均數與標準差衡量之。

(二)信度與效度分析

信度分析為測量的可靠性(trustworthiness)，係指測量結果的一致性(consistency)或穩定性(stability)，一份良好的問卷或是量表應具有足夠的信度。Cronbach's α 是目前社會科學研究股常使用的信度量測方式，因此本研究以 Cronbach's α 作為衡量問卷的內部一致性。Cronbach's α 係數大小所代表的可信程度，當 α 小於 0.5 時，表示信度不可信，當 α 介於 0.5 至 0.6 之間時，表示信度不足，當 α 介於 0.6 至 0.7 之間時，表示信度不可靠的，當 α 介於 0.7 至 0.8 之間，表示信度可接受，當 α 介於 0.8 至 0.9 之間時，表示信度良好，當 α 大於 0.9，則表示信度十分可信(George and Mallery, 2003)。因此，當 α 值大於 0.7 則代表此量表具有高信度具有意義；當 α 值小於 0.3 則代表此量表具有不具信度為無意義(Robinson and Shaver, 1973)。

所謂效度(Validity)是表示，一份測驗能真正的測量到他所要測量能力或功能的程度，即測量的正確性。指測驗或其他測量工具確實能夠測得其所欲測量的構面之程度，亦即能反映測量分數的意義為何。測量的效度越高，表示測量的結果越能顯現其所欲測量內容的真正特徵(邱皓政, 2006)。效度評估形式為內容效度與區別效度。內容效度(content validity)反映測量工具本身內容範圍與廣度的適切度。內容效度的評估是從測量工具的內容來檢查，看看是否符合測量目標所預期的內容。區別效度(discriminate validity)為量表內所有兩兩配對因素間的相關性要低，即各個因素間是有所區別的。

(三)相關分析

本研究使用 Person 相關係數檢定兩變項之間的相關性，相關係數介於+1 與-1 之間，相關係數數值越接近±1 時，表示兩變項之間的關係越顯著，相關係數的絕對值若在 0.1 以下為微弱或無相關;0.1~0.39 為低度相關;0.4~0.69 為中度相關;0.7~0.99 之間為高度相關;1 為完全相關(邱皓政, 2006)。

(四)階層式迴歸分析

本研究透過階層式迴歸分析分法，將自變數、控制變數與違反資訊安全行為之意圖

逐步納入回歸方程式之中，透過多層次迴歸來進行迴歸預測，檢定自變數、控制變數與違反資訊安全行為之意圖的影響。

共線性問題可以說是影響迴歸分析重要的因素之一。自變數具高度相關時，可能造成係數估計之偏誤。一般在判斷共線性問題會用 VIF，當 VIF 等於 1 時，表示完全無共線性，當 VIF 大於 1 時表示具有共線性。當 VIF 約為 1.5 時，雖然變數間有共線性，但是影響不大。當 VIF 在 5~10 之間時，變數間具共線性但是在可容忍範圍。當 VIF 大於 10 以上，表示變數間具有嚴重的共線性，已嚴重威脅參數估計的穩定性(邱皓政, 2006)。

（五）中介效果

在 X→Y 的關係中，第三變項 Z 除了可能以中介者的身分介入迴歸方程式中。換言之 X 對 Y 的影響是透過 Z 的作用。中介路徑階段模型，主要是透過迴歸分析來驗證變項間是否其有中介效果或稱間接效果。

三、問卷前測

問卷情境的設計部分是與指導教授討論哪種情境內容受測者比較願意點選信件內連結，再將討論出來後的情境給親友們做前測，並詢問親友們在哪一種情境下比較願意點選信件內連結，最後決定以生日送禮的情境作為本研究問卷的情境，情境中禮物的選擇是以可客製化的品牌的郵差包作為本問卷的生日送禮的禮物。在問卷問項的部分，為翻譯國外學者的問卷題項，因此在問卷正式發放以前，與指導教授討論過問項的用字遣詞、問法加以修飾，並請其他老師與同學檢視問卷問項的內容，根據指導教授與其他人的意見，將問卷內容用字遣詞及語意不清的部分進行修改，減少填答者的誤解或不理解問題的機率，降低可能導致的偏誤，修正後的問卷以紙本與線上問卷的方式發放。

第肆章　研究結果

本章的第一節為樣本的基本資料分析與敘述統計，了解受測者的分布情形與填答狀況。第二節為樣本的信度與效度分析，了解問卷題項是否具有一致性與能否了解該研究構面。第三節使用階層式迴歸分析，分析知覺風險、知覺利益、信任與資訊安全認知是否對違反資訊安全行為之意圖是否有影響，並檢測個人的風險傾向、知覺風險與違反資訊安全行為之意圖是否為中介關係。

第一節 基本資料分析與敘述統計

一、受測者基本資料分析

表 4-1 受測者基本資料(N=282)

項目	人數	百分比%	項目	人數	百分比%
年齡			**職業**		
21 – 25 歲	144	51.1%	公教	14	5.0%
26 – 30 歲	56	19.9%	服務業	13	4.6%
31 – 35 歲	19	6.7%	金融/保險業	61	21.6%
36 – 40 歲	15	5.3%	電子/資訊業	16	5.7%
46 – 50 歲	13	4.6%	學生	151	53.5%
51 歲以上	9	3.2%	製造業	11	3.9%
教育程度			其他	16	5.7%
高中	14	5.0%	**性別**		
大學	132	46.8%	男性	123	43.6%
碩士	123	43.6%	女性	159	56.4%
博士	13	4.6%			
去年是否收過釣魚郵件?					
是	188	66.7%			
否	94	33.3%			

將回收 282 份有效樣本，依據填答者的作答，將受測者基本資料分類，調查受測者的年齡、教育程度、職業、性別與去年是否收過釣魚郵件等五項，如表 4-1 所示。填答者的年齡以 21-25 歲最多共 144 筆，佔全部樣本的 51.1%;填答者的教育程度以大學與碩士最多，共佔全部樣本的 90.4%;填答者的職業以學生為最多共 151 筆資料，佔全部樣本數的 53.5%，其是為金融保險業共 61 筆資料，佔全部樣本數的 21.6%；填答者的性別，

男性與女性的樣本數均為各半；受測者的填答資料中，去年收過釣魚郵件的人高達 188 人，佔全部樣本的 66.7%。

二、敘述統計分析

根據回收的有效樣本，將不同研究構面做分類後，利用 SPSS 17.0 for Windows 分析工具得到以下結果。從表 4-2 到表 4-8 為各構面問項之敘述統計。

表 4-2 為受測者所填答的知覺風險構面的平均數與標準差，問卷題項共 2 題，在李克特 7 點量表中，平均數為 4.72 與 5.04，均高於平均值 4。顯示受測者認為此信件為釣魚郵件的機率偏高，且點下郵件中的連結後造成損失是大的。

表 4-2 知覺風險構面之敘述統計

問項	平均數	標準差
我覺得此電子郵件為釣魚信件的機率是大的。	4.72	1.512
我覺得點下此郵件中的連結後所造成個人資料外洩的損失是大的。	5.04	1.452

表 4-3 為受測者所填答的知覺利益構面的平均數與標準差，問卷題項共 5 題，在李克特 7 點量表中，平均數為 4.33 到 5.10 平均數均高於平均值 4，顯示受測者認為此商品所具的功能可以為自己帶來好處與意義。

表 4-3 知覺利益構面之敘述統計

問項	平均數	標準差
整體而言，我覺得這個商品的品質是可信賴的。	4.33	1.627
我覺得這個商品的實用性高。	4.78	1.515
我覺得這個商品讓人覺得是值得的。	4.63	1.546
我覺得這個商品可依照我的傾向來設計。	5.10	1.634
我覺得這個商品品牌有好的聲譽。	4.56	1.373

表 4-4 為受測者所填答資訊安全認知構面的平均數與標準差，問項分為對資訊安全的了解與對釣魚郵件的了解，在李克特 7 點量表中，問卷題項共 7 題，其平均數為 4.33 到 5.23，表示受測者認為自己對資訊安全方面具備一定的知識。

表 4-4 資訊安全認知構面之敘述統計

問項	平均數	標準差
整體來說，我了解違反資訊安全行為的相關威脅與可能的負面結果。	5.23	1.312
對於潛在的資訊安全問題，我具有足夠的知識。	4.77	1.363
我了解與資訊安全相關的議題及違反資訊安全的相關可能的風險。	4.93	1.329
我熟悉釣魚郵件的相關資訊。	4.47	1.505
對於釣魚郵件的相關風險，我具有足夠的知識。	4.42	1.484
我了解釣魚郵件的結構特徵。	4.33	1.535
我了解與釣魚郵件的相關議題。	4.47	1.505

表 4-5 為受測者所填答的朋友信任構面的平均數與標準差，問卷題項共 5 題，在李克特 7 點量表中，平均數為 4.93 到 5.35，平均數均高於平均值 4。顯示受測者對寄信來的這位朋友具有情感上的連繫。

表 4-5 朋友信任構面之敘述統計

問項	平均數	標準差
我能夠與這位朋友自由地分享想法、感受和期許。	4.93	1.575
當我與這位朋友表達問題時，我相信對方願意傾聽。	5.25	1.384
如果告訴這位朋友我的問題，我相信對方會給我有建設性的回應。	5.14	1.431
我與這位朋友已建立深厚的關係。	5.29	1.444
當我與這位朋友斷了聯繫時，我會感到失落。	5.35	1.473

表 4-6 為受測者所填答的網站信任構面，問卷題項共 4 題，在李克特 7 點量表中，其平均數為 3.75 到 4.24，顯示受測者對信件內連結信任偏低。

表 4-6 網站信任構面之敘述統計

問項	平均數	標準差
我相信這個網址。	4.00	1.706
Timbuk2 網站具備專業水準。	4.24	1.469
我可以放心地點選這個網址。	3.88	1.659
我相信點下這網址之後的結果不會造成困擾。	3.75	1.673

表 4-7 為受測者所填答風險傾向構面的敘述統計，此構面問卷題項共 3 題，以李克特 7 點量表衡量共有 2 題，此構面第一題為反向題。風險傾向的第一題與第二題，其平均數為 2.10 與 2.45，此兩題填答方向為一致，構面的第三題，以另一種情境測驗，其平均數為 2.43。由結果可知，大部分受測者為風險趨避者。

表 4-7 風險傾向構面之敘述統計

問項	平均數	標準差
我認為開啟此信件連結的風險(危險程度)高。	2.10	1.157
我認為開啟此信件連結的風險(危險程度)低。	2.45	1.468
在下列哪一種最高機率情況下，您會建議 A 先生不要點這封信件內的連結? □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 10%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 30%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 50%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 70%。 □ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 90%。 □ 無論機率為何，都不會建議 A 先生點這封信件內的連結。	2.43	1.940

表4-8為受測者違反資訊安全之意圖所填答的平均數與標準差，問卷題項共2題，在李克特7點量表中，其平均數為4.16到4.26，其平均值高於平均值4，顯示大部分受測者較有意願開啟郵件內連結。

表 4-8 違反資訊安全行為意圖構面之敘述統計

問項	平均數	標準差
我打算開啟此電子郵件中的連結。	4.26	1.924
我將會開啟此電子郵件中的連結。	4.16	1.952

各研究構面之描述統計分析，如下表4-9

表 4-9 各構面之描述統計分析

衡量構面	題數	平均數	標準差
知覺風險	2	4.881	1.403
知覺利益	5	4.678	1.332
網站信任	4	3.969	1.515
朋友信任	5	5.190	1.331
資訊安全認知	7	4.660	1.273
違反資訊安全行為之意圖	2	4.211	1.912

第二節 信度與效度分析

一、信度與效度分析

所謂信度(reliability)即測量的可靠性(trustworthiness)，係指測量結果的一致性(consistency)，或穩定性(stability)。因此一份良好的問卷或是量表應具有足夠的信度。本研究使用Cronbach's α來分析問卷構面的內部一致性，若α值大於0.7以上，屬於內部一致性良好;另外使用總項相關係數(item-to-total correlations)來衡量分項對總項的相關係數，而分項對總項的相關係數須大於0.5(吳萬益、林清河, 2000)。

反映性指標(reflective indicator)只為構面外在的表現形式，通常反映一共同的理論構面，指標間是高度一致的。形成性指標(formative indicator)為構面的不同層面，構面立基於測量指標的整合基礎上，由指標共同決定了構面的意義(MacKenzie et al.,2005)。本研究知覺風險與風險傾向兩個構面為形成性構面的題項，由於內不一致性與傳統的效度並不適用於形成性(formative)的構面(Chin, 1998)，故知覺風險與風險傾向不用考慮信度與效度。

表4- 10顯示各構面的因素負荷量(factor loading)，知覺利益題項中的PB1不具區別效度故刪除。將剩下的各構面問題題項再跑一次因素分析，結果如表4-11所示。

本研究對知覺利益、網站信任、朋友信任與資訊安全認知等構面做驗證性因素分析，採用主成分分析法以及最大變異數法以萃取出主要影響構面的因素。

本研究的研究構面的信度與效度分析主要包含對違反資訊安全之意圖、知覺利益、

網站信任、朋友信任、資訊安全認知與違反資訊安全等五項構面。信度分析結果如表4-11所示，本研究各構面的Cronbach's α係數均大於0.9，整體而言，故本問卷的信度具有高信度。而在分項對總項的相關係數中，由表4-11可看出各題項的分項對總項的相關係數皆大於0.5以上，因此可判斷本研究的問卷具有良好的信度。

效度分析部分，知覺利益構面PB1刪除後各個構面的問題題項的因素負荷量皆大於0.5以上，故本問卷具良好的效度。

表 4- 10 轉軸後的成份矩陣

構面/題項	資訊安全認知	朋友信任	網站信任	知覺利益
PB1	-0.087	0.230	0.630	0.566
PB2	-0.048	0.323	0.330	0.775
PB3	-0.007	0.275	0.363	0.811
PB4	-0.060	0.383	0.160	0.714
PB5	-0.015	0.330	0.478	0.659
TRA1	-0.015	0.711	0.303	0.413
TRA2	0.040	0.857	0.206	0.280
TRA3	0.041	0.888	0.216	0.189
TRA4	0.032	0.891	0.200	0.243
TRA5	0.015	0.869	0.144	0.186
TRC1	-0.115	0.219	0.885	0.216
TRC2	-0.108	0.217	0.756	0.431
TRC3	-0.132	0.222	0.887	0.222
TRC4	-0.115	0.202	0.883	0.191
AWI1	0.711	0.226	-0.178	-0.134
AWI2	0.909	0.019	-0.019	0.023
AWI3	0.883	0.081	-0.036	-0.018
AWP1	0.928	-0.050	-0.090	0.015
AWP2	0.931	-0.049	-0.039	-0.030
AWP3	0.899	-0.053	-0.088	-0.048
AWP4	0.911	-0.048	-0.071	-0.012

表 4-11 各構面信、效度分析

構面	子構面	題項	因素負荷量	Item-to-total correlations	Cronbach's α
知覺利益		PB2	0.762	0.826	0.915
		PB3	0.793	0.858	
		PB4	0.704	0.694	
		PB5	0.641	0.761	
信任	朋友信任	TRA1	0.730	0.794	0.948
		TRA2	0.867	0.890	
		TRA3	0.899	0.889	
		TRA4	0.895	0.906	
		TRA5	0.867	0.822	
	網站信任	TRC1	0.884	0.900	0.948
		TRC2	0.757	0.813	
		TRC3	0.884	0.921	
		TRC4	0.877	0.874	
資訊安全認知	資訊安全認知	AW1	0.715	0.660	0.955
		AW2	0.910	0.868	
		AW3	0.884	0.840	
	釣魚郵件認知	AWP1	0.924	0.899	
		AWP2	0.928	0.899	
		AWP3	0.897	0.864	
		AWP4	0.909	0.879	
意圖		INT1	0.653	0.949	0.974
		INT2	0.680	0.949	

第三節 相關分析與階層式迴歸分析

本節探討違反資訊安全之意圖，是否會受知覺風險、知覺利益、對朋友的信任、對網站的信任、與資訊安全認知影響。在進行迴歸分析前，先探討個構面之間的相關程度。證實變項之間的具有相關性之後，再利用階層式迴歸分析探討各變數與違反資訊安全之意圖之關聯性。

一、相關分析

本研究利用Person相關係數檢定兩變項之間的關聯性，如表4-12所示。知覺風險、知覺利益、對朋友的信任、對網站的信任、資訊安全認知、風險傾向與違反資訊安全行為之意圖共七個變項，其中違反資訊安全之意圖為依變項，知覺風險、知覺利益、對朋友的信任、對網站的信任、資訊安全認知與風險傾向為自變項。在探討知覺風險與風險傾向兩變項之關聯時，自變項為風險傾向，依變項為知覺風險。

違反資訊安全行為之意圖與知覺風險、資訊安全認知之間的相關係數為-0.395、-0.228，在顯著水準為0.01時，由Person相關係數可看出知覺風險違反資訊安全之意圖為顯著負向關。

表 4-12 相關矩陣分析

變數	1	2	3	4	5	6	7
1.知覺風險	1						
2.知覺利益	-0.312**	1					
3.朋友信任	-0.207**	0.668**	1				
4.網站信任	-0.588**	0.674**	0.504**	1			
5.資訊安全認知	0.334**	-0.089	0.007	-0.207**	1		
6.違反資安意圖	-0.395**	0.603**	0.470**	0.748**	-0.228**	1	
7.風險傾向	-0.285**	0.114	-0.057	0.318**	-0.293**	0.252**	1

**在顯著水準為0.01時 (雙尾)，相關顯著。

違反資訊安全之行為意圖與知覺利益、對朋友的信任、對網站的信任之間的相關係數為0.603、0.474、0.748，在顯著水準為0.01時，由Person相關係數可看出，知覺利益、對朋友的信任、對網站的信任與違反資訊安全之意圖為顯著正向關。且對網站的信任與

違反資訊安全之意圖的相關係數為0.748，顯示對網站的信任與違反資訊安全行為之意圖呈高度正相關。

知覺風險與風險傾向之間的相關係數為-0.285在顯著水準為0.01時，由Person相關係數可看出，知覺風險與風險傾向之間為顯著負相關。

二、階層式迴歸分析

(一)整體模式

本研究利用階層式迴歸分析法，了解知覺風險、知覺利益、朋友信任、網站信任與資訊安全認知對違反資訊安全行為意圖之影響。在此模式中，將知覺風險、知覺利益、資訊安全認知、朋友信任、網站信任與違反資訊安全行為之意圖合併計算出一個平均數，其中，知覺風險、知覺利益、資訊安全認知、朋友信任與網站信任為自變項，違反資訊安全行為之意圖為依變項，個人基本資料為控制變項。依據自變數與違反資訊安全行為之意圖的相關性的高低依序選入。在模式1中為選入知覺風險與個人基本資料兩項變數，模式2再選入知覺利益與個人基本資料，模式3再選入資訊安全認知與個人基本資料，模式4再選入朋友信任與個人資料，最後模式5再選入網站信任。模式1到模式5之間為階層式迴歸關係，分析如下表4-13所示。

模式1的F值15.222(P<0.001)，整體模型是顯著的。知覺風險、性別與職業均達顯著，整體解釋力21.6%。職業的標準化係數為正值，表示此變數與違反資訊安全行為之意圖呈正相關。知覺風險與性別的標準化係數為負值，表示此兩變數與違反資訊安全行為之意圖呈負相關，在此模型中以知覺風險對違反資訊安全行為之意圖具影響力。由此可知，個人的知覺風險較高時，此人在從事某一項資安行為時，知覺發生損失的可能性與損失的嚴重性就會比較大，則較不容易做出違反資訊安全的行為。也由模式1可以看出，本研究的假設一是成立。

模式2加入知覺利益後，模式2的F值35.471 (P<0.001)整體模型是顯著的。知覺風險、知覺利益與職業均達顯著，整體解釋力43.6%，知覺風險的標準化係數為負值，表示知覺風險與違反資訊安全行為之意圖呈負相關，知覺利益與職業的標準化係數為正值，表

示此兩變數與違反資訊安全行為之意圖呈正相關。其中，以知覺利益對違反資訊安全行為之意圖較具影響力。加入知覺利益後此變數對模型2的解釋力增加2.2%。由此可知，當個人知覺到其商品可以帶給自己好處與利益時，則使用者較容易做出違反資訊安全的行為。也由模式2可以看出，本研究的假設二是成立。

模式3加入資訊安全認知後，模式3的F值31.115(P<0.001)整體模型是顯著，整體解釋力44.3%。知覺風險與知覺利益均達顯著，資訊安全認知與職業均達邊際顯著。其中，以知覺利益對違反資訊安全行為之意圖較具影響力。加入資訊安全認知後此變數對模型3的解釋力增加0.7%。知覺利益與職業標準化係數為正值，表示此兩變數與違反資訊安全行為之意圖呈正相關。知覺風險與資訊安全認知標準化係數為負值，表示此兩變數與違反資訊安全行為之意圖呈負向關係。在此模型中雖然資訊安全認知達邊際顯著，顯示個人的資訊安全認知對違反資訊安全行為之意圖具影響力且呈負向關，當個人的資訊安全認知越高時，此人對資訊的威脅、攻擊與弱點感到敏感，則較不容易做出違反資訊安全之行為。由模式3可以看出，本研究的假設三是成立。

模式4加入朋友信任後，模式4的F值28.244(P<0.001)整體模型是顯著的。整體解釋力45.3%，知覺風險、知覺利益與資訊安全認知與朋友信任均達顯著，而職業為邊際顯著，加入朋友信任後此變數對模型4的解釋力增加1.0%。其中，以知覺利益對違反資訊安全行為之意圖較具影響力，知覺利益VIF大於2，表示在此模型中知覺利益與違反資訊安全行為之意圖具有共線性。知覺風險與資訊安全認知的標準化係數為負值，表示此兩變數與違反資訊安全行為之意圖呈現負相關。知覺利益、朋友信任與職業標準化係數為正值，表示此三個變數對違反資訊安全行為之意圖呈正向關係。朋友信任對違反資訊安全行為之意圖是具影響力的且呈正相關係，表示使用者與朋友有情感上的聯繫，則使用者收到以朋友名義寄來的信件時，則對此信件的信任程度就會較高，進而容易做出違反資訊安全的行為。由模式4可以看出，本研究的假設四是成立。

模式5加入網站信任後，模式5的F值46.039(P<0.001)整體模型是顯著的。整體解釋力60.4%，資訊安全認知、網站信任與職業為均達顯著，知覺利益為邊際顯著。知覺利益、網站信任與職業的標準化係數為正數，表示此三個變數與違反資訊安全行為之意圖

呈正向關係。資訊安全認知標準化係數為負值，表示資訊安全認知與違反資訊安全行為之意圖呈負向關係。其中，以網站信任對違反資訊安全行為之意圖最具影響力。加入網站信任後此變數對模型5的解釋力為15.1%，知覺利益與網站信任的VIF值皆大於2，表示在此模型中知覺利益、網站信任與違反資訊安全行為之意圖具共線性。在模式5中，整體模式是顯著的，因網站信任的影響力太大$\hat{\beta}$值高達0.633且與違反資訊安全行為之意圖呈高度相關，使前面的變項變的不顯著。網站信任對違反資訊安全行為之意圖是最具影響力的且呈正相關係，顯示當使用者對網站的信任程度越高時，則此人越容易做出違反資訊安全行為之意圖。

表 4-13 階層式迴歸分析

	模式1	模式2	模式3	模式4		模式5	
	b值	b 值	b 值	b 值	(VIF)	b 值	(VIF)
自變項							
知覺風險	-0.346***	-0.207***	-0.181***	-0.177***	(< 2.0)	0.080	(< 2.0)
知覺利益		0.507***	0.512***	0.420***	(2.016)	0.116†	(2.628)
資訊安全認知			-0.088†	-0.097*	(< 2.0)	-0.084*	(< 2.0)
朋友信任				0.136*	(< 2.0)	0.074	(< 2.0)
網站信任						0.633***	(2.653)
控制變項							
性別	-0.117*	-0.056	-0.054	-0.047	(< 2.0)	-0.053	(< 2.0)
年齡	0.007	-0.044	-0.037	-0.038	(< 2.0)	0.007	(< 2.0)
教育	0.074	-0.008	-0.014	-0.005	(< 2.0)	0.029	(< 2.0)
職業	0.217**	0.123*	0.112†	0.113†	(< 2.0)	0.112*	(< 2.0)
R^2	0.216	0.436	0.443	0.453		0.604	
ΔR^2		0.22	0.007	0.01		0.151	
F	15.222***	35.471***	31.115***	28.244***		46.039***	

顯著水準 †P<0.1 ; *P<0.05; **P<0.01; ***P<0.001

第四節 中介效果

中介變項成立與否必須符合三個條件：第一個必須成立的條件是屬直接效果的假設，在中介變項尚未納入考慮時，自變項與依變項間應存在顯著之關係。第二個必須成立的條件為，自變項與中介變項之間應存有顯著的關係。第三個必須成立的條件是，當自變項與中介變項均到納入模型中時，前述第一個條件的效果必須顯著地減少，即所謂的部分中介效果;或是全然地轉為不具顯著性，即所謂的完全中介效果。分析結果如表4-14所示：

根據以上的理論檢測中介變項，必須有三個迴歸式成立。第一，風險傾向對違反資訊安全行為之意圖的關係存在著顯著性的正向關係。第二，風險傾向與知覺風險之間存在著顯著性的負向關係。第三，當知覺風險納入風險傾向與違反資訊安全行為意圖之迴歸式後，後來的風險傾向對違反資訊安全行為之意圖為顯著，且後來的風險傾向之β值小於原先的風險傾向之β值，故為部分中介。在本研究中知覺風險是中介變項，由分析結果得知知覺風險、風險傾向與違反資訊安全行為之意圖為部分中介，意指風險傾向構面不一定要透過知覺風險構面才可以影響違反資訊安全行為之意圖。

表 4-14 中介效果分析

	模式1	模式2	模式3
依變項	意圖	知覺風險	意圖
自變項			
風險傾向	0.207***	-0.250***	0.129*
知覺風險			-0.313***
控制變項			
性別	-0.134	0.027	-0.125*
年齡	0.003	0.038	0.015
教育	0.101	-0.093	0.072
職業	0.240	-0.110	0.206**
R^2	0.144	0.113	0.231
Adj-R^2	0.128	0.097	0.214
F	9.273***	7.018***	13.768***

顯著水準 †P<0.1 ; *P<0.05; **P<0.01; ***P<0.001

從表 4-14 中的模式 2 來看，風險傾向與知覺風險之間為負向關係。顯示當受測者為風險趨避者時，此人較不易做出涉險行為，因此風險趨避者知覺到從事某項活動的風險是大的，則此人的知覺風險將隨之提高，進而不願意做出違反資訊安全之行為，故本研究的假設五是成立的。

第伍章　結果與建議

在此章，將討論本研究的研究結果、研究管理意涵與研究貢獻，本研究在操作時面臨的限制，並給與後續的研究學者建議與方向。

第一節 研究結論

本研究的研究目的欲探討使用者違反資訊安全行為之意圖，透過第四章的分析，得到的結果如表 5-1 所示：

表 5-1 研究假設檢定結果摘要表

研究假設	結果
H1：使用者的知覺風險與違反資訊安全之意圖呈負向關係。	成立
H2：使用者的知覺利益與違反資訊安全之意圖呈正向關係。	成立
H3：使用者的資訊安全認知與違反資訊安全之意圖呈負向關係。	成立
H4：使用者對資訊安全行為相關的人、網站的信任程度與違反資訊安全之行為意圖呈正向關係。	成立
H5：風險趨避者知覺某一項違反資訊安全行為的風險程度會比風險愛好者高。	成立

一、知覺風險與違反資訊安全行為意圖之關係

本研究結果顯示，知覺風險與違反資訊安全行為之意圖為負向關係。當使用者從事某項網路活動時，他/她所知覺到此活動結果的負面機率大或對自身的損失嚴重性是大的，則使用者比較不會去從事違反資訊安全的行為。

二、知覺利益與違反資訊安全行為意圖之關係

本研究結果顯示，知覺風險與違反資訊安全行為之意圖為正向關係。當使用者知覺此商品可以帶給自身好處與意義時，則使用者做出違反資訊安全行為的意圖會比較高。例如在網路活動中，當使用者發現某個網站中有自己需要的資訊時，則使用者登入此網站的意願就會變高，因為她/他認為網站中的資訊對自己來說是有用的，即可以帶給自己好處與利益。

三、資訊安全認知與違反資訊安全行為意圖之關係

本研究顯示，使用者的資訊安全認知與違反資訊安全行為之意圖為負向關係。當使用者具備較高的資訊安全認知時，則此人對於網路上的威脅、攻擊與弱點感到敏感，並且瞭解當自己做出違反資訊安行為後的負向結果。因此比較不願意做出違反資訊安全行為。

四、信任與違反資訊安全行為意圖之關係

本研究顯示,對朋友的信任、對網站的信任與違反資訊安全行為之意圖為正向關係。因為使用者與朋友具有情感上的聯繫，當使用者收到以朋友名義寄來的電子信件時，他/她對此信件的信任程度就會偏高，進而做出違反資訊安全行為。當使用者認為某網站具有一定的專業水準、聲譽，則對此網站的信任度就會偏高，因為她/他相信此網站不會對自身造成不好的結果，進而容易做出違反資訊安全行為。

五、風險傾向與知覺風險之關係

本研究顯示，風險傾向與知覺風險為負向關係。使用者為風險趨避者，比較不容易做出涉險的行為，當此人認為某件事的風險性是大的時候，則會提高他的知覺風險，因而不輕易做出違反資訊安全行為;反之，使用者為風險喜好者，因為此人愛好風險，會高估某件事情的正向結果，因而容易做出違反資訊安全行為。

第二節 研究貢獻與管理意涵

一、研究貢獻

透過本研究結果，提出過去未被學者所關注的新議題，也提供後續的研究者有繼續討論的方向。

過去的研究大部分都以正向觀點，了解使用者從事網路活動的行為以找出使用者遵循資訊安全的因素，進而使使用者願意遵循資訊安全。但本研究是以反向觀點，從使用者違反資訊行為中找出是什麼因素，會讓使用者不顧自身的資訊安全而願意做出違反資訊安全的行為。本研究以個人涉險行為為研究目的，以知覺風險、知覺利益、信任與資訊安全認知等因素探討個人違反資訊安全行為之意圖。研究結果顯示，知覺風險、知覺

利益、信任與資訊安全認知等因素都會影響個人的違反資訊安全行為之意圖，其中，個人對網站的信任最具影響力。本研究中探討個人的風險傾向是否會影響個人的知覺風險。發現當使用者為風險趨避者時，在從事某項網路活動時將會提高自身的知覺風險，進而不易做出違反資訊安全行為，且也發現個人的風險傾向也會直接影響違反資訊安全行為之意圖。

二、管理意涵

在這篇違反資訊安全行為之意圖的研究中,從研究結果中發現知覺風險、知覺利益、信任與資訊安全認知對使用者違反資訊安全行為之意圖均有顯著的影響。實務上從資訊安全的管理者與從業人員的角度來看，提高員工的資訊安全教育訓練是重要的。在日常生活中員工收到的電子郵件都具有一定的風險，因此在員工的資訊安全的教育訓練上要提高人員對資訊安全的認知，使人員對網路上的威脅、攻擊與弱點感到敏感，並且可以辨別釣魚郵件的結構與特徵，以避免員工點選下釣魚郵件。提高人員的風險意識，網路釣魚郵件的來源通常是假造的電子郵件地址，而且郵件中經常包含連接到詐騙網站的網址，因此無論是收到親友或主管所寄來的信件都要注意，因為這些信件的寄件者不一定是自己的親友或主管，有可能是詐騙者以他人的名義所寄出的信件，所以在點選信件之前最好要先與朋友或主管做確認，且信件內所附上的連結也要仔細的觀察，避免點選信件內可疑的連結。當員工收到一封看似利益很高卻又不須付出成本的信件時，都要注意可能是釣魚郵件。另外對於風險愛好者，要加以宣導資訊安全的認知與點下釣魚郵件的後果，進而提高風險愛好者的知覺風險，降低風險愛好者冒險點下疑似釣魚郵件內連結的意願。

第三節 研究限制與後續研究建議

一、 研究限制

本研究受到人力、時間與發放問卷等方面的限制，提供給未來後續研究的研究者最為參考並修正，使後來的研究者的研究能夠更完善，以下為本研究所受的研究限制：

本研究的樣本多數來自於親友幫忙，在受測者的職業的樣本中以學生居多，在受測者的年齡中以 21 到 25 歲的人居多，受測者年齡的差距、職業對違反資訊安全行為之意圖的因素所感受的程度不同，所以填答的方向也不同。

二、後續研究建議

(一)因為本研究對違反資訊安全之意圖的研究議題為個人涉險行為，之後的研究學者可以擴大違反資訊安全行為之研究，可對違反道德但卻不違反法律以及違反法律等兩大類的違反資訊安全行為之意圖加以研究探討。

(二)職業身分的不同對違反資訊安全行為意圖的因素所感受的程度也不同，冀希能夠在各職業收到的資料比例都相同，以期能夠分析不同職業之比較。

參考文獻

英文部分

Alba, J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A., & Wood, S. (1997). Interactive home shopping: consumer, retailer, and manufacturer incentives to participate in electronic marketplaces. *the Journal of Marketing, 61(3),* 38-53.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *Mis Quarterly, 26(3),* 243-268.

Bauer, R. A. (1960).Consumer Behavior as Risk Taking. in R. S. Hancock (Ed.), Dynamic marketing for a changing world, Chicago: American Marketing Association, pp.389-398.

Bhattacharya, R., Devinney, T. M., & Pillutla, M. M. (1998). A formal model of trust based on outcomes. *Academy of management review, 23*(3), 459-472.

Bloch, P. H., & Richins, M. L. (1983). A theoretical model for the study of product importance perceptions. *the Journal of Marketing, 47(3),* 69-81.

Boon, S. D., & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. *In R. A. Hinde & J. Groebel (Eds.), Cooperation and prosocial behaviour (pp.190-211). Cambridge: Cambridge University Press.*

Brockhaus, R. H. (1980). Risk taking propensity of entrepreneurs. *Academy of Management journal, 23*(3), 509-520.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Mis Quarterly, 34*(3), 523-548.

Carnevale, D. G., & Wechsler, B. (1992). Trust in the Public Sector Individual and Organizational Determinants. *Administration & Society, 23*(4), 471-494.

Cavusoglu, H., Son, J., & Benbasat, I. (2009). Information security control resources in organizations: A multidimensional view and their key drivers: working paper, Sauder School of Business, University of British Columbia.

Chang, A.-T. (2010). *Roles of perceived risk and usefulness in information system security adoption.* Paper presented at the Management of Innovation and Technology (ICMIT), 2010 IEEE International Conference on.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *Mis Quarterly, 22(1),* vii-xvi.

Chowdhury, S. (2005). The role of affect-and cognition-based trust in complex knowledge sharing. *Journal of Managerial issues, 17(3),* 310-326.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving

themes, a model. *International Journal of Human-Computer Studies, 58*(6), 737-758.

Cox, D. F. (1967). Risk handling in consumer behavior–an intensive study of two cases, risk taking and information handling in consumer behaviors: Harvard University Press, Boston.

Cunningham S M. The Major Dimensions of Perceived Risk. in Cox, D.F. (Ed.), Risk Taking and Information Handling in Consumer Behavior[M]. Boston Graduate School of Business Administration, Harvard University Press, 1967. 82-108

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *Management Information Systems Quarterly, 13*(3), 319-340.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of consumer research, 21(1),* 119-134.

Drennan, J., Sullivan, G., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: an exploratory study of household end users. *Journal of Organizational and End User Computing (JOEUC), 18*(1), 1-22.

Dunn, J. (2000). Trust and Political Agency. in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, *Department of Sociology, University of Oxford,* chapter 5, 73-93.

Fagley, N., & Miller, P. M. (1990). The Effect of Framing on Choice Interactions with Risk-Taking Propensity, Cognitive Style, and Sex. *Personality and Social Psychology Bulletin, 16*(3), 496-510.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474.

Forsythe, S., Liu, C., Shannon, D., & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. *Journal of Interactive Marketing, 20*(2), 55-75.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM Sigmis Database, 33*(3), 38-53.

George, D., & Mallery, M. (2003). Using SPSS for Windows step by step: a simple guide and reference: Boston, MA: Allyn & Bacon.

Ghosh, D., & Ray, M. R. (1992). Risk Attitude, Ambiguity Intolerance and Decision Making: An Exploratory Investigation*. *Decision sciences, 23*(2), 431-444.

Gutman, J. (1982). A means-end chain model based on consumer categorization processes. *the Journal of Marketing, 46(2),* 60-72.

Hansen, M. H., Morrow Jr, J., & Batista, J. C. (2002). The impact of trust on cooperative membership retention, performance, and satisfaction: an exploratory study. *The International Food and Agribusiness Management Review, 5*(1), 41-59.

Hoover, R. J., Green, R. T., & Saegert, J. (1978). A cross-national study of perceived risk. *the Journal of Marketing, 42(3),* 102-108.

Jacoby, J., & Kaplan, L. B. (1972). The components of perceived risk. *Advances in Consumer Research, 3*(3), 382-383.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross‐Cultural Validation. *Journal of Computer‐Mediated Communication, 5*(2), 0-0.

Johnson, D., & Grayson, K. (2005). Cognitive and affective trust in service relationships. *Journal of Business research, 58*(4), 500-507.

Keil, M., Wallace, L., Turk, D., Dixon-Randall, G., & Nulden, U. (2000). An investigation of risk perception and risk propensity on the decision to continue a software development project. *Journal of Systems and Software, 53*(2), 145-157.

Kim, D. C. (1992). Risk preferences in participative budgeting. *Accounting Review, 67(2),* 303-318.

Kogan, N., & Wallach, M.A.(1964). Risk Taking: A Study in Cognition and Personality. Holt, Rinehart & Winston, New York.

Kwak, D.-H., Kizzier, D. M., Zo, H., & Jung, E. (2011). Understanding Security Knowledge and National Culture: A Comparative Investigation between Korea and the US. *Asia Pacific Journal of Information Systems, 21*(3), 51-69.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications, 8*(3), 130-141.

Levi, A., & Koç, Ç. K. (2001). Risks in email security. *Communications of the ACM, 44*(8), 112.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces, 63*(4), 967-985.

Litwin, G. H., & Stringer, R. A. (1968). Motivation and organizational climate: Division of Research, Graduate School of Business Administration, Harvard University Boston.

Lovelock, C. H. (1983). Classifying services to gain strategic marketing insights. *the Journal of Marketing,* 47(3), 9-20.

MacCrimmon, K. R., & Wehrung, D. A. (1985). A portfolio of risk measures. *Theory and decision, 19*(1), 1-29.

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of applied psychology, 90*(4), 710.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20(3),* 709-734.

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management journal, 38(1),* 24-59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of management review*, 23(3), 473-490.

Miller, P. J., & Rempel, J. K. (2004). Trust and partner-enhancing attributions in close relationships. *Personality and Social Psychology Bulletin*, *30*(6), 695-705.

Mitchell, V. W. (1999). Consumer perceived risk: conceptualisations and models. *European Journal of marketing, 33*(1/2), 163-195.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *the Journal of Marketing*, 58(3), 20-38.

National Security Agency. National Information Systems Security Glossary. NSTISSI 4009 Fort Meade, MD. Sept. 2000

NIST (National Institute of Standards and Technology) 1995. An Introduction to Computer Security: The NIST Handbook. (Special Publication 800-12).

Park, C. W., Jaworski, B. J., & Maclnnis, D. J. (1986). Strategic brand concept-image management. *the Journal of Marketing*, 50(4), 135-145.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28.

Peter, J. P. (1979). Reliability: A review of psychometric basics and recent marketing practices. *Journal of marketing research*, 16(1), 6-17.

Petrick, J. F., & Backman, S. J. (2002). An examination of the construct of perceived value for the prediction of golf travelers' intentions to revisit. *Journal of Travel Research, 41*(1), 38-45.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness. Oulu, Finland: University of Oulu.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of personality and social psychology, 49*(1), 95.

Robbins, S. P. (2001). *Organizational Behavior, 14/e*: Pearson Education India.

Robinson, J. P., & Shaver, P. R. (1973). Measures of Social Psychological Attitudes (Rev. ed.). Ann Arbor, MI: Institute for Social Research.

Rohrmann, B. (2002). Risk attitude scales: Concepts and questionnaires. *Melbourne: University of Melbourne*.

Roselius, T. (1971). Consumer rankings of risk reduction methods. *the Journal of Marketing*, 35(1), 56-61.

Sheth, J. N., Mittal, B., & Newman, B. (1999). Consumer behavior and beyond. *NY: Harcourt Brace*.

Shimp, T. A., & Bearden, W. O. (1982). Warranty and other extrinsic cue effects on consumers' risk perceptions. *Journal of consumer research, 9(1),* 38-46.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8(1),* 31-41.

Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management journal*, *38*(6), 1573-1592.

Slovic, P. (1972). Information processing, situation specificity, and the generality of risk-taking behavior. *Journal of personality and social psychology*, *22*(1), 128.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security, 3*(2), 20-26.

Stone, R. N., & Grønhaug, K. (1993). Perceived risk: further considerations for the marketing discipline. *European Journal of marketing, 27*(3), 39-50.

Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *Mis Quarterly*, 14(1), 45-60.

Swaminathan, V., Lepkowska‐White, E., & Rao, B. P. (1999). Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange. *Journal of Computer‐Mediated Communication*, *5*(2), 0-0.

Tsai, Y. C., & Yeh, J. C. (2010). Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products. *African Journal of Business Management*, *4*(18), 4057-4066.

Vardi, Y., & Weitz, E. (2003). Misbehavior in organizations: Theory, research, and management. Mahwah, NJ: Erlbaum.

Wang, C.-C., Chen, C.-A., & Jiang, J.-C. (2009). The impact of knowledge and trust on e-consumers' online shopping activities: an empirical study. *Journal of computers, 4*(1), 11-18.

Warshaw, P. R., & Davis, F. D. (1985). Disentangling behavioral intention and behavioral expectation. *Journal of experimental social psychology, 21*(3), 213-228.

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain‐specific risk‐attitude scale: Measuring risk perceptions and risk behaviors. *Journal of behavioral decision making, 15*(4), 263-290.

White, G. B., White, G. W., Fisch, E. A., & Pooch, U. W. (1996). *Computer system and network security* (Vol. 7): CRC PressI Llc.

Willman, P., Fenton-O'Creevy, M., Nicholson, N., & Soane, E. (2002). Traders, managers and loss aversion in investment banking: a field study. *Accounting, organizations and society*, *27*(1), 85-98.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*, 50.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86-110.

Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence. *the Journal of Marketing*, *52(3)*, 2-22.

中文部分

吳萬益、林清河(2000)。企業研究方法，台北:華泰書局。

宋明哲(2001)。 現代風險管理: 五南圖書出版股份有限公司。

李碩育(2010)。線上信任之影響因素探討，未出版碩士論文。大葉大學，彰化縣。

周宣光(2001)。管理資訊系統-管理數位化公司。東華書局，民國 92 年。

邱皓政(2006)。量化研究法: SPSS 中文視窗版操作實務詳析，統計原理與分析技術。台北市:雙葉書廊。

蕭瑞祥、許容豪(2008)。圖形教學運用於資訊安全認知訓練之研究。資訊管理展望, 10(1), 69-87。

黃洲煌(2000)。個人人格特質、激勵認知、工作態度與組織公民行為之關聯性研究。國立台灣科技大學管理研究所企業管理學程。

網頁

賽門鐵克（2012）。駭客藉奧運搗亂 網路詐騙攻擊花樣百出，取自 http://www.symantec.com/zh/tw/about/news/release/article.jsp?prid=20120810_01

賽門鐵克（2009）。釣魚網站報告第 7 期，取自 http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_07-2009.en-us.pdf

賽門鐵克（2006）。倫敦奧運將近網路個資安全面戒備，取自 http://www.symantec.com/zh/tw/about/news/release/article.jsp?prid=20120613_01

反網路釣魚工作小組（2008）。2008 年第一季全球網路釣魚趨勢調查報告，取自 http://www.i-security.tw/learn/sub_200811_2.asp

經濟合作及發展組織理事會(OECD), Security Guideline http://www.oecd.org

NIST Special Publication 800-50, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf, October 2003.

附錄 問卷

親愛的先生、女士您好：

感謝您抽空填答此問卷。這是一份關於資訊安全相關議題之研究的學術問卷，期盼獲得您的協助。本問卷純屬學術研究之用，不做其他用途，並採不具名方式填寫，敬請安心作答。我們在此致上最誠摯的謝意與祝福。非常感謝您在百忙之中撥冗幫忙。

敬祝

平安順心

東海大學企業管理研究所
指導教授：張榮庭　博士
研究生：丁紫涵　敬上

【第一部份】請先閱讀下述信件的情境內容。

再過三天就是您的生日，假設您收到高中時期很要好的朋友寄來的電子郵件，在高中時期您與這位好友很要好，做什麼事都是一起的，雖然現在無法常常碰面，但依然保持聯絡(請預想一位高中朋友)。信件中的內容告知您，朋友為了要慶祝您的生日從 Timbuk2 網站中挑了個包包當禮物送給您。禮物的錢已經付了，因為網站的包包可以客製化的關係，假如您不中意朋友為您選的款式與圖案，也可以到 Timbuk2 網站重新選擇您喜歡的款式與圖案。以下是信件的內容：

看完上述情境內容後，請依照您個人的看法並加以預想後回答下列的問題，答案沒有對錯之分，請您依看完情境後所引發的個人看法或感受圈選即可。

(請依順序填答)

		非常不同意						非常同意
1.	我打算開啟此電子郵件中的連結。	1	2	3	4	5	6	7
2.	我將會開啟此電子郵件中的連結。	1	2	3	4	5	6	7
3.	整體而言，我覺得這個商品的品質是可信賴的。	1	2	3	4	5	6	7
4.	我覺得這個商品的實用性高。	1	2	3	4	5	6	7
5.	我覺得這個商品讓人覺得是值得的。	1	2	3	4	5	6	7
6.	我覺得這個商品可依照我的傾向來設計。	1	2	3	4	5	6	7
7.	我覺得這個商品品牌有好的聲譽。	1	2	3	4	5	6	7
8.	我能夠與這位朋友自由地分享想法、感受和期許。	1	2	3	4	5	6	7
9.	當我與這位朋友表達問題時，我相信對方願意傾聽。	1	2	3	4	5	6	7
10.	如果告訴這位朋友我的問題，我相信對方會給我有建設性的回應。	1	2	3	4	5	6	7
11.	我與這位朋友已建立深厚的關係。	1	2	3	4	5	6	7
12.	當我與這位朋友斷了聯繫時，我會感到失落。	1	2	3	4	5	6	7

上述的情境中，希望您能點選信件內所附的網址，請繼續回答下列問題，答案沒有對錯之分，請依您個人的想法圈選即可。

		非常不同意						非常同意
13.	我相信這個網址。	1	2	3	4	5	6	7
14.	Timbuk2 網站具備專業水準。	1	2	3	4	5	6	7
15.	我可以放心地點選這個網址。	1	2	3	4	5	6	7
16.	我相信點下這網址之後的結果不會造成困擾。	1	2	3	4	5	6	7

請依據您個人的看法來決定同意程度，答案沒有對錯之分，請您圈選最適合的選項即可。

	非常不同意 ← → 非常同意						
17. 我覺得此電子郵件為釣魚信件的機率是大的。	1	2	3	4	5	6	7
18. 我覺得點下此郵件中的連結後所造成個人資料外洩的損失是大的。	1	2	3	4	5	6	7
19. 整體來說，我了解違反資訊安全行為的相關威脅與可能的負面結果。	1	2	3	4	5	6	7
20. 對於潛在的資訊安全問題，我具有足夠的知識。	1	2	3	4	5	6	7
21. 我了解與資訊安全相關的議題及違反資訊安全的相關可能的風險。	1	2	3	4	5	6	7
22. 我熟悉釣魚郵件的相關資訊。	1	2	3	4	5	6	7
23. 對於釣魚郵件的相關風險，我具有足夠的知識。	1	2	3	4	5	6	7
24. 我了解釣魚郵件的結構特徵。	1	2	3	4	5	6	7
25. 我了解與釣魚郵件的相關議題。	1	2	3	4	5	6	7

【第二部份】此部分為第二個情境題，欲了解資訊安全決策者之風險喜好，對個人資訊安全決策的影響。下述的情境請依您個人的感受，圈選最適合的選項，答案沒有對錯之分。

A 先生經常以電子郵件與工作同儕聯絡。昨日 A 先生收到以直屬長官名義寄來的一封疑似釣魚郵件，且因近年來釣魚郵件詐騙頻傳，因此 A 先生決定將此信件交給熟識的資訊安全專家 M 先生判斷。

當 M 先生看過這封電子郵件後，他告訴 A 先生此郵件為釣魚信件的機率為 **75%**，而且可能會造成 A 先生的個人資料外洩，包含**身份證字號**、**信用卡卡號**、以及其常用社交網站**帳號**及**密碼**被盜。

想像一下，如果您是 A 先生的要好同事，您覺得 A 先生打開啟此信件連結的風險(危險程度)高或低?

	非常不同意 ← → 非常同意						
我認為開啟此信件連結的風險(危險程度)**高**。	1	2	3	4	5	6	7
我認為開啟此信件連結的風險(危險程度)**低**。	1	2	3	4	5	6	7

承上述情境。雖然這封信件具有潛在個資外洩的風險。但另一方面，這封郵件可能有主管交辦的重要資訊，使得 A 先生猶豫要不要點選這封信件內的連結。想像一下，身為 A 先生好友的您，在下列哪一種最高機率情況下，您會建議 A 先生
不要點這封信件內的連結。

□ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 10%
□ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 30%
□ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 50%
□ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 70%
□ 此信件被資訊安全專家(M 先生)評估為釣魚信件的機率為 90%
□ 無論機率為何，都不會建議 A 先生點這封信件內的連結。

【第三部份】基本資料 請您在適當□中「勾選」，皆為單選題。

1. 請問您的性別： □男 □女
2. 請問您的年齡： □16-20 歲 □21-25 歲 □26-30 歲
   □31-35 歲 □36-40 歲 □41-45 歲
   □46-50 歲 □51 歲以上
3. 您的教育程度： □國中(含)以下 □高中(職) □專科
   □大學 □碩士 □博士
4. 您的職業類別： □軍警 □公教 □服務業
   □金融保險 □電子資訊 □醫護
   □學生 □製造業 □研究員
   □其他(請填寫)_____
5. 去年是否曾收過釣魚郵件
   □是 □否

問卷到此，感謝您的填寫。