國 立 交 通 大 學 教 育 研 究 所

碩 士 論 文

中學生資訊安全課程設計與發展

研究生：謝淵任

指導教授：周倩博士

中 華 民 國 九 十 三 年 八 月

中 文 摘 要

本研究主要在設計與發展一套適合中學生(包含國中與高中)的「資訊安全」課程。近年來隨著網路與資訊科技的發達，與資訊安全有關的議題也不斷衍生，因此本研究者認為凡涉及與資訊有關的安全防護或傷害，都可將其歸於資訊安全所探討的議題中。

根據文獻分析的結果，研究者認為資訊安全的課程內容至少應包含三個面向，分別為「電腦網路與通訊安全」、「資訊的正確與合宜性」以及「使用者的人身安全」等三部分，前者包含了如電腦病毒、駭客相關資訊，另一則包含網路謠言與垃圾郵件，後者涵蓋了使用電腦的安全須知等內容，此外，在教學設計方面，採系統化教學設計，以達成課程的教學目標。

藉由教師深度訪談、國高中電腦課本內容分析以及對學生資訊安全概念與態度上的調查，瞭解資訊安全課程的需要性與應包含教學項目、適合的教學活動，同時也對學生的起點能力有基本的瞭解。本研究將資訊安全課程規劃為四個單元，分別是「網路安全ｅ起來」、「電腦健康百分百」、「網路逍遙遊」以及「個人資料不漏白」，在所設計之「資訊安全教學單元」中，包含教學流程、教學活動以及參考資料等，提供教師作為資訊安全課程教學上的參考。

研究者並根據此份「資訊安全教學指引」，實際到新竹建功國中國一的兩個班級及台北市大同高中的高一某班試教，課後並就教學內容、作業評量和對學生的影響方面，請同學填寫問卷。

由資料的分析結果顯示，本教材在內容豐富度、組織性和帶給學生的收穫方面，普遍獲得學生肯定。除了請學生做課後評估之外，本研究亦請在學科內容以及教學設計方面的專家就「課程規劃」、「課程目標」和「課程內容」、「教學」及「評量實施」等方面做專家評鑑，整體說來，受訪的專家教師多認為整份教學指引內容豐富，教學方式多元，很能引起學生學習興趣。

關鍵詞：資訊安全、中學生、課程設計

Abstract

The goal of this study was to design and develop an information safety curriculum for Taiwan junior and senior high school students. With the development of Internet and information technology, issues related to information safety have been growing fast in recent years. The concept of information safety is defined by this study as “any protection and damage related with information should be included within information safety topic.” According to reviewed literature, the information safety curriculum should have three parts. The first is “Internet and Communication Safety”, including computer virus, hacker and so on. The second one is “Correctness and Appropriateness of Information”, including Internet rumor and spam. The last one is “Body Safety of Users”, covering safety guidelines for using computers. The curriculum of the presented study was developed based on Dick & Carey’s “Systematic Instructional Design” model to reach the instructional target.

In order to analyze the needs, learning contents, and related activities to be covered in the curriculum, the researcher used multiple methods: conducting in-depth interviews with representative teachers, analyzing the content of high school computer textbooks, and surveying students on their existing knowledge and attitudes of information safety. The resulting curriculum was divided into four units: (1) Network safety together, (2) Healthy computer-using habits, (3) Surfing the Internet, and (4) Keep your secrets online. This study designed an “Information Safety Teaching Guide (ISTG)” which covered the teaching flows, lesson plans, learning resources, and references.

This study also conducted a formative evaluation of the ISTG. Four units based on the ISTG were actually taught to two high school classes. Students’ opinions toward the curriculum content, homework and the learning experiences were collected and analyzed. The results showed that most students considered these units rich and well

structured, and they felt they did learn some new and useful information. In addition, the experts of content and instructional design were invited to evaluate five dimensions of the curriculum: (1) instructional design, (2) curriculum target, (3) learning contents, (4) pedagogies, and (5) evaluation. Basically, most of the experts thought that the curriculum was versatile in activities and abundant in information, and could arouse students' interests effectively. Recommendations for future studies were also provided.

key words：information safety, Taiwan high school students, curriculum design

誌　謝

兩年前，颱風來襲的傍晚，一通電話的響起，從此決定往後兩年的落腳處；兩年過去了，一個炎熱的夏日午後，就在鍵入結尾的標點符號後，我的論文，終於、好不容易告一段落，心頭中懸了兩年的大報告，總算可以放下了。

今日得以完成這本論文，要感謝的人真的太多了，其中最感謝的是我的父母親以及我的哥哥與姊姊們，家中排行老么的我，不論是在成長或求學階段，家人都給我無限的支持與鼓勵，讓我在生活方面沒有後顧之憂，也減少了許多不必要的麻煩，這樣的心情，真的很難用鍵盤敲打出對家人的感激。

而讓論文從無到有，逐漸搓揉成形，最辛苦的可能是我的指導教授周倩老師，因為我的腦筋一向不甚靈光，加上創意不足，寫論文的過程真的好像大冒險似的蹉跎好多光陰，幸好周老師始終沒放棄我，最令我佩服的是，每次論文寫到連自己都看不下去時，老師還是可以把我的論文仔細檢查個好幾回，這樣認真、敬業的態度，真的是讓我不知如何對老師表達我的欽佩與感謝之意。

此外，在這段期間內，也很感謝所上的每位老師，對自己的協助，老師們親切以及豐厚的學養，都為我提供了相當好的表率。而所上的每位學長姊，也都是很好的模範，讓我不論在生活上或研究的過程，都有遵循的對象。在研究所同窗兩年的同學，小惠、蕙玲、素蘋、建妤、佩陵、琇櫻、佩珊、俊昇、芳吟，真的很高興在這邊認識大家，也一起渡過了許多美好的日子，擁有很好的回憶；也要感謝教育所所辦的嘉凌姐跟慧珍姐，感謝她們的照顧，讓我在所辦打工時，學了很多也認識了許多人。

更感謝在口試時，兩位口試委員所提供的寶貴意見，讓我找出自己研究中的盲點，也讓自己的思路變得寬廣許多。最後也感謝教育部電算中心「中小學網路素養與認知」計劃、國科會研究計劃(NSC92-2520-S-009-006)對本研究之支助，並感謝研究中所拜訪的各位資訊教師的協助。

差點還忘了該感謝一個人，那就是雅婷，這一年因為有妳的陪伴，讓我在新竹枯燥的生活，逐漸有一點色彩，也讓我得以堅持下去，完成論文，當然，今後

更要一起努力。

在寫完論文的剎那，突然感受到以前在研究法時，周老師跟方老師提到的，我們做的研究，其實是累積了很多人的研究結果而逐漸堆積而成的，就如同站在巨人的肩膀上，這時，我終於瞭解，原來，在研究領域中，自己的渺小以及微不足道。

目　錄

表　目　錄

圖　目　錄

第一章　緒論

第一節　研究背景

資訊時代的來臨，世界各國無不戮力推行資訊建設，隨著國家政策性的引領，資訊工業的發展已經成為我國首屈一指的產業；資訊科技的應用，從個人電腦的普及，到網路行銷事業的蓬勃發展，以及學習科技的推動，所涵蓋的範圍甚為廣泛；自從民國八十三年起政府積極推動國家資訊通信基本建設（NII），負責推動國內資訊網路的建設與資訊科技的應用，使國內網際網路的使用人口不斷成長。

教育向來為國力的基石，在 NII 的基礎上，為推動各級學校資訊教育，教育部自民國八十七年，推動擴大內需方案，編列了六十七億元的經費（行政院，1998），購置全國中小學的電腦設備，大幅的提昇學校的資訊環境與教師學生的資訊能力；如此在整個大潮流的帶動下，講求數位化、電子化的學習環境儼然成形。就在我國教育政策的推動下，資訊教育伴隨著國民中小學九年一貫課程的進展，以往安排在國中的電腦課程已向下延伸至國小階段，對許多國小學童來說，具備基本的電腦操作技巧不再是遙不可及的願景，資訊科技已成為生活中必備的工具，更是學習的好幫手。

然而，科技的易取得性以及網際網路的快速傳播等特性，一方面為生活帶來許多便利之處，但相對的，許多伴隨資訊科技的問題也相繼產生，例如電腦病毒的散佈與駭客的入侵等資訊安全問題，更是對資訊時代中一切強調資料數位化、網路普及化的環境，產生困擾甚至是災難；因此，如何預防這些資訊時代所產生的問題，便成為當前重要的課題之一。

過去有關資訊安全的議題，大多限於商業團體或政府機關等組織，因為對於電子商務的推動以及公文資料的數位化而言，安全實屬一個不可或缺的議題；但是近年來隨著個人電腦及網際網路的普及化，許多人感受到資料保存以及網路通訊安全的重要性，多數學者專家在提出相關的因應之道時，都認為從教育層面著

手，將可以有效地提升對資訊安全的重視；據此，本研究的目的，即希望發展一套適用於中學生的資訊安全課程，一方面可以加強學生在資訊安全相關的認知，同時也可以對安全防護的技巧有所了解。

第二節　研究動機

安全一詞可以就兩個層面來探討，其一是使人的生命不受到傷害，其二是讓人的心裡不會感受到威脅或恐懼，甚至產生恐懼。資訊科技有其便利性，但也有其黑暗面，而資訊安全所要探討的，就是使人們不僅可以自在地運用科技來豐富生活，同時也可以避免科技所產生的許多負面效應，排除各種由人為或設備所造成的不良影響，降低生活中所可能產生的危機。隨著產業的升級，電腦網路硬體設備的完善，當前的教育潮流，對於資訊科技的運用，正值方興未艾之際，然而正當教師或學生對電腦網路環境的熟悉程度以及多數人運用資訊科技的能力已大幅提升之際，對於資訊科技使用的「適切性」與「合理性」認知，卻未必能同步成長；例如青少年沈迷於網路世界中，或在網路上所引發的敵意等問題，以及在網路上不斷充斥著各種如電腦病毒的惡意程式，與到處入侵系統的駭客，還有各種謠言的充斥以及垃圾信件的氾濫（李維倫，2003；林修遠，2001；黃宏宇，2003；蔡靚萱，2002；Chou & Hsiao, 2000），都是目前使用資訊科技時不可忽視的威脅；此外，對於使用者在使用電腦時所應注意的健康資訊，以及網路上個人隱私的保護（蔡敦仁，2002）等，在在與日常生活密切結合，且成為近年來備受關注的重要議題。

近年，在我國中小學資訊教育的課程中，逐漸加入有關資訊素養的內容（尹玫君，2000a；何志中，1999；康春枝，1999；張郁蔚，2003），期望改善資訊科技使用的合宜性。然而，資訊安全似乎是一個較易為人所輕忽的內容；或許一方面，在校園當中，不論對象是學生或教師，總是較為單純的族群，另一方面在校園中所面對的環境，也大多不如商業場合般有機密性的顧慮，因此在校園環境

中，儘管享受資訊科技帶來便利性的同時，卻往往忽略對資訊的安全性的關注(李忠憲，2001)。

根據許怡安（2001）對網路媒體素養課程所做的研究，認為網路素養課程應包含批判性思考、資訊評估、近用能力等幾個面向之外，安全保護、法律規範以及網路倫理與禮儀等面向也是不可或缺的內容。另外，張芳綺（2002）在中學生網路素養課程設計發展研究中，將網路素養分為五個面向，分別為人際的互動、資訊評估、網路犯罪與法律問題、網路對個人與社會的影響以及電腦網路資料的處理與安全，由此可知，資訊安全的重要性已逐漸突顯出來；本研究者以為，置身於資訊與網路無所不在的知識經濟時代裡，除了一切講求資訊的便利與豐富性之外，對電腦網路安全的重視，亦屬刻不容緩的事，因此，我們應該藉由學習，以了解與建立起相關的知識，方能為自己或他人甚至整個團體，提供有效的保障。

第三節　研究目的

本研究旨在研發中學生學習資訊安全教育的課程，針對資訊安全的內涵、目標以及課程教學指引的可行性與有效性，發展出適合中學生學習的課程內容，並對該課程進行形成性評鑑。本研究的具體研究目的如下：

一、資訊倫理、資訊素養的意涵分析，歸結出資訊安全應涵蓋的範圍。

二、估中學生學習資訊安全的需求性。

三、界定中學階段學生所應學習的資訊安全課程內容。

四、設計適合中學生的資訊安全課程內容、指引以及素材。

五、對該課程的內容進行形成性評鑑，以評估該課程的使用性和學習內容與策略的適切性。

第四節　研究架構與章節配置

為了達成研究目的，本研究所採取的程序如後：首先，本研究將藉著文獻的探討，由資訊素養與資訊倫理出發，整理出研究中所要探討有關資訊安全的意涵與範圍，同時進行資料的蒐集與分析，在擬定的資訊安全課程內容中，探討各主題的意涵以及管理與防治措施；最後，檢視當前我國資訊教育的現況，指出課程中不足之處，再根據所蒐集的資料與文獻推論出資訊安全課程設計的基本原則以及指引，並探討中學生在資訊安全教材中所應具備的認知能力與態度。

藉由文獻探討的結果，確立本研究的設計理念與方法，正式進行教學課程的研發階段。在教學設計的過程，主要依照分析、設計、發展、評鑑與修正等課程設計的階段，進行課程教材的研發，並於評鑑階段檢視整個課程設計理念，提出研究的結論與建議，參見圖 1-4-1。

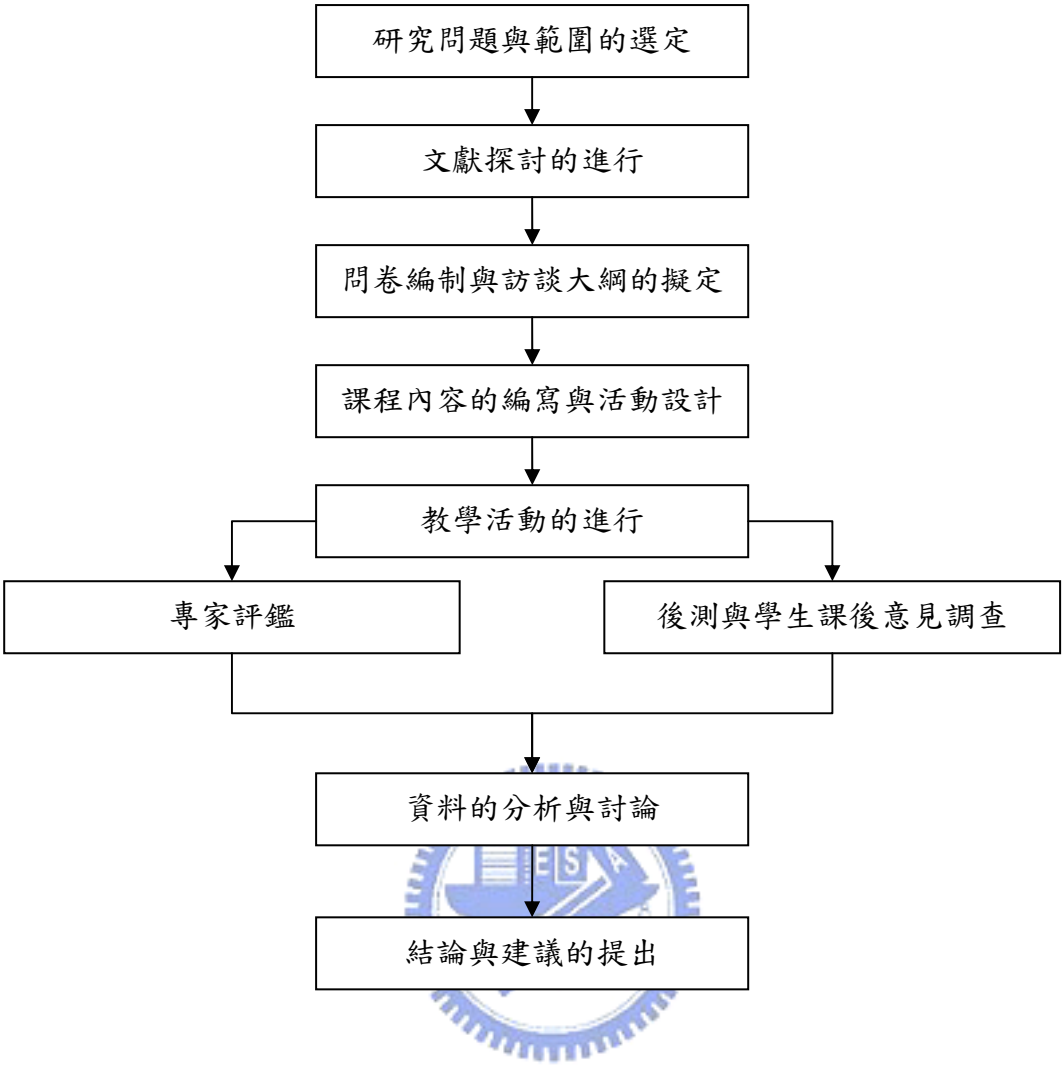


圖 1-4-1 研究程序

第五節　預期研究成果

本研究預計達成下列幾項成果：

一、透過文獻的分析，預期可以歸納出中學生學習資訊安全的課程內容。

二、透過本研究的完成，預期可以編擬出「中學生資訊安全概念與態度評量表」。

三、本研究所建構的資訊安全課程，設計的教學指引，教導學習者在學習資訊課程當中增進有關資訊安全的認知與防護的技巧，預期可以使中學生對資訊安全的瞭解與預防等相關概念有顯著提升之成效。

四、所設計的資訊安全課程，將可作為中學生實施資訊相關課程的參考。

五、根據研究的結果，提出具體的建議，以作為實施中學生資訊素養課程之參考。

第二章、文獻探討

本研究的主要目的在發展中學生的資訊安全課程，因此本章所要探討的主題可以分為六個方向，第一節從資訊素養、資訊倫理的所涵蓋的主題歸結出資訊安全所應具備的意義與內涵，第二節探討電腦網路通訊安全如駭客、電腦病毒等相關問題，第三節則討論資訊的正確、合宜與私密性，包括網路謠言、垃圾信件與個人隱私等議題，第四節則討論個人使用電腦的保健資訊，而上述三節所探討的內容，將作為資訊安全課程內容設計的基礎。第五節則探討我國現階段的資訊教育，第六節為本研究所採取的教學設計模式。

第一節　資訊素養、資訊倫理與資訊安全

我們常認為當前的時代是所謂資訊爆炸的時代，但究竟何謂資訊，資訊科技所指的是什麼？在一般的理解中，可以經由符號、文字、圖形等來表示特定目的與意義的便稱為資訊（Information），謝清俊（1997）將資訊科技（Information Technology）定義為「利用電子媒介所發展出的新系統或新的傳播方式」，而黃淑靜（2002）從教育的觀點出發，認為資訊科技所指的就是與傳遞訊息有關的技術領域，尤其是電腦、數位電子學和電信有關的技術。因此舉凡過去的廣播電視到現在的電腦網路多媒體等，我們都可以將其囊括在內；面對新的時代、新的資訊傳播工具，人們應該發展出可以與新興科技相對應的新思維與素養。

一、資訊素養

隨著資訊時代的到來，面對生活中，資訊化腳步的加快，漸漸的，具備適應未來社會生活或有效應付急遽變遷環境的能力也變得更重要，資訊素養（Information Literacy），便是在這樣的情形之下所產生的一種概念；素養（Literacy）一詞原指的是一個人讀、寫的能力，然而時代的更迭，傳統的素養已逐漸擴大為對一件事物有判斷、解決問題以及應用的能力（關淑尤，2002）；

早在 1974 年，當時的美國圖書館與資訊科學學會主席 Paul Zurkowski，在一次全國資訊服務及圖書館人員的委員會會議報告上首次提出「資訊素養」這個名詞（Doyle, 1994），認為資訊素養者所指的是某些人，可以學習擁有豐富資源的工具，並有效的解決他們所面臨的問題。

此外，許多的學者專家也都曾對資訊素養加以詮釋，例如美國圖書館學會(American Library Association，簡稱 ALA)在 1989 年對資訊素養的定義為「一個人具有能力知道何時需要資訊、且能有效的尋得、評估與使用所需要的資訊。」1992 年 Doyle 進一步利用 Delphi 循環問卷法的方式，結合全美各地 136 位受訪者的意見，將「資訊素養」進一步定義為：「有能力自各種不同的資訊來源，獲取、評估及使用資訊」（引自陳敬衡，2002），我國學者吳美美（1996a）討論資訊素養的意涵，認為可分成內外兩個方面：首先，就內在而言，係指能釐清問題，能分析所需的資訊，並能解讀資訊，以及整理資訊。就外在而言，指知道如何去尋找資訊，以及能將資訊加以整合後展現出來。

而關淑尤（2002）針對國小行政人員的資訊素養之研究中，認為資訊素養並非僅屬於資訊科技時代的代名詞，而是一種解決問題的關鍵能力、一種可以和外界做合理而有效溝通和互動，且終身受用的能力。

由以上看來，過去對於資訊素養的定義，大多與圖書館學當中利用資訊以及搜尋資料並用於解決問題的能力有關，或者狹義的解釋，便是指「電腦素養」（Computer Literacy），泛指操作電腦的能力；例如康春枝（1999）則提出資訊素養有廣義及狹義之說：廣義上來看，資訊素養包括傳統素養、媒體素養、電腦素養及網路素養。狹義上來看，有的人將之視為只是電腦素養而已 。此外，McClure（1994）提出資訊素養應涵蓋四個層面能力之觀點，他表示資訊素養不但是一種觀念，更是一種態度與解決問題的能力，所涵蓋的素養包括傳統素養(Traditional Literacy)、媒體素養(Media Literacy)、電腦素養(Computer Literacy)以及網路素養(Network Literacy)等四種；而 Plotnick（1999）更認為資訊素養是一種決定未來成功與否的關鍵能力，除了熟識平面印刷文字之外，

包含各種視覺媒體、聲音媒體、電腦、網路及其他基本的能力都可以囊括在資訊素養的範疇之內。

雖然各方對資訊素養的定義莫衷一是，不過可以發現，因為研究者的角度不同，對資訊素養一詞有不同的延伸，但大抵跳脫不出某種技能方面的認知；然而資訊素養除了能夠閱讀、寫作以及正確的搜尋自己所需的資訊，並具備使用資訊科技的能力之外，對於人類社會所存在的內涵以及在資訊時代應有的認知，也逐漸的被涵蓋在資訊素養的定義中；例如我國教育部在民國八十七年推動的擴大內需方案中，針對中小學資訊教育教師在職進修與教學應用提出計畫，計畫中所訂之教師的資訊基本素養指標包括三大類，分別為：(一)資訊課程專業素養；(二)套裝軟體及應用軟體操作素養；(三)各科應用網路資源進行個人教學活動。此素養指標所列大多以教學應用與網路應用為主，然而在資訊課程專業素養當中的能力類別，也列出了如能了解網路禮節、能尊重智慧財產權、能了解資訊安全的重要性以及能了解電腦為一般教學工具等幾項能力（教育部，1998)。

前述提及資訊素養的概念可說是一種綜合的能力，然而網路的興起，面對網路世界多元化與訊息瞬息萬變的特性，許多人提出了「網路素養」的概念；何志中（1999）認為「網路素養」，是指個人在學習的過程中，了解對資訊需求後，能利用網路去檢索、評估、組織程利用電子型式資訊的能力，並認同網路的價值，願意與人互動溝通，此外還必需能遵守網路的倫理規範。

陳炳男（2002)，探討國小學生所應具備的網路素養內涵，認為教師在培養學生資訊素養時，應該要有新的體認以及省思資訊時代的意義，並適當的調和人文與科技，因此學生所應具備的資訊素養係指「網路知識」、「網路操作技能」及「網路使用態度」等三部分：

（一）網路知識：指學生能理解網路的發展、功能與多樣性，也就是學生能理解網路的基本概念，並對網路的特性有所認識。

（二）網路操作技能：是指學生具有檢索與重組資訊的能力，亦即學生能尋找並評估自己所需的資訊。

（三）網路使用態度：是指具有網路使用倫理及人際溝通互動的能力，學生在使用網際網路時，對人際之間的基本認知以及相關的規範都有所體認，並能加以遵守。

在美國，國際教育科技學會（International Society for Technology in Education, ISTE）所提出的教師教育科技標準（National Educational Technology Standards for Teachers, NETS-T），就是在提供師資培育計畫或機構培訓教師科技能力的導引，共分為六大能力及二十三個指標（ISTE, 2002）。其六大能力分別為科技的操作及概念、規劃學習環境與經驗、課程的教與學、評估與評鑑、生產力和專業實務以及社會、倫理、法律以及人類方面的議題，除了前五大基本能力，是以科技的相關概念與教學的成效考量為主之外，第六個能力中包含了對人類社會、倫理、法律方面的基本認知，而其能力指標一共包含了五種能力的展現，如下：

（一）進行有關科技使用上的法律和倫理觀念的教學活動及示範。

（二）運用科技資源，使不同背景、特性和能力的學生均得以發揮潛能。

（三）確認並使用多樣化的科技資源。

（四）促進科技使用的安全與健康。

（五）促使所有學生能公平使用科技。

其中第四項能力指標即為本研究中所探討的議題。而陳泰安（2002）在探討九年一貫課程教師資訊素養能力的研究中也表示，國中教師應具備之資訊素養能力可以依照高雄市中小學教師資訊素養能力指標，將其分為初級指標、中級指標及高級指標三大類，並在初級指標中，除了原本強調一般電腦軟體的操作能力之外，也加入資訊倫理、網路禮節、智慧財產及資訊安全等必備資訊素養能力。

此外，黃淑珠（2000）對於高職生的電腦網路態度、素養及使用現況的研究中，由文獻的歸納結果，將電腦網路素養分為三個構面，分別為

（一）電腦網路基本知識：及電腦網路的概念、構成等認知。

（二）電腦網路的操作：如檢索資料或是檔案的傳輸等基本技能。

（三）電腦網路道德：包括了電腦網路的安全、資訊智慧財產權的意義、資料的保護等。

根據以上的討論，我們可以了解，對於「資訊素養」的解釋，從過去單純用來指資訊搜尋以及應用的能力，到所謂的電腦素養，意指操作電腦的能力，最後又加入了在資訊時代中，所必須具備的倫理觀等議題的認知；因此今日所指的資訊素養，是一種綜合的認知、概念與能力，也是一種善用資訊解決問題的能力，更可說是一生受用的能力。今後，面對日益繁雜的資訊社會，學生或教師不但應該具備基本的讀寫或資訊搜尋與運用的能力，同時也要對電腦網路虛擬社會有相關的認知與理解，才能在一波波的資訊洪流之中，面對並解決接踵而來的問題。

二、資訊倫理

倫理學（ethic）在拉丁文稱Ethica，原意是指風俗習慣，廣義來說，倫理學的範疇包括了人行為的性質、標準、良心以及法律的基礎；另外，對於倫理，我國古籍「淮南子•要略」記載：「經古今之道，治倫理之序。」意思就是指℃人倫道德的常理，也就是人跟人之間所產生的種種關係，所應該遵守的規範（線上國語辭典，n. d.）；因此我們可以將倫理當作是一個社會的道德規範系統，作為人們在動機或行為上判斷是非善惡的標準，易言之，倫理其實就是懂得人與人之間的相處之道，判斷是非，以及知道要為自己的行為去負責（Schwartau, 2001）。

（一）資訊倫理的意義

資訊科技是一項影響這個時代非常深遠的產物，人們的生活因它的普及，而逐漸有了重大的改變，面對這樣的新媒介與新的互動模式，資訊倫理便是規範人在使用任何資訊時所需遵守的準則，簡單的說，就是人與資訊之間的關係，藉

由倫理道德的是非善惡觀念，建立起行為的標準與規範，提供使用者取用資訊的依據（許秋芬，2001）。

而 Baird（2000）認為，傳統在資訊倫理上的問題，是因為在使用資訊科技上缺乏適當的行為基準，所以資訊倫理的主要任務就是用來決定人們在使用資訊科技的情形之下，應該有怎樣的行為表現，也就是有一定的行為基準來規範；他並表示，資訊倫理是複雜的而且隨時在改變的，它會隨著資訊科技的改變而持續改變事實、概念、方針與價值等之間的關係，因此資訊倫理不是一個固定的規則，也不是將死板的倫理原則應用到沒有價值的科技上，資訊倫理的出現讓人們重新思考自身和科技資訊的本質；Johnson（2001）也表示，探討資訊倫理的重要性，是因為當新的科技為人類的行為創造出新的可能性時，同時也造成了某些倫理議題和概念的混淆，因為這些被創造出來的新的可能性並非永遠都是有益的，因此，人們需要加以評估這些可能性並藉由這樣的評估方式，在科技發展的每一個階段，塑造出更好的科技，同時也能將負面效應減到最低。

另外，黃貞芬、許孟祥和林東清（2000a）由決策制定的方向著力，認為資訊倫理涉及某些關係人的受害或受益的行動決策。不論是資訊產品的政策訂定、規畫、設計、製造到銷售等不同階段之決策人員，在制定相關決策時，都會面臨不同的資訊倫理議題，因此他們認為所謂的資訊倫理，為決策者對於資訊相關之倫理議題上的權利與義務，以及賦予決策者對此倫理議題在決策或行動上之是非善惡判斷之基準。

面對日益繁雜的資訊議題，資訊倫理的探討也就益發的重要；Hester 與 Ford（2001）將研究資訊倫理的重要性，由淺至深地分為六個層次，分述如下：

第一層、可以讓我們對自己的行為舉止負責。

第二層、可以教導我們如何避免電腦的濫用與災難。

第三層、資訊科技的發展會產生暫時無法解決的問題，因此資訊倫理可以在此時建立起重要且獨立的規則。

第四層、資訊科技的使用，已經對一些倫理議題產生永久性的改變，因此需

要對其單獨加以研究。

第五層、資訊科技的使用，持續的創造了新的倫理議題，需要對這方面特別地研究。

第六層、新產生的以及改變的議題已經擴大到足夠定義一個新的領域。

據此，我們可以發現，傳統的倫理在探討人際之間行為的適切性，讓人可以分辨善惡對錯，然而時代的轉變，資訊社會不僅對傳統社會產生衝擊，傳統的道德觀也被迫面臨許多挑戰，因此探討資訊倫理的重要性，便成為當前社會中不可或缺的要務之一；此外，即使我們探討資訊倫理已經經過很長的一段時間了，但是很多領域仍有待釐清，因為社會大眾並沒有一個完整一致清晰的概念；資訊科技的發展，也會使資訊倫理的概念不斷的衍化。

（二）資訊倫理的內涵

Mason（1986）將資訊倫理分為分為四大議題，分別為隱私權（privacy）、正確性(accuracy)、所有權(property)與使用權(accessibility)，簡稱「PAPA」；以下分述之：

1.隱私權：規範個人擁有隱私的權力或防止侵犯他人之隱私。

2.正確性:是指要擁有正確資訊的權力,並有責任或義務對錯誤的訊息加以修正。

3.所有權：幾乎是今日社會上對最複雜的問題，包含了經濟與倫理議題等面向，由於資訊的總類繁多，因此所有權是指有關享有資訊或軟體製造者之所有權。

4.使用權：指維護個人對資訊存取的權力，而不限於特定人士或團體。

Mason 在十多年前對資訊倫理所提出的四大議題，目前都成為了資訊社會中相當關注且重視的課題，可見對資訊時代所可能產生的問題，他具有相當洞燭機先的觀察力。

榮泰森（2002）表示，資訊時代，由於開創了社會改變的機會，並威脅到既

有的權力、金錢、權力及義務的分配，因此資訊的使用，除了必須遵守法律的規定之外，尚需借助倫理道德的規範，以提供使用者一個遵循的方向，他認為涉及資訊倫理的五個議題分別為資訊權、財產權、責任與義務、系統品質以及生活品質等。以下分別陳述之：

1. 資訊權：是指個人在社會中所擁有的隱私與自由權，目前數以百萬計的員工受到電子或其他高科技形式的監督，個人隱私權正受到資訊科技的威脅。
2. 財產權：指智慧財產權如何受到保護；尤其是網路軟體的複製，正對既有的智慧財產權制度提出嚴格的挑戰，引發倫理、社會與政治議題。
3. 義務與責任：新資訊科技對責任法與社會慣例也產生挑戰，例如色情等不當資訊的傳布，該由誰來負起責任？
4. 系統品質：指資料品質與系統錯誤到達一個可接受的程度水準，只是到目前為止，軟體產業似乎還沒訂出一個標準。
5. 生活品質：隨著資訊能力的提升，資訊科技所帶來的負面影響有逐漸增加的趨勢，例如健康、工作、家庭或電腦犯罪等。

由此我們可以理解，資訊倫理最簡單的定義，其實就是藉由另一種角度來探討原有倫理關係中所產生的改變或新的議題，倫理的本質並不具備法律的強制性，然而卻是對人類社會的一種道德規範；在本研究中所探討的倫理議題，將涵蓋電腦、網路以及所有與資訊相關的範圍。

（三）小結

綜觀上述的討論，其實資訊倫理就是所有與提供資訊、使用資訊、受到資訊影響的相關問題。而這些問題是資訊科技普及化、應用範疇擴大與複雜性提高後所衍生的結果。資訊時代大量的科技使用，我們的生活也將因應這樣的改變而有所變化，本研究者以為，科技進步的腳步是相當快速的，連帶地，社會不斷的產生舊秩序重組的情形，同時發展出許多需要重新整合與規範的新問題，例如對於

資訊不當使用，網路駭客入侵與病毒的製造，以及網路上不實謠言的散播等等，面對社會如此快速的轉變，法律對於網路秩序的規範尚有不足之處；因此，部份秩序須依靠使用者本身的倫理道德來維持，因此其自身的態度及行為就益發顯得重要。

根據以上的探討，我們可以發現，「資訊素養」，通常探討的是如何以及為何搜尋資訊，也就是偏重技巧的取向，後來慢慢加入了有關倫理、法律以及禮節等議題；而資訊倫理所討論的範圍，不外乎電腦病毒、禮節甚至使用電腦對環境的潛在衝擊；例如 Gilber（2000）認為，除了教導學生資訊科技的使用技巧之餘，也應該教導他們可能遭遇的道德議題，以免造成使用上的無知；據此可得知，資訊素養與倫理的內涵有一部分是共通的，然而面臨資訊社會不斷產生的各種新興議題，過去資訊素養或資訊倫理所探討的議題，已顯得龐雜而無法涵蓋所有層面，值得進一步探討。

三、資訊安全

因應資訊社會的轉變，塑造出資訊素養的新意涵，成為可以受用一生且解決問題的能力，然而資訊行為的增加，新的威脅也接踵而來，使得多數人對安全的需求驟增，資訊安全的理念遂應運而生。

根據莊道明（1998）對台灣學術網路使用的調查結果顯示，不論是網路使用者或網路教學人員，在二十項的資訊網路議題當中的重要性，個人電腦資料的保護以及個人隱私等問題是最為人所關注以及重視的；本研究者將資訊安全由資訊素養與資訊倫理的範圍中提出，三者的關係如圖 2-1-1 所示。本研究者以為，資訊安全有一部份牽涉到資訊素養，另外一部份也與資訊倫理有關，兩者之間可能有交集，但也有各屬於自身的範圍。雖然在教育上，無法事先覺察學生所可能遭遇到的問題，然而當前的重要課題，應該是要教導他們如何維護自身的安全，並避免在電腦網路上遭受到來自各方的襲擾。

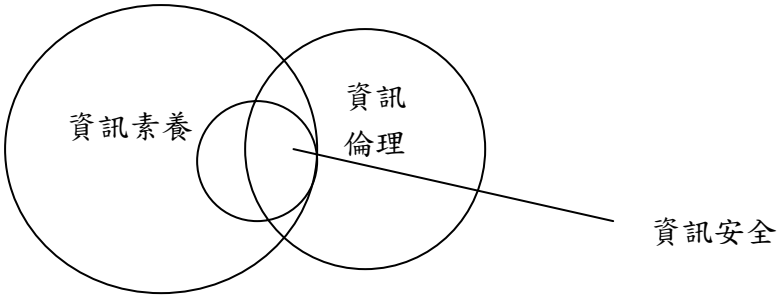


圖　2-1-1 資訊安全與資訊素養、資訊倫理的關係圖

安全向來是生活中重要的概念，但要對它下一個正確而完整的定義，恐怕也非三言兩語可以輕易帶過。自小我們就會被耳提面命地教導有關安全的觀念，小心也許可以避免一次意外事故，但並不能保證能避免所有意外事件，這充分說明生命的不安全性，亦即是生命本身是具有危險性的。也許就是因為生命充滿著不安全，追求安全乃成為人類的基本需要。著名心理學家馬斯洛（Maslow）在一九六九年，發表了一篇名為「Z 理論」（Theory Z）的文章，將過去所發表的需求層次重新詮釋，分為三個次理論，即「X 理論」、「Y 理論」以及「Z 理論」，並將人類的多種需求由高而低分為生理需求、安全需求（X 理論）、隸屬與愛的需求、自尊需求、知的需求、自我實現需求（Y 理論）以及最高層次的超越靈性需求（Z 理論），當中除了最底層的生理需求外，安全的需求（safety need），係指需要受保護與免於遭威脅從而獲得安全感的需求，則排在第二階層，安全對人類的重要性可見一般（李安德，1992；張春興，1996）。

由此說來，安全就是沒有讓我們感到危險的突發事故的發生，資訊社會為生活帶來許多的便利性，然而卻也因此產生許多問題，資訊科技有其光明面，但黑暗面也隨之而來；網路或資訊安全，便是近來日益嚴重且為人重視的問題之一。而我們所提到的資訊安全，由於個人的認定標準不同，因時而異，都有不同的陳述，根本的做法就是，我們應該要建立一個社會多數人認可的資訊安全標準。

（一）資訊安全的意義

對資訊安全最簡要的定義不外是利用各種方法或工具來保護靜態或動態的

資訊。也就是說，多數探討有關資訊安全的議題，大部分都集中在電腦系統或網路通訊上的保全與資料的完整性；例如林詠章與黃明祥（2000）認為，資訊安全可以分為電腦安全(computer security)及通訊安全(communication security)兩種，前者包括了所有電腦系統上的防護措施，後者則泛指資訊在公開的網路上傳送所需的安全防護。

而吳賢明（2000）表示，資訊安全至少應該要包含三點，分別為：

1. 資料的完整性(Integrity)：能夠確保儲存於該系統的任何資料不被竄改或破壞，資料的完整性遭損壞，便屬於一種破壞性的入侵；在網路環境下，可能遭受不當竄改或破壞的如使用者的帳號及密碼、系統設定與使用者資料等。
2. 私密性(Privacy)：電子式的資料很容易遭人複製，因此這類的入侵不太容易被察覺，不過作為一個安全的電腦系統，應該要能確保儲存於其中的任何資料及透過該系統傳輸的資料不被竊取。
3. 系統可用性（Availability)：就是隨時隨地都可以讓系統維持正常的服務。

上述主要著眼在對資料的安全以及系統的穩定可靠性，同時也包含了資料在傳輸、儲存方面所應考量的重點。另外，劉國昌與劉國興（2000）也認為，資訊安全的保護範圍包括：機房、電腦主機、終端機、電腦網路、軟體與資料等有形及無形的電腦相關事務，而良好的安全措施維護了這些資源的機密性、正確性以及可用性。

蔡敦仁（2002）則表示，資訊安全是保護資訊資產的一種概念、技術及管理方法，使資訊資產免受有意或無意地洩漏、破壞、遺失、假造，及未經授權之獲取、使用和修改。

由此可知，對於資訊安全的定義大多跳脫不出機密、完整與有效性，或者有人把資訊安全認為是對實體以及抽象資料的存取，預防各種未經授權的竄改或窺視的行為，然而這樣的概念通常是模糊不清而且沒有一定的規準，雖然它們都認為資訊安全的範圍很廣，並圍繞著不慎的活動，所顧及的不僅是部份的電腦或資

訊安全，而是一種整體的安全機制與人員所應具備的態度（Anderson, 2003）。然而一般較重視資訊安全的，不外乎商業團體、國防機構等，因為它們的資料一向具有商業機密或有關國家安全等級的特性，因此對於資訊安全有所鑽研的，多數為工程師、系統發展者等相關資訊專業人員，但是近來資訊安全的相關議題不斷的衍生擴大，資訊安全已經不單純是電腦技術上的問題。

其實，資訊安全有很大的部分是和人的管理有關的，因此也最為複雜，需要各個不同層面的專家參與。近年來隨著網路的普及，衍生了許多電腦犯罪的問題，不是正在醞釀當中，就是已發生在你我週遭，所以面對接踵而來的資訊安全問題，研究資訊此類的議題勢必不斷的在調整與擴充（李忠憲，2001）。

（二）資訊安全的內涵

安全就是使自身免於受到威脅或傷害，因此凡涉及與資訊有關的安全防護或傷害，都可以羅列在資訊安全之內涵中；一般使用者常遇到的安全問題大致可分為作業系統與應用程式的漏洞、木馬及後門程式、網路的監聽以及不當的使用習慣，如帳號密碼的管理不當與任意安裝來歷不明的程式等（李維倫，2003）。李忠憲（2001）表示，校園網路有關的安全問題包括學校的行政系統缺乏資訊安全的應變與規劃能力、病毒肆虐、同時對於不當的資訊氾濫並未加以管制，以及資訊流通地下化和網路犯罪問題等。

另外在探討資訊安全的種類中，大致可以分為軟硬體安全、網路及通訊安全、資料安全、個人安全等，除此之外，與個人安全有密切關係的健康議題，也是相關的內容（蔡敦仁，2002）。

由前述的資訊安全，我們可以發現取向的不同，會對資訊安全有不同的概念，此外如許怡安（2001）在探討網路素養課程的內涵中，將課程中的安全防護包含了個人資料（如個人分份資料的洩漏）、人身安全（如網路交友安全）、電腦保護（如防毒的預防工作）以及個人電腦及帳戶保護（如設定密碼）等。

據此，本研究者以為，資訊安全至少可以從幾種不同的面向來加以探討：

1. 電腦網路通訊安全（例如駭客入侵、病毒、以及相關的安全機制等），衍生出許多資訊犯罪問題，同時隨著社會的轉型不斷擴張，學校成為散佈的溫床。
2. 資訊的正確、合宜與私密性（如網路上散播的不實謠言、垃圾信件以及有關在網路上的個人隱私等議題）。
3. 防護個人安全，如正確使用電腦設備以確保身體健康的概念。

近年來，我國推動資訊教育計畫方面，不但培養學生資訊擷取、應用與分析的能力，同時也要求學生具備適應生活並善用科技的認知，例如教育部在九年一貫課程的資訊教育領域中，羅列了五項學生在資訊教育的課程當中所應具備的核心能力，分別為「資訊科技概念的認知」、「資訊科技的使用」、「資料的處理與分析」、「網際網路的認識與應用」以及「資訊科技與人文素養的統整」(教育部，2003)。

表 2-1-1 中，有關資訊教育相關學習內涵指標，我們可以發現在「資訊科技的概念認知」裡，電腦使用安全包括了維護身體健康以及教導學生注意軟硬體的保養、備份資料等概念，都羅列在其中，教學階段則擺在第二階段，即國小三、四年級中；而在「資訊科技與人文素養的統整」能力中，遵守網路應有的道德規範以及懂得保護自身等能力指標，則散落在二、三階段，也就是國小三年級到六年級間，但是並沒有一個概括的資訊安全課程。

表 2-1-1 九年一貫課程資訊教育分段能力指標

核心能力	學習目標	學習內涵	學生完成左列核心能力學習內涵後具備之資訊能力
1、資訊科技概念的認知	了解資訊科技在生活與學習上的應用、以及對人類社會生活的影響。	電腦與生活	了解資訊科技在人類生活之應用。
		電腦使用安全（一）	正確規劃使用電腦時間及與電腦螢幕安全距離等，以維護身體健康。
		電腦使用安全（二）	教導學生注意軟硬體的保養、備份資料等資訊安全概念。

5、資訊科技與人文素養的統整	應用資訊科技提升人文關懷、促進團隊和諧。	資訊倫理（一）	認識網路規範，了解網路虛擬特性，並懂得保護自己。
		資訊倫理（二）	了解與實踐資訊倫理，遵守網路上應有的道德與禮儀。
		資訊相關法律（一）	認識網路智慧財產權權相關法律，不侵犯智財權。
		資訊相關法律（二）	認識網路隱私權相關法律，保護個人及他人隱私。
		網路世界正負面的影響	善用網路分享學習資源與心得。了解過度使用電腦遊戲、bbs、網路交友對身心的影響；辨識網路世界的虛擬與真實，避免網路沉迷。
		認識網路犯罪	了解網路犯罪型態，避免誤觸法網及受害。
		正確使用網路的態度	適時應用資訊科技，透過網路培養合作學習、主動學習的能力。

資料來源：國民中小學九年一貫課程綱要-重大議題（頁 20），教育部，2003，台北：教育部。

由以上的討論，相信對資訊安全應具備的內涵有所瞭解，同時也可發現在現有的資訊課程規劃中，資訊安全已經列為課程中不可或缺的內容；因此，本研究的主要目的，是使學生在當前電腦網路發達的資訊社會中，能夠瞭解本研究所探討的資訊安全內容，從而加以防治，改善日益嚴重的安全問題；此外，諸如網路交友或色情氾濫等與人際所產生的問題以及有關法律的認知，由於所牽涉的層面甚廣，因此不在本研究的討論範圍內。以下三節所探討的議題，將作為資訊安全課程發展之基本內容。

第二節　電腦網路通訊安全

電腦網路是一個開放式的環境，任何人都可以在這環境中搜尋或瀏覽甚至存取資料，也因此容易受到一些有心人士製造的程式干擾或影響使通訊中斷

（Spinello, 2003），不僅日常的工作停擺甚至連資料都有遭受洩漏或竄改的可能，從而衍伸出種種的問題。一般來說，最常為人所熟悉的就是有關駭客（hacker）與病毒（virus）的訊息；此外，電子商務的發達，使得從事網路交易的安全性也逐漸為人所重視，因此，本節首先要介紹的主題為電腦網路通訊安全，其中包含了三個子議題，分別為一、駭客；二、電腦病毒；以及三、電子資料與網路通訊安全。

一、駭客的定義

（一）何謂駭客？

「駭客」一詞源自英文 hacker，過去提到駭客，總不免令人聯想到入侵網站、破壞他人電腦的人，甚至將他們歸類為恐怖份子，多數媒體對駭客的報導也顯露出恐懼、不確定以及猜疑的特性，然而到底 hacker 所指為何，卻很少有人可以提供正確的知識（Richard, 2001）。

根據 Levy（1985）的說法，最早的駭客是一群在麻省理工學院（MIT）的學生，他們主要的興趣是在了解電腦系統內部的運作，所寫的程式可以開放分享給一般大眾使用，同時也尋求更進一步的交流與發展（引自 Hester et al., 2001）；根據駭客們透過網路共同編纂的「行話檔」（jargon file），駭客被定義為「一群高度熱中於寫程式的人」，他們「相信資訊的共享是一種力量強大的美德，並且認為，盡可能藉由撰寫自由軟體（free ware），以及促進資訊及電腦資源的自由流通，以將他們的專業分享給其他人，這是他們的道德義務。」（頁 9）這就是所謂的「駭客倫理」（hacker ethic）（Himanen, 2001）。然而因為時代的遷移，過去主張駭客所應具備的倫理價值觀已經逐漸受到挑戰，並顯得不合時宜了（Duncan, 1995）；今日所謂的駭客，大抵都帶著負面的意涵，用來指那些使用電腦從事不法行為，特別是未經許可擅入電腦系統並竊取軟體的人（Johnson, 2001）。

對駭客的種類，許多人有不同的見解，如 Richard（2001）認為，駭客可以

由其入侵的手法的深淺分為三類，分別為最粗淺的年輕小夥子（script kiddies），他們可以做到下載適合的軟體來進行簡單的入侵行為，至於第二類的駭客（hacker），則是指了解網路運作的原理以及網路的通訊協定，甚至懂得運用最適當的工具從事入侵的工作，第三種破網客（cracker），則是用來形容一種利用網路從事對人或機關團體的破壞行為，並有著超乎一般人的入侵技巧的駭客；至於 hacker 跟 cracker 的分別，即使他們對於電腦網路或系統的知識幾乎不相上下，但是分界在 cracker 已經具有惡意或犯罪的動機了，而 hacker 大多只是出於好奇心。因此有人表示應該要將 hacker 跟 cracker 作一區別，並保留 hacker 原來當初具有較正面的意義，而將 cracker 視為從事不法入侵行為的人，然而這樣的區別並不為大家所接受，目前最為人所熟知或一般報章雜誌電視媒體所刊載，仍將 hacker 認為是那些經常非法入侵並造成破壞的人（Johnson, 2001）。

宋振華、楊子翔、樊國楨（2001）主張，駭客如果依其技術能力來分類，可以分為以下四種：

1. 業餘的玩家：多半是對網路技術有興趣的人，他們覺得入侵只是用來證明自己的技術能力，但通常不懂得如何善後，所造成的傷害通常是無心之過。
2. 專業的入侵者：他們將入侵當成事業，有能力成為一流的資訊安全專家，甚至其本身的工作就是資訊安全工程師。
3. 玩票性質的電腦高手：可能是相當聰明的學生或熟練的電腦工程師，對於電腦的運作相當熟悉，但對入侵不感興趣，有時只是懶得循正常管道申請系統使用權限，其實他們對系統的破壞性不高。
4. hacker 級的 cracker：也許我們所使用的作業系統就是由他所開發的，不過這種人應該在少數。

根據前述，本研究者以為，關於駭客，許多人對其行為或類別有不同的認定，不論是 hacker 或 cracker 或者是其他的稱謂，甚至有不同的技巧或等級之分，但是在本研究中，為撰寫適合中學生的相關內容，本研究者以為可以將其歸結

為，凡是從事電腦資訊網路系統等入侵行為的人，不論其是否涉及破壞或竊取的行為，都可以稱之為駭客（hacker）。

（二）駭客入侵的動機與目的

關於駭客入侵的動機，據宋振華、楊子翔、樊國楨（2001）表示，不同的入侵目的會對系統有不同程度的影響，主要可以分為：

1. 好奇心與成就感：對這些人而言，沒有特定的目的，入侵可以為他們本身帶來成就感就是他們心中的目的。
2. 當作入侵其他機器的跳板：入侵者會選擇安全防護較差的系統作為侵入的前哨，以迴避牽涉到自己本身的責任。
3. 盜用系統資源：例如免費的帳號或者盜用系統上的軟體，形同具有一大筆的財富。
4. 盜取機密資料：由於對網路的依賴日深，許多重要資料是散佈在網際網路中，對於許多人來說，這些機密資料是相當具有價值的。
5. 惡意攻擊：有許多可能的原因，例如因為政治立場的差異而進行入侵或者相同企業間的競爭而癱瘓對方的資訊系統等。

另外 Hester 與 Ford（2001）也指出，駭客進行入侵的原因不外乎賣弄小聰明，就像猜測密碼或者製造某些陰謀的陷阱等，甚至進行某種的報復行為，可能是由於不滿前任雇主的行為。從心理學家的角度來看，也有可能是因為那些人把電腦當作是人類的替代品，因為電腦不需要與其產生互動，甚至不必考慮到複雜的人際社會關係，例如社會上的地位、肢體語言等，如此一來，人們在群體中許多決定的方式也因此產生轉變。

而 Richard（2001）認為駭客依其入侵動機，主要可以分為七種：

1. 出於好奇心（Curiosity）：純粹是為了追求挑戰，藉由入侵的過程，來獲得本身的成就感，並不會產生很大的破壞行為。

2. 故意破壞（Vandalism）：採用的方法或工具，有時讓人摸不清楚他們到底是入侵者還是受害人。
3. 入侵（Hacktivism）：可能是由於生態、政治上或某種倫理原因進行入侵，造成破壞的行為。
4. 工業間諜（Industrial Espionage）：例如企業間竊取商業機密，通常會花費一段時間來進行，同時也會開啟系統上的後門，隨時可以自由進出。
5. 勒索和詐騙（Extortion and Fraud）：涉及到有組織的犯罪集團，他們主要的目的就是金錢。
6. 資訊戰爭（Information Warfare）：例如在政府間的衝突或者政治社群間的交戰，彼此都嘗試去癱瘓對方的基礎設施。
7. 白帽子（White hats）：是指有倫理的駭客們，他們入侵只是為了告知該團體或組織系統上的漏洞，並提供建議，同時也協助警察單位將不法的駭客繩之以法。

根據以上所述，我們可以發現，駭客入侵的動機有許多，而且不同的人也會產生不同的看法，本研究者認為可以粗略的將其歸納為三種，分別為：

1. 好奇心的駭客：只是為了滿足自己對他人相關資訊的好奇心。
2. 耍小聰明的駭客：為了證明自己的能力。
3. 有目的性質的（不論好或壞）駭客：包括報復或為了自己與他人的便利性甚至為了利益入侵，但也有人是為了找出系統的安全漏洞而入侵。

值得注意的是，即使在此所談的都是駭客的入侵動機，但並非所有駭客的入侵行為都是不好的具有破壞性的，有些人只是為了滿足自己的好奇心，才會鋌而走險，甚至有些人是為了測試系統的安全性，避免讓有心份子有機可趁，釀成更鉅大的傷害或損失，這些都可以讓人重新省思駭客的意涵。

（三）駭客行為的合理性

雖然未經授權而入侵他人系統是不法甚至是犯罪的行為，但是根據前述的文獻，不論是從駭客的定義或是其入侵的動機來看，產生了許多的爭議。有些人認為這種侵入他人電腦系統的行為根本無足輕重，因為這樣的行為相對於實體上的入侵（如小偷入侵房舍）是很抽象的，而一些正在學習入侵的人也表示，他們沒有從事任何破壞活動或者改變任何的東西，純粹只是學習有關電腦系統的運作方式，照這種邏輯說來，沒有得到授權而闖入電腦系統的行為根本就不值得大驚小怪的（Spinello, 2003）。此外，某些入侵行為是為了測試系統的安全性，例如在美國一些過去曾經擔任駭客的人，經常聚集在一起為一些組織提供安全上的建議，以建立起更完善的安全防護網（Hester & Ford, 2001）。有些人甚至認為，某些駭客的行為是為了避免政府的專制，隱瞞大眾知的權利，藉由侵入可以警告大眾某些濫權行為的發生（Johnson, 2001）。

另一方面，許多人認為駭客的行為是不可原諒的，例如網絡安全公司 Network Flight Recorder 的首席執行者 Marcus Ranum 認為，闖入他人的電腦系統意味著受害者經受「絕對的精神和情感痛苦」，品格高尚的駭客道德規範忽視了最善意的入侵也會給人們造成極大痛苦的現實（引自李建平，2003）。Ranum 認為，假如有一位在華爾街工作的系統或網絡管理員的系統遭受駭客的入侵，他會為自己的工作擔心，害怕失去工作，無法支應自己的生活。此外，法律專家認為入侵電腦系統應當是違法行為，這與未經許可穿越住宅不合法是一樣的道理。一般來說，真實世界中的非法闖入罪會予以緩刑，而入室行竊應當更嚴肅地處理，這同樣適用於網絡犯罪（引自李建平，2003）。

探討入侵行為是否正當的爭議，正反雙方似乎永遠堅持不下；由道德的觀點來看，即使所指的入侵只是擅自進入他人的電腦系統，並沒有造成直接的破壞，但這樣的行為已經違反個人隱私，而隱私通常被視為一項重要的倫理以及社會價值；Spinello（2003）認為也許我們對於駭客的行為沒有一定的處理原則，但是未經他人同意就擅自進入他人系統，是一個基本的道德原則。此外，就商業的角

度而言，並非所有的資訊都是免費的，因為蒐集及整理資訊也需要花費相當大的力氣，對那些主張資訊應該是公開並且自由流通的人而言，非法入侵並取得未經授權的相關資訊的人，無疑是做了不勞而獲的負面示範(Hester & Ford, 2001)。再者，對於主張駭客的入侵是為了避免專制政府的產生的這種說法，也備受爭議因為就民主國家來說，法律已經設置了相關的機構對政府加以監督，並不需要藉由入侵的行為來防治寡頭政府的專擅（Johnson, 2001)。

綜括上述，對於駭客的行為，從最初形成的歷史到入侵的動機以及行為的產生等，也許在法律上並沒有明確的規範或是相對應的政策，然而從道德層面來說，入侵行為的發生，就如同走在街上閒晃，並挨家挨戶的試著去開啟他人門戶一樣，這種行為或動機是不見容於現今社會。從教育的角度來說，教育者往往肩負著培養國家社會未來公民最基本的責任，一方面不僅要教導學生有關行為的正確性與合法性，同時也要針對那些遊走在法律邊緣的行為予以明確的規範，即使在行為上不違法，不代表其合理性或可為他人接受，因為法律通常代表的是道德的最低標準。

二、電腦病毒的傳播

2003 年八月份，名為疾風（BLASTER）的電腦病毒，讓許多人的電腦一開機不久又關機，情況一再重複，重要的工作都因此中斷，使得許多公司面臨業務停擺，造成企業界不小的損失；電腦病毒一向讓人聞之色變，同時也是電腦使用者心中永遠的夢魘，因此有效的防治工作是相當重要的。

（一）電腦病毒的起源

病毒（Virus）通常指在生物或醫學上可以使人體致病並導致傳染的一種微小病菌，在電腦網路的世界中，其實有個與生物病毒相近的特性，可以不斷的繁衍複製，並對電腦系統造成破壞的電腦程式，大家稱之為「電腦病毒」(Computer virus)；有關電腦病毒的命名，其實會影響大眾對該程式製造者的想法以及預防和處罰的觀念，一些學者也發現使用這種生物學上的隱喻可以有效的防堵並降低

電腦病毒的感染（Andy & Geraldine, 2000）。

Hester 與 Ford（2001）表示，電腦病毒是一種可以自我複製並造成破壞的程式，通常是指刪除硬碟或造成檔案的損毀，同時也藉著複製的動作來感染其他程式；電腦防毒軟體公司「趨勢科技」(Trend Micro）的解釋，電腦病毒是會將本身複製到其他乾淨的檔案或開機區的惡性程式，使用者在不自覺的情形下執行到已受病毒感染的檔案時，該程式就會以相同方式繼續向外散播出去（陳清芳，2002），同樣是電腦防毒軟體公司的賽門鐵克（Symantec）認為，電腦病毒是一種藉由重新寫入檔案或是將本身的副本插入或附加到檔案以感染系統的程式；由此可知對於電腦病毒的解釋，其實就是一種可以對資訊系統產生影響甚至破壞，且不斷的自我產生複製的惡性程式。

最早且正式使用電腦病毒這名詞的人，是由 Fred Cohen 在 1983 年，執行一項學術實驗時所提出的，他清楚定義電腦病毒為「任何可以修改其他程式使其能嵌入的軟體」(any software which can modify other programs to include a version of itself)（引自 Dwan, 2000）。而電腦病毒的前身，稱為蠕蟲（Warm），在 1980 年代初期，由 John Schoch 和 Jon Hupp 修改一支程式，可以藉由機器間散佈出去，它幾乎是完全無害的，只有在晚上網路擁塞時才會被釋放出來，佔住那些沒有用到的電腦並利用他們的資源與頻寬，當時的蠕蟲不會造成電腦永久性的破壞（Hester & Ford, 2001）。然而現今的蠕蟲本身，已含有特殊破壞目的的程式碼，開啟或執行後，會對作業系統造成破壞，或對正常作業造成干擾，蠕蟲與病毒最大的不同就是牠能獨立繁殖，例如 ILOVEYOU 這種蠕蟲就是透過電子郵件將本身自動傳送到收件者通訊錄上的每個人（Symmantec, n. d.）。

電腦病毒的發展有很長的一段醞釀期，一般以電腦為主的系統都是考量其重製性並可以透過單一機器或網路來散佈，第一個相容於 IBM/PC 的電腦病毒 Brain virus 出現在 1986 年，是一個可以常駐在開機磁區的開機型病毒，這支病毒沒多久經過一些人的修改後，專門感染一些副檔名為.COM 或.EXE 的檔案，同時很難被偵測到（Dwan, 2000）。然而時至今日，網際網路潮流席捲全球以來，電腦

病毒透過傳統一對一的感染方式慢慢的減少；相對的，利用連鎖信、惡作劇程式、免費優待卷等方式，誘騙使用者下載並執行程式的手法相繼出現，使得電腦病毒的傳播進入到多重感染的境界。因此，電腦病毒不再只是侷限在電腦病毒狹義的定義裡，而是應該從惡意軟體這個廣義的角度來檢視電腦的病毒現象（林修遠，2003）。

（二）電腦病毒的種類

據賽門鐵克公司表示，目前的電腦病毒至少有 53,000 種，多數的感染方式不外乎透過電子郵件附加檔案，磁片上的檔案，以及任何可以附加檔案的媒體(如光碟)，附著或隱藏在某些特定型態的檔案上，進入作業系統的開機磁區，或利用文書處理軟體的特定程式碼（一般稱之為巨集）快速感染重要文件，藉以達到快速破壞干擾正常作業的目的。依據以上特性，病毒大略可區分成檔案型、開機型、巨集型病毒等三大類，除此之外，某些病毒會結合上述型式的特性出現，這種型式的病毒，稱之為混合型病毒(Symantec, 1999)；趨勢科技(Trencend Micro)則將電腦病毒分為八類，以下分述之：

1. 開機型病毒（Boot strap sector virus）：藏匿在磁片或硬碟的第一個磁區，由於過去作業系統 DOS 的設計，使得病毒可以在每次開機時，在作業系統還沒載入前就先載入到記憶體中，進行破壞。
2. 檔案型病毒(File infector virus)：通常感染一些執行檔，例如副檔名為.com 或.exe，當其被執行時，病毒的程式也隨之執行。
3. 複合型病毒（Multi-partite virus）：兼具前兩種病毒的特性，具有相當傳染力，且破壞力十足。
4. 隱形飛機式病毒（Stealth virus）：又稱中斷擷取者（interrupt interceptors），藉由控制 DOS 的中斷向量，把所有受感染的檔案還原，亦即可以將受感染的病毒喬裝起來，讓使用者不易察覺。
5. 千面人病毒(Polymorphic/Mutation virus)：由於該種病毒每經過繁殖一次，

就會以不同的病毒碼出現，所以不易偵測。

6. 巨集病毒（Macro virus）：主要是利用軟體本身有提供巨集能力的特性來進行設計病毒，因此如微軟的 word、excel 具有巨集的功能，因此也都有可能是病毒存在的地方。

7. 特洛伊木馬病毒（Trojan）與電腦蠕蟲（Worm）：前者是指可以將自己喬裝成某種應用程式來吸引使用者下載或執行，進而破壞電腦資料或竊取重要訊息的程式，然而它並不會像傳統電腦病毒一樣感染其他檔案；至於後者指的是某些惡性程式碼像蠕蟲一樣在電腦網路中爬行，從一台電腦爬到另一台。

8. 駭客型病毒：是指夾帶後門程式的病毒，利用該程式的運作，駭客可以遠端遙控該程式記錄相關的動作或將資訊傳回駭客手中，導致機密外洩；2001 年七月一支名為紅色警戒（CodeRed）的病毒利用微軟網路伺服器（IIS）的漏洞，在網路上展開新的攻擊行為，造成全球 26.2 億美金的損失，不久之後，以同樣攻擊手段的娜坦（Nimda）病毒所造成的損失，卻遠超過紅警戒，可見此一形式的攻擊手法，已經是日後電腦病毒的趨勢。

雖然上述列出多達八種的電腦病毒，但是現今電腦病毒的成長速度之快，幾乎無法讓人正確地加以估算，多數甚至將現有的病毒稍加修改就成為新的病毒（Andy & Geraldine, 2000），然而面對日益精進的攻擊型態，以及電腦軟體本身的漏洞，相信日後有更多的電腦病毒類型繼續產生，例如病毒只針對某個特定使用者在某個特定的網路當中產生影響（Hester & Ford, 2001），而所侵襲的對象甚至包括手機、PDA 等高科技無線通訊工具；此外，網路專家也認為，CodeRed 已經成為電腦病毒、電腦蠕蟲和駭客三者兼備的開路先鋒，今後勢必會變本加厲的在網路上肆虐（陳清芳，2002）；由於我們生活中對網路的依賴漸深，因此可以預見的是，未來所面對的將是一個充滿病毒威脅與挑戰的資訊環境。

三、駭客與病毒的防治之道與相關研究

藉由前述的探討，可以了解今日的電腦網路世界裡，充斥著各種如電腦病毒般的惡意程式，也有到處翻人隱私的駭客，為日常的生活帶來許多的困擾，然而預防甚於治療，對駭客或電腦病毒的預防工作雖然相當費心且艱苦，但是置身於資訊與網路無所不在的知識經濟時代裡，我們應該藉由學習、了解而建立起相關的知識，才能為自己或他人甚至整個團體，提供有效的保障。以下分別探討相關問題的解決之道。

Cohen（1999）表示，資訊安全的複雜度不是可以輕易解釋清楚的，而目前教導有關資訊安全的課程並無法契合需求，尤其是這個領域變動得太快，因此他建議在課堂上可以提供學生實際的經驗，並透過與學生互動的方式來進行教學，如此將更能有效彌補在教育上的不足。

根據林珊如、劉旨峰、袁賢銘（2001）一項對技術學院資訊相關科系學生的研究，發現學生對於電腦病毒會產生五種的迷思概念：

（一）對電腦病毒概念模糊的迷思：例如錯把當機的原因歸為病毒所致。

（二）對電腦病毒感染軟硬體對象的迷思：也許是對電腦軟硬體設備知識的不足、作業經驗不夠產生的，這同時也是許多資訊新手的問題。

（三）把電腦病毒類比為生物性病毒的迷思：是由於病毒名稱的定名，使得學生產生語意雙關聯的迷思。

（四）對電腦病毒發作徵狀與周期的迷思：例如學生可能由於應用程式開啟過多，而導致系統的資源不足，但學生卻誤認是病毒的危害，這方面可能就是因為學生對於系統的相關知識仍欠缺。

（五）對電腦病毒傳染途徑的迷思：對電腦病毒無親身體驗，以及把電腦類比為家電用品而產生的。

據研究的結果顯示，擁有前四種迷思概念的學生比例從 78%~90%，居高不下，由此可見學校在課程的安排上，對電腦病毒的教學仍有其不足之處。

李維倫（2003）認為有關防範病毒的資訊安全，應該由使用者本身做起，對於使用者提出三點建議：

（一）注意隨時安裝修正程式：針對系統或應用軟體有安全漏洞的存在，常使駭客或病毒趁機入侵，因此使用者應該視需要更新或修補程式才能降低安全顧慮。

（二）加裝個人防火牆：個人防火牆是一種安裝在個人電腦上的程式，如同在電腦與網路之間築起一道防護牆，保護電腦降低被攻擊或植入程式的機會。

（三）建立正確的使用習慣：除了對密碼的設定避免過於簡單或容易猜測外，不要隨便安裝或執行來路不明的程式也是一個很重要的基本安全防護觀念，例如近來很多病毒是藉由電子郵件的附加執行檔來傳播。

蔡均璋(2002)認為企業中常見的資訊安全機制，除了架設網路防火牆之外，另外也包括了以下幾點：

（一）對病毒的防護：透過集中政策，例如制定病毒碼的更新週期、檢查出病毒時的處理流程等等，徹底實行到每個用戶端，將可有效控制病毒的擴散。

（二）安全掃描及評估機制：包括安裝市面上的安全評估軟體以及研聘專業的安全顧問廠商，由他們提供安全檢查服務。

（三）入侵偵測與網路監督：主要針對可疑的活動進行分析以及偵測，亦即分析每個發生事件底層所顯示的行為模式，並據此來判斷是否為入侵事件。

另外，根據香港政府的資訊安全署（2003）所公布的幾個處理資訊安全的原則，可以由幾點著手，分別為：

（一）提高本身的資訊保安意識：即從個人對資訊安全的認知上著力，時時有危機感。

（二）處理帳戶及密碼的原則：關於密碼的設定以及帳號的使用都應該要謹慎且小心。

（三）使用軟體需知：防護軟體的使用，以及讓軟體保持在最佳狀態。

（四）處理電子郵件需知：例如使用郵件過濾軟體過濾有害電子郵件。

（五）瀏覽網頁及網上購物需知：如不啟用瀏覽器的應用程式，避免受到惡意程式的侵害。

（六）個人處理原則：採取鎮定的應對原則，沉著地面對危機。

多數人感受到和資訊有關的恐懼來自兩個面向，一是使用者不了解所處的網路環境及所使用的作業系統等所提供的安全性；而另一個則是網路服務業者（ISP）無法提供一個免於威脅的環境，可將病毒、駭客或垃圾信件阻擋在外；另外，當前法律的制定常常無法跟上時代演進的步伐，因此即使有相關法令，也大多不夠周詳。

本研究者綜合前述文獻的探討，認為預防駭客以及電腦病毒的威脅，應該由下而上的教育民眾建構起完善的資訊安全網，從個人做起，再逐漸擴展範圍至團體甚至社會大眾，同時在技術上的防護加以改善，相信可以有不錯的成效。

（一）教育層面的防護

1. 加強對資訊安全的認知：指對基礎的資訊安全認知的建立：從平日使用電腦的習慣著手，例如電子郵件、瀏覽器的使用，以及帳號密碼的設定等，同時摒除苟且及輕忽的心態。
2. 對於駭客與電腦病毒製造者的動機加以深入研究：事出必有因，往往我們太專注於防護工作的進行，反而忽略了對事情的發生探求根本的原因。
3. 法治道德觀念的培養：雖然法令修訂的速度常跟不上時代的腳步，然而生活中道德觀念應是基礎課程，例如入侵系統或製造電腦病毒即使可以巧妙規避法律的制裁，但在道德層面上仍是不被允許的行為。
4. 對電腦病毒與駭客的認識：例如傳統使用文字敘述的方式來介紹病毒，也可以利用電腦動畫呈現電腦病毒的造形，藉以吸引使用者了解電腦病毒的成因及病

毒行為，提升自己對電腦病毒的認識，以便及早採取合適的防禦措施，確保系統功能與資料安全（林修遠，2003）。

（二）技術層面的防護

1. 定期更新系統並關閉不必要的服務：指的即是隨時注意所使用軟體，如作業系統的原創公司所發布的各種更新程式，同時關閉不必要的服務與通訊埠。
2. 訂定更嚴謹的存取規則：導入各種存取機制，例如政府單位率續成立政府憑證管理中心（Government Certification Authority, GCA）、自然人憑證等管理中心，藉由憑證機制有效整合加強各項資訊的存取控制。
3. 加強上網電腦的自我防護：例如安裝個人防火牆軟體，或者透過 E-mail 病毒掃描、垃圾信件以及定時的備份資料等來降低網路上的威脅。

本研究者認為，過去我們對於駭客與電腦病毒的資訊不足，因此往往在多次的破壞行為發生後，才逐漸累積起相關的經驗；或許在駭客以及電腦病毒的肆虐之下，任何人都無法提供最完善的防護機制，然而，在歷經許多的教訓之後，我們已經可以慢慢的歸納出一些行為模式，個人可以事先預防且加以控制，因此只要能確實的由個人以及整體環境的配合，並在教育到技術面都兼顧，相信可以將電腦病毒帶來的災害減至最低。

四、電子資料與網路通訊的安全

網路的發達，帶動了傳統產業的另一個新契機，在我們享受電子化、數位化所帶來的便利性同時，對網路傳輸安全性的評估也是不可或缺的一環，例如日前傳出某銀行信用卡資料遭外洩，造成許多消費者的恐慌與困擾，該銀行於是立即關閉線上申辦業務（孫中英，2003）。此舉也使得對網路依賴日深的公司行號、機關團體乃至於個人，曝露出許多可能的危機；網路是一個公共的場域，任何人都可以從網路中間攔截或修改資訊，而電子檔案以數位的方式儲存，使得檔案的

複製、偽造及竄改變得更加容易，因此電子資料與網路的安全性就顯得特別的重要。以下先簡述電子檔案的安全管理，繼而討論較為常見的網路安全機制。

（一）電子檔案的安全管理

網路熱潮的漫延，使得數位化資料或資料的數位化頓時間蔚為風尚，但是在安全性上也面臨許多的考驗，例如資料內容被竊、偽造或遭到竄改，甚至網站遭駭客入侵，此外，電子公文的傳遞上，也產生了「發送者否認傳送」或「接受者否認接收」，以及被人冒名發文的疑慮；李正吉、林詠章、黃明祥（2002）就認為，一個安全的檔案認證系統除了要有安全的儲存以及傳輸機制外，檔案來源的合法性以及檔案內容的完整性也是必須具備的。

近年來，以密碼學（Cryptography）為基礎的安全技術，可為上述的安全困擾，提供相當程度的安全保障。當前許多國家推動如「資料加密」、「數位簽章」等「公開金鑰基礎建設」(Public Key Infrastructure, PKI)，將可確保資訊在網路作業中不容易受到偽造、竄改或竊取，且能鑑別交易雙方的身分，同時防止事後否認已完成的交易事實，是目前最重要也最為信賴的安全管理機制（盧鄂生、吳啟文，2001)。

目前PKI主要可以衍生出三種的應用，分別為：

1. 強化身分驗證(Enhanced Authentication)：傳統上一般的身分均為利用使用者的帳號名稱與密碼，雖然簡單易用，卻也容易遭人偽冒，採用數位憑證的機制，可以某種程度上解決這種問題。由於數位憑證均為憑證中心所發出，不易遭人偽造，比帳號名稱與密碼的方式更安全，可應用在如網路銀行、網路股票下單以及網路報稅等。
2. 加密(Encryption)：PKI的基本原理，是利用一雙成對的「金鑰編碼」，一支金鑰所編碼過的資料只有另一支可解碼，因此即使其他的使用者接收到同樣的資料，在缺乏金鑰的情況下是無法進行解碼的動作以讀取資訊。
3. 數位簽章(Digital Signatrue)：由於該對金鑰的產生是根據使用者的資料及

產生的時間，採亂數的方式形成，不會重複出現；公開金鑰會在經過憑證管理中心的認證後公布，但是私密金鑰則由使用者保管不會散布在外，因此利用私密金鑰獨一無二的特性，在文件上加以私密金鑰經過雜湊（Hash）方式處理過而產生的數位簽章，就可作為印鑑或簽名的功能（陳長榮、崔友經，2002）。

我國在推動電子化政府時，即將資訊安全管理措施列為重點，並於八十七年二月建置政府憑證管理中心（Government Certification Authority, GCA），提供公鑰憑證服務，民眾如果要使用數位簽章（Digital Signature），必須從網路下載數位簽章的製作軟體，根據使用者的資料及產生時間，採亂數的方式產生一對密碼，一為「私密金鑰」，由使用者自己保存在磁片或 IC 卡，一為「公開金鑰」，則由憑證管理中心用來對外公開，因此公鑰與私鑰具有一對一的配對關係（盧鄂生、吳啟文，2001）。在法源的依據上，民國九十一年四月開始實施的「電子簽章法」，首條便說明該法之制定以推動電子交易之普及運用，確保電子交易之安全，並促進電子化政府及電子商務之發展為其主要目的，該法立法程序之完成，將可律定電子文件電子簽章法律效力，並規範認證機構管理機制（經濟部，2001）。

（二）常見的網路安全機制

藉由前述，可以了解有關電子檔案的認證管理與相關措施的運作，接下來所討論的是目前在網路上常見的安全機制：Secure Socket Layer（SSL）及 Secure Electronic Transaction（SET）。

1. SSL（Secure Socket Layer）

為保護資料於網際網路傳送時具安全性及信賴性，Netscape Communications 公司首先設計的 Secure Socket Layer（SSL）Protocol，主要是提供在網路上交易的雙方，在交易的過程中最基本的點對點(End-to-End)通訊安全協定，以避

免交易訊息在通訊的過程中被截取甚至變造，因此，SSL 協定是一個像 Web 伺服端(Server)與用戶端(Client)的安全通訊協定，但是並非一個完整的交易機制（陳則黎、蘇偉慶，2000)。由於 SSL 應用範疇廣泛、且具彈性，許多產品都已經支援此協定,其目的則是在提供網路應用軟體之間一個安全可信賴的傳輸服務（張德群，2001)。鄭美枝（2000）表示，SSL 協定提供安全之連線，有三大功能：

（1）私密性：使用對稱式金鑰系統，對傳輸的訊息與資料進行加密，以確保資料的私密性。

（2）身份驗證：使用非對稱金鑰演算法如 RSA 及證書管理架構，對交易雙方中伺服器端的身份進行驗證。並由伺服器端決定是否要驗證使用者端的身份。

（3）完整性：使用安全的 Hash 函數計算傳輸資訊的驗證碼並附加於訊息的最後面，以確保資訊傳輸的正確性與完整性。

據此可以了解，SSL 主要的功用即是確保顧客端與伺服器端資料傳送之安全，並利用密碼學之技術，來確保其機密性。由於 SSL 具備了安全機制，可以有效地防範日趨嚴重的網際網路侵害事件，因此在市場上受到普遍的歡迎。然而 SSL 即使有上述許多的優點特性，但在加密的過程中較為耗時，故其連線的效率較傳統未加密的降低許多，因此，一般只將 SSL 用於須加密保護的連線，普通連線仍採傳統的協定。

2.SET

安全電子交易(Secure Electronic Transaction，簡稱 SET)，是 VISA 與 MasterCard 兩大信用卡組織和其他公司於一九九六年共同宣佈， 並在一九九七年五月公布了 SET 1.0 版本，這是一種應用在網際網路上以信用卡為基礎的電子付款系統規範。簡單地說，SET 規格使用了公開金鑰(public key)與私密金鑰

(private key)所編成的密碼文件(cryptography)技術，以維護在開放網路上的交易安全性。具有 SET 規格的軟體，儲存在持卡人的個人電腦及特約商場的電腦網路中，此外，收單銀行的電腦也能夠以特殊的科技解讀金融資訊密碼，以及確認 VISA、MasterCard 或其他認證單位所發出的數位認證(Digital Certificate)（張德群，2001）。

SET 是一個定義相當完整，且針對信用卡做電子購物付款的一個交易協定，就其安全性來說，麻少華（2003）認為 SET 具有以下四種特性：

（1）資料保密性：SET 使用「電子信封」（Digital Envelope）的觀念，保護資料內容不會被其他的傳送者看到，電子信封的實行是利用「對稱金鑰」與「非對稱金鑰」來達成，其中對稱金鑰主要的作用是對訊息加密，而非對稱金鑰則是用來進行簽章以證明訊息發送者的身份，或者用來傳送對稱金鑰。

（2）資料完整性：利用「數位簽章」技術及 Hash 函數來進行訊息加密解密結果的比對，因此可以保證資料的完整性。保證資料完整的同時，可以傳送包含發送方公開金鑰的證書，使得接收方得以獲得其公開金鑰進行摘要的驗證。

（3）身份識別及不可否認性：SET 對身份識別與不可否認性的安全機制，採用「數位簽章」及可信賴的憑證管理中心（Certification Authority,CA）所核發的「憑證」共同達成。由於交易參與者可由層級式 CA 的公開金鑰來驗證對方(持卡人、特約商店、收單銀行)憑證的目的，因此不但可以確知交易對方的身份，更可以由證書中所包含的公開金鑰證明交易訊息是由憑證的所有人所傳送，藉此來達到身份識別以及交易的不可否認性。

（4）持卡人私密性：在 SET 的交易過程中，訂單資訊與付款指示分別由收單銀行及特約商店的公開金鑰進行加密的動作，因為「付款指示」中

包含持卡人卡號資訊、信用卡有效期限等牽涉到持卡人私密性的資訊，這些資訊必須避免讓交易的特約商店得到。

目前利用 SET 的技術，已經開發出可供相關特定對象使用的軟體；例如可供持卡人使用之電子錢包(E-Wallet)軟體、網路特約商店使用之 SET POS 軟體以及收單銀行使用之 SET Payment Gateway 軟體。除了可供直接使用之 SET 規格相關軟體外，此項安全電子交易技術已做模組化設計，可方便落實到各層級的應用界面，其中，發卡銀行模組讓發卡銀行可依需求設計有自己特色之電子錢包軟體，SET POS 模組讓網路特約商店可方便與密切的和其各種網路商場應用系統整合，收單銀行模組讓收單銀行可以和其各自不同的銀行主機系統加以整合，提供了最具彈性化設計，擴大安全電子交易技術之應用層面（張德群，2001）。

（三）小結

根據前述，可以概略的了解目前網路上的兩個安全機制 SSL 與 SET。綜括來說，SSL 只是一個資料傳輸的安全協定，它保證了交易雙方資料的傳輸安全，但未涉及各種交易的程序及訊息內容。而 SET 則為應用於網際網路上以信用卡為基礎的電子系統交易機制，它所採用的正是前述所提及的「公開金鑰基礎建設」（PKI）認證服務方式，兩者的安全機制比較表見表 2-2-1（麻少華，2003）；不同的需求設計就會有完全不同的安全等級，但兩種協定之間確保資訊上的安全、完整以及機密性而做的各項安全措施，是今日倚賴電子商務日深的社會大眾所不可不知的。

表 2-2-1　SSL 與 SET 的安全機制比較表

項　　目	SSL	SET 及其他 PKI
憑證申請與標準規範	無特別的標準規範，只要用戶端確認伺服器端的憑證即可，對申請者文件之身分確認較不嚴謹。	有明確且標準的憑證申請架構及規範，申請者的身分確認嚴謹。

資訊的隱密性 (Confidentiality)	用戶端與伺服器端間點對點的加密(RC4,RC5,DES,IDEA,Triple DES)	交易資訊以 DES key 亂碼保護，卡片帳號以 RSA 數位信封亂碼保護或 Triple DES key 保護。
資訊的完整性 (Integrity)	訊息有 Hash MAC 保護	訊息有 SHA-1 摘要值加數位簽章保護。
交易來源辨識性 (Authentication)	缺乏	由發送方的交易內容加簽章來辨識。
交易的不可否認性	缺乏	由發送方的交易內容加簽章來辨識。
風險性	較高	非常低

資料來源：信用卡網路安全機制探討，麻少華，2003，中華博碩士論文，91NTU00318112。

第三節　資訊的正確性、合宜性以及私密性

由於在網際網路上的訊息快速的流通以及使用者的匿名等特性，讓每個人都可以在網路上傳遞訊息，加上多媒體技術的發達，使得所呈現的內容除了文字外，各種的聲音、圖像等內容的呈現，更豐富了網路世界所提供的資訊，相較於過去學生受到傳統媒介的影響，網際網路兼備聲光效果更增添了許多的誘因，讓許多學子在網路上駐足而流連忘返。富邦文教基金會針對兩千七百位國小三至六年級兒童的「媒體使用行為」調查顯示，網路已經成為學童心目中最重要的媒體（61%），使用時間最多的電視，重要性已經降為第二（47%），報紙降為第三名（39%），而廣播則敬陪末座（27%）（引自李怡志，2003）；而根據美國 UCLA 大學的調查，在 12 到 17 歲的美國網路使用者中，有超過一半的人認為網路上的訊息大部份甚至是全部可信的（引自 Poftak, 2002），因此在網路成為學生目前訊息主要來源的同時，對於其所接受訊息的正確良莠與否，是值得深入探究的，此外對於日益氾濫的垃圾信件以及在網路上個人隱私遭侵犯等問題，也都是近來社會大眾、家長以及教育工作者所關心或擔憂的現象。以下將討論三個不同的主題：一、網路謠言的散播；二、垃圾信件；三、網路上的個人隱私。

一、網路謠言的散播與流通

網路上訊息多元化的呈現與快速的傳遞，讓人們不斷感受到各種資訊的充裕，卻很難對其分辨真偽良莠，透過如電子郵件（E-mail）或電子佈告欄（BBS）等工具散佈一些似是而非的訊息，使得社會大眾對其內容的詳實無法掌握，有人深信不疑，但也有人對網路上訊息的精確性失去信心。

（一）網路謠言的意義及其發生

由於人類是社群的動物，人與人或團體當中需要藉著語言來傳遞彼此的訊息，然而所傳達的內容卻很難分辨其真偽與否，Peterson 與 Gist(1951)表示，「謠言」(rumor）是指在群眾間針對某個對象、事件或是符合大眾興趣的問題，而流傳開的一種說明或未經証實的解釋（轉引自 Pendleton, 1998)。謠言通常牽涉到缺乏可靠的來源所證實的消息，根據 Aftab（2000）表示，多數「成功的」謠言都具備了三種特性，分別為

1. 謠言所提的內容是有可能會發生的。
2. 謠言涉及到某些我們所知道的或認為是真實的事件(例如經由器官的移植而感染到愛滋病)。
3. 謠言加入了恐懼感（例如與陌生人有性行為可能會感染愛滋病)。

劉莉秋(2002)歸納許多人的意見，認為一般流傳的謠言通常具有四種共同的要素：

1. 與現實有關的訊息：謠言是一種訊息，傳遞的是與時事或現實相關聯的訊息，也就是說謠言所傳播的訊息是大眾有興趣的現實事件。
2. 未經証實：謠言是一種未經証實其真實性為何的訊息。
3. 使人相信：謠言的目的在於使人相信，通常具備了強而有力的說服訊息。
4. 口耳相傳：是藉由人際之間的溝通來傳遞資訊，例如在人與人之間所交換的資訊，通常沒有真實或確切的證據來支持，這樣的特性也使得謠言散布的相當快。

汪志堅、駱少康（2002）也表示，謠言是否可以受到他人的相信，並不斷的加以散播，有很大的因素是謠言附上了可資佐證的證據，甚至加上了照片，讓整個謠言變得更為合理化；除了前述的幾種特性，再藉著網路的匿名、不受時間場域的限制等特性，在網路上散播的謠言顯得威力十足。網路雖然可提供更廣的言論自由空間，卻也可能因傳布謠言損及他人的名譽或企業的商譽。吳美瑩(2001)從電腦中介傳播（Computer-mediated communication，CMC）的角度來看，認為網路媒體中的傳播較缺乏面對面溝通所具有的「非語言線索」(nonverbal cues)，因此很容易在訊息交換的過程中，喪失了一些非文字所能表達的重要資訊。

過去在網路上的謠言，如喧騰一時的「衛生棉長蟲」事件，此謠言在 BBS 上傳播時，出現了同一人在幾個不同的留言板傳播的現象，同一篇謠言文章再由其他網友轉貼到其他討論區，等於是經過多人的散佈情形，因此很快的在一週內就達到顛峰，然而類似的謠言在香港透過傳統媒體的散布，歷時二週才爆發（蔡靚萱，2002)。近來還有如瓶中貓事件，在網頁上教人如何將小貓塞進瓶中飼養，由於內容過於殘忍，引起了動物保護組織與網路上很多人的撻伐，並發動連署抗議，後來都證明這只是一名 MIT 的學生和朋友之間所開的一個玩笑（廖肇祥，2001)。

藉由上述的例子，可以發現在網路上的謠言不斷的以各種形式推出，但大多具備了幾個條件：(1）彷彿真實事件般的陳述，(2）多媒體技術的運用，使人對其深信不疑，(3）傳遞的速度快且範圍廣。許多網路謠言甚至涉及了人身的安全問題，因此我們應該教導學生，使其對網路上謠言散佈的情形有所了解，同時也要懂得維護自身的安全。

（二）網路謠言的種類

網路謠言的種類有許多的類型，多半都是虛擬杜撰而產生，也有部份是真實但經過渲染誇大之後，變得似是而非；李怡志（2000)，以一位新聞從業人員的

角度出發，將網路謠言分為以下幾種典型：

1. 恐怖型：即利用人類恐懼的心態所創造出來的謠言，讓人心生害怕。著名的如：「旅行者小心，如果你昏迷醒來後發現自己躺在旅館充滿冰塊的浴缸中，小心你的腎臟已經被取走了。」
2. 陰謀不詭型：例如前述的衛生棉事件，以及肯德基所採用的鷄肉非真正雞肉等，涉及抹黑公司的形象。
3. 病毒型：例如前一陣子要使用者尋找視窗作業系統中是否存在某個檔案，如果在電腦中發現該檔，表示電腦中毒了，後經證實該信為惡作劇。
4. 憐憫型：例如之前「淡水賣鐵蛋的孤獨老人」，作者希望透過轉寄該信來幫助對方，沒人知道這老人是否真如信中描述般的可憐，不過卻為信中人帶來不少商機。
5. 貪心嚼不爛型：利用人性的喜好或貪小便宜的心態，例如轉寄某些信件可以獲得大獎。

劉莉秋（2002）根據 Knapp（1944）對謠言的分類，對消基會選出 2000 年網路十大網路謠言郵件，做出如表 2-3-1 之分類：

表 2-3-1 網路謠言分類

謠言的種類	網路十大謠言
1. 傳達夢想的謠言	「水晶肥皂是治療青春痘聖品」
2. 恐懼、憂心的謠言	「精鹽會使農藥化學成分鎖在蔬菜上」、「炸蟑螂可以使回鍋油變清」、「可樂能夠在十天內溶解鐵釘和牙齒」、「螞蟻會從耳朵入侵腦部」、「蠶絲被比化學纖維被產生更多靜電而危害健康」、「任何女人吃了 Progesterex 這種藥將無

	法懷孕」、「正露丸會導致直腸癌」
3.具攻擊或事件成因的謠言	「新光人壽對於B型肝炎帶原者的任何保險均不生效」

本研究者認為，上述的分類方式不論是從網路謠言的「內容」或以謠言所達成的「目的」來分類，我們不難發現這些內容大多對人們在日常生活中可能遭遇的危機，似乎是提供告誡。而汪志堅、駱少康（2002）也表示，謠言未必都是有害的，一些謠言甚至具有正面的效果，而其所傳播的訊息，只是要將某種訊息傳播給整個社會，例如手機具備的救援功能；許多人甚至已經將這些被認為有益於日常生活的警示性的訊息，當作可以和別人交換資訊的資源，然而訊息的正確與否，卻很少人加以探究。

（三）防堵網路謠言

如前所述，網路已經變成現代人接收知訊的一種重要途徑，如何讓學生收取正確、合宜的資訊，而不會被虛偽、不良的資訊所誤導，是當前最重要的課題，因此本研究者從保護自身安全的觀點，並根據許多學者專家意見，認為可以從下列幾個方面來著手：

1.信賴知名的網站：可以引導學生透過學校或圖書館許可的連結來搜尋資料，或是瀏覽搜尋引擎所提供的目錄連結，而不是用幾個簡單的關鍵字所找到的網站，因為在搜尋引擎上的目錄所連結的網站是經過專人檢視過內容，並決定是否要放在目錄之下（Aftab，2000）。

2.謠言查証網站：例如國內外有幾個知名的網路謠言查證網站，來防止謠言的無限擴張。

3.透過可信度較高的大眾媒介進行追蹤報導：經過更具公信力的媒體進行追蹤報導，也可降低網路中以訛傳訛的現象（劉莉秋，2002）。

4.網路討論區的自律：例如在BBS討論區內可以觀察到網友提供闢謠資訊，資訊的豐富程度與正確度甚至超越專業新聞媒體，同時BBS站內的管理機制也即時

運作，位居第一線的板主們進行刪除謠言文章、將闢謠文章做標記或收入精華區等動作。顯示 BBS 自律力量能一定程度地打擊謠言傳播（蔡靚萱，2002）。

在網路已經變成日常生活不可或缺的一部分的同時，很多時候個人的一個故意或不經意動作，常會造成許多的連鎖反應，網路謠言就是藉由如此來達到散播的目的，有時候連一般的成人都無法分辨出訊息內容的真偽，因此除了透過上述的幾種方式來遏止網路謠言的傳遞之外，最重要的是教導學生對事件內容或資訊做合理的懷疑，同時藉由正反面資料的蒐集，才能做出合理的判斷。

二、垃圾信件（Spam）

電子郵件（E-mail），伴隨著網路的發達而興起，由於它的即時性並結合了多媒體和可以大量傳送等特性，加上網路不受限於空間地域的限制，使得電子郵件不但已成為現代人生活密不可分之通訊工具，更隨著網路廣告之蓬勃而成為便捷、成本低廉的行銷利器，但是未經收信者同意而濫發電子廣告郵件，卻造成嚴重的垃圾電子郵件(Spam)氾濫問題，不僅浪費頻寬引發許多爭議，同時也是資訊安全中，所不可忽視的一環。

（一）垃圾電子郵件之定義與所產生的困擾

自從第一封垃圾信件流通在 ARPANET 上到目前為止，已經有二十五年的時間了，但是直到十年前才有 Spam 這個名稱出現，用來指稱將一份內容相同的電子郵件，未經收信人許可，大量寄給很多人而其內容多數是與收信人不相干的商業廣告（廖述惟，2002），發送 Spam 的人則稱為 Spamer；追其字源，Spam 原本是指一種流行在二次大戰期間但是卻在六十年代被大家所排斥的一種豬肉罐頭，後來逐漸被人用來引伸作為多數人都不想收到的垃圾電子郵件；垃圾電子郵件的特性，通常都是無用的，甚至是充滿詐欺或侵犯到個人的，近年來電子商務的發展熱潮，更使得垃圾信件的數量暴漲；據統計，在美國垃圾信件所出現的型態，大

致上以三種類型居多，分別為資金的再提供（refinancing）、信用諮詢（credit counselling）以及促銷情趣用品（sexual enhancement product）(Hinde, 2003)。而根據賽門鐵克（2004）對全球的統計，垃圾信件的種類所佔比例最多的前三名依序為產品推銷（25%）、金融（18%）以及成人廣告（15%）等，可見，大量發送廣告信件已經逐漸成為一種新的產品行銷或服務提供的最佳利器。

根據調查，有百分之四十九的美國人每週必須多花超過四十分鐘來刪除垃圾信件，他們每週刪除垃圾信件的次數比他們所做的其他活動還多出許多(Hinde, 2003)。在台灣，使用者每天收的信有超過 4 成是垃圾郵件，另外有超過 2 成的使用者覺得收垃圾信件讓他們覺得不堪其擾，而清理這些垃圾每年耗掉台灣的社會成本超過 600 億元，全球每年的垃圾郵件數更超過 2 兆（邱俊吉，2003)。

Spam 對企業來說更造成很大的支出，例如時間以及金錢，它不只塞滿每個人的信箱，也拖慢了網路與全球的伺服器，由於垃圾信件的流量已經遠超過一般信件，許多公司必須花費更多的時間去刪信，同時也要買更大的郵件 server 跟存取系統避免郵件塞爆伺服器，以及維持網路的暢通，據 Stephen, Heather, Ira, Steve & Andrew（2003）的調查，Spam 使得公司對每人每年多了 874 美元的支出；對校園來說，許多人認為垃圾信件在學校所產生的問題將比對企業的影響更大，因為校園網路的基本任務是分享資訊，較一般企業網路更開放，而學校也比公司更少去阻擋疑似垃圾信件的傳輸，這些都使得校園中垃圾信件的問題將更趨於嚴重（Florence, 2002)。

也有學者表示，Spam 對於接收者與提供網路服務的業者（Internet service provider , ISP）都造成很明顯的時間與財產上的浪費，一些提供網路服務的業者甚至控訴 Spamer 的做法如同侵犯財產，因為垃圾信件從寄件者發散出來的過程，透過許多的伺服器傳遞到收件者的郵件伺服器，最後到郵件被收件者打開，這當中需要花費許多的時間，因此 Spam 不僅影響了 ISP，同時還影響了收件者的權利（Spinello, 2003)。

由上述的討論，可以了解垃圾信件快速成長的情形，對個人、團體或是整個

社會都帶來很大的困擾，造成社會成本的耗損，同時也使得一向扮演知識分享角色的學校網路，逐漸為垃圾信件淹沒而效能不彰，這種濫用社會與網路資源的情形，都讓大家不得不正視這樣的問題。

（二）常用的垃圾信件技巧與相關建議

就目前來說，每個使用電子郵件的人，幾乎已無可避免的受到垃圾信件的騷擾，究其原因，主要是因為現有的電子郵件本身傳遞機制上的缺陷以及大量發送信件所需的成本相當低廉（王正豪，2004）。但令人好奇與不解的是，在眾多的電子郵件位址中，究竟發送的人是如何找到屬於每個人的信箱位址。以下將探討 Spam 所常用的手法，最後歸結之，並提出相關的建議。

垃圾信件不容易去防止，是因為發送的人一直在改善他們所使用的技巧，常見的手法一般來說有以下幾種：

1. 購買郵件清單：部份不肖之徒，利用某些場合取得的個人 e-mail address，轉賣給一些意欲圖利的人，一個發送 Spam 的新手可以用很低的價格來買到幾百萬個電子郵件位址，所需要的只是更大一點的頻寬來寄送 Spam（Schwartau, 2001）。
2. 使用軟體程式去網頁上蒐集 e-mail：使用這一類軟體，可以在網頁上獲得大量的郵件位址（Florence, 2002）。
3. 用一些稱作「字典攻擊」（dictionary attacks）傳送 Spam：使用軟體可以隨機產生出一些常被用來做為電子郵件的帳戶名稱，雖然此種方式偶爾會產生一些無效的位址，不過仍是有效的垃圾信件發送方式（Florence, 2002）。
4. 蒐集新聞群組討論區上用來張貼訊息的使用者郵件位址（廖述惟，2002）。
5. 修訂許多技巧去防止一些阻擋技術：例如「軟體機器人」（Software robots）建立空的信件帳號，並增加一個獨特的號碼到每一封訊息上，讓過濾器無法判定是否為 Spam（Florence, 2002）。
6. 一些公司販賣寄送垃圾信件的軟體，並告訴初學者可以偽造 e-mail，這樣他們就不會接收到很多人憤怒的回信（Schwartau, 2001）。

由上可知，傳送垃圾郵件的手法多元化，在日常生活當中依賴網路漸深的人，很容易在不知不覺中，就讓自己的電子郵件位址流露出去，成為有心人士販賣的名單之一，一些人甚至利用某種技巧，躲避過濾軟體的運作，達到放送信件的目的，使用者已經對其防不勝防。

（三）防堵垃圾電子郵件的相關建議

許多人認為垃圾信件已經侵犯到個人或者機關團體的權益，因此要求法律對相關行為提出明確的處罰，例如在 2003 年，美國眾議院以壓倒性的高票通過了「反垃圾郵件法案」，根據該法案，那些利用 e-mail 亂傳垃圾信或是色情內容的人，將會被處以數百萬美元的罰鍰甚至被判刑（歐陽宜珊，2003）。然而透過立法真的有效嗎？Hinde（2003）認為，如果某國立法案來防堵 Spam，或許可以對該國內寄發垃圾電子郵件的業者有所懲治，但是對於從他國的發送者卻毫無赫阻效果，當然，垃圾信件的發生不應是單一國家所應承擔的責任，而是全球的問題。

以下根據許多專家建議，本研究者整理出幾種使用者本身可以採用的垃圾信件防治方式，期能對個人層次的反制垃圾信件有所助益。

1. 利用「郵件規則」封鎖或使用過濾軟體：多數的人都會建議使用具有過濾軟體的收信系統，但要特別注意使用的適切性，最好能對該軟體有一定的熟悉程度，否則可能連使用者想收到的信都被阻擋在外（王正豪，2004；Florence, 2002）。
2. 保護自己的郵件位址：不要開放分享自己的 e-mail，例如在網站上公佈自己的 e-mail 位址通常都會變成有心人士蒐集的對象，或者加入某些需要會員資料時，自己的郵件位址也因此而外洩了（Hinde, 2003）。此外，當需要對兩個以上的朋友發信時，盡量採用「密件副本」的方式發送，以避免郵件位址到處流傳。
3. 將信箱作區隔：可以申請免費的公眾信箱，作為其他申請入會用的資料或在討論區用，如此大量的降低自己私人信箱接收垃圾信件的危機（王正豪，2004；

Hinde, 2003)。

4. 當收到 Spam 時刻意的忽略：許多廣告信件都會告知使用者，如果不想再接受到同樣的訊息時，可以按下不想再收到的字樣，但是一旦使用者這樣做，反而讓對方知道該電子郵件是有效的，後果可能會是收不完的垃圾信(Schwartau, 2001)。

5. 檢視網站的隱私政策：一些網站在登錄時，會提供相關的隱私政策，如果使用者不想接收任何多餘的訊息，要記得勾選不想接收的選項 (Hinde, 2003)。

6. 通知 ISP 處理：目前台灣的 ISP 以透過網路自律公約的約束方式，約定業者與使用者無正當理由不得發送大量信件給其他用戶，如經發現則 ISP 將進行刪除信件並且取消該業者在 ISP 中所享有的權利，甚至可能在 Router 中過濾該業者 IP 或所利用的 E-mail server 所傳來的封包（廖述惟，2002)。

（四）小結

垃圾信件目前來說已對電子郵件的使用者經造成很大的不便，不論是網路的頻寬被佔據、企業增加的成本乃至於降低國家社會的生產力等，也許有人對垃圾信件存有不同的看法，認為垃圾信件在某方面代表了言論的自由，不論其是否從事廣告行為，發送的人都有權如此；但就道德面來說，垃圾信件形同某種入侵行為 (Spinello, 2003)，發送垃圾信件的人知道使用各種方式來對網路使用者進行推銷，這樣的行為幾乎是毫無限制的，他們可以販賣任何的東西，甚至不顧購買對象為何，例如業者大力散發情色商品的廣告，但卻沒有顧慮到消費者很有可能是未成年的青少年；因此，即使目前缺乏具體的管理機制，但是由教育上著手，教導學生懂得垃圾信件的意涵，並盡量避免接受廣告信件的騷擾仍不失為一個好對策。

三、網路上的個人隱私

在網路的世界中，很多時候會讓人誤解自己是隱形的，所作所為別人很難察

覺，但事實上在網路裡的個人並沒有想像中擁有那麼多的隱私，我們的網路行為都在某處被紀錄了下來，這由每天家裡所收到的垃圾信件就可以明顯地反映出來（Schwartau, 2001）。目前網路使用的族群，多數為學生、青少年族群甚至兒童，在對於隱私的概念不是很明瞭的情況下，特別是當他們想獲得一些有趣的小贈品或小遊戲時，學生或孩童們似乎很難理解洩漏個人資料會招致什麼樣的後果（Aidman, 2000）。但是，洩漏有關個人資料的後果，將使得這些資訊流傳在網路上數年之久，任何人都將輕易的取得個人資料，不僅帶來困擾，也為社會增添了更多的亂象，因此教導學生保護個人資料，將是重要且刻不容緩的。

（一）網路上的個人隱私

隱私（Privacy），通常包含了兩個要素，分別為「有能力去掌握自己的資訊」以及「能完全掌握有關自我的價值」，第一個因素存在現有的法律條文中，每個人都有權力去掌握自己有關的消息，至於第二個要素就比較難達成，尤其目前的電子交易盛行，許多人在還沒察覺中就不經意的洩漏出自己的資料，一些公司甚至很少提出保護消費者隱私的相關措施，讓維持隱私的第二個因素很難達成（Senicar, Jerman-Blazic & Klobucar, 2003）。

許多人以為隱私只對那些想隱瞞某些事情的人是重要的，其實這樣多半誤解了隱私的意義，隱私包括了個人的資料，如果個人資料遭盜用，被其他的人用來申請金融帳戶，從事不法的行為，勢必使身分被冒用的人無辜承擔許多責任，隱私也包含個人家裡的住址跟電話，如果這些資訊被公開，當事人被騷擾與跟蹤的機會一定增加了，其他如一些資料如疾病史的公開，甚至會使得當事人覺得難堪，因而喪失尊嚴（Kang, 1999）。

當前有許多網路專家不斷鼓吹、許多網站奉為圭臬的「個人化」（Personalization）的策略，便主張蒐集個人資訊、然後據以提供「個人化」的服務，對網友可能有兩個好處：

1.節省時間：公司能瞭解使用者的需求，將能讓使用者上網時，不必經過層層鏈

結就可以找到所需的資訊，節省使用者的時間。

2.拓展視野：行銷人員透過電腦系統所掌握的潛在消費者個人資料，加以歸納分析後的假設，使用者可以有機會得到行家的建議，或是獲得跟他生活形態相近的人所接觸的資訊（劉一賜，民 88）。

然而在網站蒐集「個人化」的資訊之後，連帶的會造成許多負面的效果，最嚴重的莫過於侵犯個人的隱私，使人覺得其他人可以掌握自己的一切而毫無機密可言，許多網站雖然提供一些如帳戶密碼的保護機制，然而密碼通常是所有的保護當中最弱的一環，個人的身份容易遭到竊取，更使得消費者必須浪費許多時間跟金錢去彌補損失（Hinde, 2003），由此可見，在網路上有關個人的資訊已經產生許多的危機，許多人甚至無法完全掌握自身的價值。

（二）常見的個人資料外洩

網際網路的使用，讓人可以恣意地遨遊在不受時間與空間阻隔的場域中，如此便利的特性也往往使人樂在其中進行一些活動，然而個人資料在使用網路的過程中，卻很容易就外洩，許多時候洩漏資料是在使用者毫無防備或察覺的情況下發生；Willard（2002）將公司蒐集資料的方式分為透過直接或間接兩種方式，直接的需要個人主動的參與，也就是使用者必須有意願去提供個人的資訊，主要是透過註冊、調查、問卷的方式。中央警察大學資訊密碼暨建構實驗室（2003）舉出，個人資料會透過如免費郵件空間、線上購物、網路社群、網路徵才、線上算命、冒牌網站以及醫療網站等管道曝光，歸納其共通處，都是提供一些服務來吸引使用者註冊，其中尤以免費電子信箱最能吸引大量使用者，是目前相當普及的服務，使用者的人數相當多，如 Pchome、Yahoo 或 Hotmail 等，都是很著名的提供商，但是註冊時需填寫個人資料，如姓名、出生年月日、身分字號、聯絡住址與電話等，業者也等於掌握了相當龐大的使用者資料庫。

間接資料的蒐集，是藉著在電腦上放一些小程式，稱做 Cookies，這些訊息

可以告訴該網站你從什麼地方來以及你在網路上做什麼，甚至去過哪些網站待了多久的時間都包含在內，目的在追蹤使用者的線上活動（Aidman, 2000）；對電子商務來說，Cookies 是種有效的科技可以加強網站的互動性，但是對個人的隱私來說，這無疑是一種威脅，因為消費者很難去掌握由 Cookies 所存取的到底是何種資訊（Senicar, Jerman-Blazic & Klobucar, 2003）。

（三）如何預防在網路上的身分資料洩漏

藉由前述，可以了解由於電子商務的發達，個人通常會提供一些有價值的訊息給那些想提供我們產品服務的人，並藉由站上註冊，在不清楚對方的動機之前，就讓它可以存取個人的資訊，這些都是導致在網路上個人身分外洩的原因（Aidman, 2000），因此有效的預防個人資料的洩漏，已經是目前相當重要的課題。

美國政府在 1998 年 10 月通過兒童網路隱私保護法案（Children Online Privacy Protection Act , COPPA），其目的就是在網路發達的今日，保障兒童參與網路活動的安全，並提高家長參與子女的網路活動，由家長扮演守護者的角色，以保護兒童在網路環境的隱私權，如該法規定，在蒐集、使用或公開 13 歲以下兒童的個人資料時，必須獲得該兒童父母之同意（葉芳如，1999）。由於成長中的青少年，對於網路上所充斥著各種廣告，不僅缺乏能力去分辨，更經常被廣告詞所吸引，而洩漏個人資訊，因此該法的設立，具有相當的指標性意義。

除了透過立法的途徑來保障兒童在網路上的隱私之外，個人隱私的保障，似乎應該要有一些更為積極的作法；Willard（2002）提供幾種關於保護個人資料的建議，希望能讓個人在網路上的行為有所警覺，以降低許多洩漏身份資料的風險。

1. 考量是否公開個人資訊：個人可以決定是否公開自己的資料，但對青少年來說，可能需要先與父母討論關於家庭的資料有哪些可以公開的，在使用網路時，最重要的就是不要將個人或家庭的資訊流露出去。

2. 尊重他人隱私：個人的秘密只有自己才有權決定如何公開，如果因為外洩了他人的資料而使對方蒙受損失，洩露秘密的人是要負責的；例如他人告知有關個人的隱私，應該採尊重的態度，或者別人用轉寄信件的形式，不應該沒有原發信人的允許就轉寄給其他的人，因為自己通常也不會希望別人這樣對你。
3. 在討論群組及聊天室保護自己的隱私：當個人在線上討論群組分享自己的資訊時要非常的小心，因為幾乎所有討論群組的資訊被會紀錄在電腦系統中，如果有心人士要尋找這些資訊的話，相信這件事對他們來說不是難事。
4. 在商業型的網站保護你的隱私：商業網站的目標就是獲利，因此多數的商業型網站對獲取個人資訊是相當有興趣，如此一來，藉由不斷寄發個人有興趣的產品服務，將可以更快達到宣傳的效果，所以個人在這種網站上的資料也要特別小心。

在美國，「民主科技中心」（The Center For Democracy & Technology, CDT, n. d.）組織，在其網站上列舉了保護個人隱私的十大原則，以下分別將其列出：

1. 參考網站的隱私政策：越來越多的網站提供詳細的隱私政策，使用者要非常小心仔細地參閱，以維護自身的權益。
2. 將電子信箱區隔：可以將個人在家使用的與工作用的分開，這樣可以減少私人信件被檢視的機會。
3. 教導孩子在網路上發送個人資料就如同給了陌生人一般：要教導孩子，在獲得允許之前不得給予其他人有關自己或家庭的資訊。
4. 在瀏覽過網頁後清除暫存區的記憶：在瀏覽網頁的過程中，通常也會將網頁上的資料或圖片紀錄下來，如果電腦是與他人共用，個人資訊就很容易外流。
5 確認線上的表單具有安全機制：就是確保在填寫一些線上表單時，是透過安全機制來存取與傳輸，如此才能有效保護個人隱私，同時不要在一些不安全的網頁上輸入一些敏感的個人資訊。
6. 拒絕不需要的網路餅乾（cookies）：cookies 可以讓網站存取有關個人的硬體

與瀏覽網頁的資訊，甚至是一些個人的帳號與密碼；減少或降低一些非必要的cookies，讓個人資訊多一些保障。

7. 使用可以匿名的軟體：運用可以寄送匿名信的軟體，甚至可以將轉信的位址都隱藏，保護個人在談論一些具爭議性話題時的個人隱私。
8. 使用電子郵件加密軟體：可以對信件的內容加密來達到保障個人隱私，許多信件軟體（如 outlook）都已內建該功能。
9. 當瀏覽網頁時使用可以匿名的軟體：在瀏覽網頁時，每項步驟都被紀錄下來，就如同飛航紀錄器般，因此維持個人匿蹤性的軟體也因應而生。
10. 不參加資訊分享：許多線上公司提供個人選擇，可以將個人從資訊分享的名單中移除，但是一般來說要如此做是相當困難甚至幾乎是不可能的。

CDT 最後還提供了一個技巧，那就是「用一般的常識來判斷」，思考在日常生活中所使用的行為模式，並將其運用到網路的世界裡，例如可以問自己在生活中會告訴他人自己的信用卡卡號嗎？或者在訂閱報紙的時候有多少資訊要如實填寫？或者想想如果填寫自己的住址或電子信箱，是不是有可能會收到大量的垃圾信件？

根據前述，可以歸納出幾種在網路上保護隱私的措施，本研究者將其分為使用者本身對隱私概念的認知、使用電腦的技巧以及外在因素的配合等三方面來加以討論：

1. 使用者本身在隱私概念的認知：例如思考個人資訊公開的程度、尊重他人的隱私、教導學生在使用網路的隱私概念、參考網站的隱私政策以及使用者用來判斷的一般常識等，這些都和個人對隱私觀念的重視與否有很密切的關係。
2. 使用電腦的技巧：如確認網路上的安全機制、拒絕不必要的網路餅乾、使用具有匿名性的軟體、清除電腦上的暫存記憶體等等，與使用者對電腦相關軟體使用技巧的閑熟度有關。
3. 外在因素的配合：例如法律的制定、網站隱私政策的制定等等，所需的是外在

環境或者網路業者的自律。

一個完整的資訊教育課程，可以幫助使用者知道在網路上所發生的事以及個人的資料有可能在網路上被濫用，因此本研究在課程的設計與發展上，將會針對網路隱私的認知與概念的導入以及相關的維護措施技巧的介紹加以安排，使學生對在網路上的隱私保護有所瞭解，從而達到保護自身安全的目的。

第四節　個人安全防護

在個人安全保健上，由於現代人對電腦的依賴逐漸加深，電腦已經變成多數人每日不可或缺的工具，然而隨著接觸電腦時間的加長，對身體健康產生不良影響的可能性就會增高。本節主要在討論常見的電腦傷害，其次提出使用電腦的相關建議，因為這些都是個人的資訊安全方面，極為基本且重要的。

一、常見的電腦傷害

報章雜誌上常見使用電腦所造成的傷害之報導，例如一名三十多歲的女性每天在電腦前工作超過十小時，連續工作了一個月後，手腕產生異常病痛，經醫生診斷是患了「累積性傷害症候群」(高麗玲，2003)。另外，許多的家長規劃電腦為孩子學習的重要工具，造成學童接觸電腦的機會增加，但接觸的年紀卻越來越小，根據衛生署近日公佈的近三年學齡前兒童視力篩檢成果，國內學齡前兒童已有 4.51%有近視、散光等毛病，其中絕大部分是近視，醫生表示可能的原因是看太多電腦或電視（張黎文，2003)，據此可知，電腦對人體的健康，存在許多潛在的危害，根據本研究者歸納出常見的電腦傷害，可分為四大類，分別如下：

（一）姿勢不良所造成的傷害

包括不當使用鍵盤、滑鼠以及坐姿不良等，產生如頭痛、頸肩部僵硬酸痛、脊椎神經的傷害，多數是因為缺乏活動筋骨或坐姿不正確而造成身體上的不適，

例如「重複施緊傷害」(Repetitive Strain Injury, RSI)，所造成的傷害包括手腕神經壓迫症(症狀包括手腕無力、疼痛、無法舉雙肩等)、脊椎神經傷害、頸部及腰部僵硬酸痛等病痛（Thomas, 1999)。

（二）缺乏休息所受的傷害

眼睛的過勞（Computer vision syndrome, CVS）是電腦族群中最普遍的疾病，包括眼睛疲勞、視力模糊衰退等使用電腦所引起的視力徵候群，而持續長時間的工作，對於身體骨骼與肌肉的傷害也是主因之一（黃翠玉，2002；Louis, 1995；Shaw-Mcminn, 2001)。

（三）電腦輻射的傷害

雖然輻射對人體是否會產生病變尚未有定論，但是科學家在某些研究中，輻射線會對一些動植物產生某種程度上的傷害，一些研究甚至提出對電器產品與癌症或流產之間的關注。雖然至目前為止，我們還不知道所有輻射與人體傷害的因果性，但是如果非必要應該避免長時間暴露在這些威脅之下(劉志明，1998;Louis, 1995)。

（四）環境的傷害

造成傷害的另一個原因，很多時候可能是設備所引起的，據調查學生在學校所使用的電腦桌椅等設備多數是為成人所設計的，學生們在使用時，不得不遷就設備而扭曲了自己的身軀，造成姿勢不良並產生傷害；多數的學校卻忽略了學生使用電腦姿勢的重要性，重點則都擺在硬體設施的建設上(黃翠玉，2002;Thomas, 1999)。

二、預防電腦傷害的方式

針對以上使用電腦所造成身體上的傷害，本研究者提出以下幾點建議：

（一）要有充足的休息：前述的 RSI 就是發生在重複維持同一個工作姿勢一段時間，或者待在電腦前很長時間，卻不讓身體有適當時間休息，因此在長時間的工作中應該試著改變姿勢，可幫助個人避免不適與疲勞；在視力的保

健上，建議使用電腦一至兩小時後，應該至少閉目或注視遠方 5 到 10 分鐘，以便讓眼睛休息（高麗玲，2003；黃翠玉，2002）。

（二）保持正確的姿勢：根據專家的建議，在使用電腦時有以下幾個方式，有助於提供個人一個更舒適的環境：

1. 能抬頭挺胸讓頭不偏前或向後，並與螢幕保持一個手臂的長度（見圖 2-4-1）。
2. 椅子應該輕微向前傾斜幫助膝蓋能夠彎曲。
3. 將鍵盤、滑鼠或軌跡球置於同一高度；這些硬體應放在約為手肘的高度平面上，另外上臂應放鬆下垂於身體兩側。
4. 將電腦螢幕上端置於接近眼睛的高度或稍微低一些。
5. 背部應該直挺或從臀部向前輕微彎曲。
6. 輕觸鍵盤、滑鼠按鈕、搖桿或其它的遊戲控制器，並保持手部與手指放鬆；避免在打字時將手掌或手腕靠在任何平面上，若附有手部休息墊，請僅在打字空檔時才使用該休息墊。（見圖 2-4-2）
7. 將桌面下的物件移開，如此可舒適地置放與移動腿部（台灣微軟，2001；Louis, 1995）

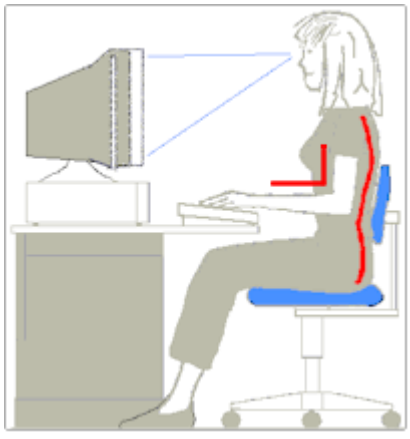


圖 2-4-1 正確的坐姿

（取自 blogtw.com）

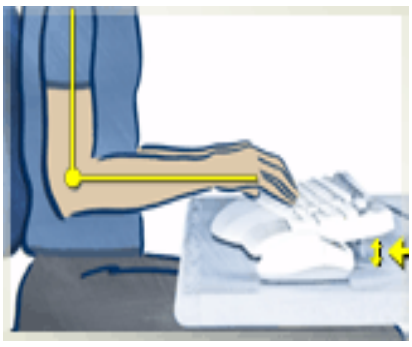


圖 2-4-2 正確的打字姿勢

（取自台灣微軟）

（三）避免暴露在電腦螢幕下的時間過久：研究指出，電腦螢幕後方的輻射量比正前方高出許多，因此不要長時間在其他人的螢幕後面工作；此外，使用螢幕的距離最好保持七十五公分以上，更能確保身體健康(劉志明，1998)。

（四）養成良好習慣並充實保健常識：如鍵盤、滑鼠操作所產生的影響是現在電腦傷害中最嚴重的後果，良好的擺設位置以及正確的操作姿勢是亟待建立的觀念，我們應該讓學生在校時就養成操作電腦的好習慣，才不致於對他們往後的身體健康產生很大的傷害；此外，許多電器產品的安全規格，對人體所可能產生的影響都有一定的檢測標準，因此對產品安全規格等相關知識的了解，將可以有效的預防電腦所引起的傷害(黃翠玉，2002，Thomas, 1999)。

目前整體的環境來說，學校在資訊設備的建置上已大致完備，多數學生的家中也多有電腦設備，對於中學生而言，使用電腦或許可以產生正面的教育意義，但電腦的運用對於人體的健康也有許多潛在性的危害值得注意。尤其正值青春年少的中學生，對於電腦使用的保健知識，更需要有正確的觀念以及養成良好的習慣；教育工作者在教導學生利用科技從事學習活動之餘，也應將這些知識融入教學中，以建立起學生正確的健康觀念，才能讓他們在快樂安全的學習環境中與電腦一起成長。

第五節　我國現階段的資訊教育

上述三節，主要在探討本研究中提出的資訊安全三個面向，本節則用來說明我國目前在資訊教育推動的現況，以及可能遭遇到的困難，同時也對現有教材作一概括的說明，作為本課程發展之基礎。

一、資訊教育現況

資訊教育泛指與資訊有關之課程、教學、師資等之教育措施與活動，狹義地說，便是指電腦教育（何榮桂，1998）。目前我國的資訊教育課程始於國民小學，並自 84 年度開始沿用至今，在此之前，國中、小並沒有電腦課程；現行的中、小學電腦課程中，國小由五、六年級開設電腦課程（民 89 年新訂），國中則於二、三年級實施電腦課程（民 87 年修訂），但是在課程的設計上都比較強調基本的電腦操作與網路的應用（龔裕民，2002）。然而教育部自民國八十七年，在國內推動擴大內需方案，編列了六十七億元的經費，購置全國中小學的電腦設備，繼而又推動教室電腦，配合九年一貫的施行，將網際網路落實到中小學的每間教室內（陳文進，2000）；民國九十年，教育部又公佈了「中小學資訊教育總藍圖」，以「資訊隨手得、主動學習樂、合作創新意、知識伴終身」為四大願景，使我國的資訊教育邁入一個嶄新階段（教育部，2001）。

近來，教育部著手於「九年一貫國民教育課程」的推動，揭示了十大基本能力，其中「運用科技與資訊」能力為此十項基本能力之一，目的是希望學生能正確、安全和有效地利用科技，蒐集、分析、研判、整合與運用資訊，提升學習效率與生活品質；然而在九年一貫的課程中，「資訊教育」已列為「非學習領域之課程」，而屬於六項重大議題之一，依其課程精神，各領域實施教學時，需將資訊科技融入教學活動當中，資訊教育不再是單一、分科的課，而將是以應用、整合的型態，存在於各學科、領域中（曹雅芳，2002；）；陳朝平（2003）以為，資訊教育應該歸入某一學習領域，而不是將之歸為「議題」，成為未定案的事項；此外，許多電腦基礎課程都提前至國小教授，但是卻缺乏一套標準的內容教材，各校的課程教材及課程內容是各校老師自行設計發展（張郁蔚，2003），而國二、三以後電腦課程取消，改由各領域教師利用電腦資源進行教學，不另設電腦課，此舉將連帶使得資訊教育的課程產生許多問題。

根據沈中偉（1999）針對國小資訊教育的現況進行研究，指出國小資訊教育所遭遇到的問題除了缺乏足夠的資訊教育師資，以及軟硬體設備的維護之外，還有課程上並未將資訊教育納入正式課程，況且課程標準不一致，教材上有些混

亂，也無法與國高中課程銜接，都是資訊教育實施的障礙。

龔裕民（2002）指出，長期以來國內的電腦基礎教學偏重於技能及操作，尤其側重於網路的相關技能，如網頁的製作、FTP、E-mail、BBS 等，類似的基本能力在國小階段已列為重點，國中階段應該朝向進一步的網路應用開展，如網路素養、道德層面的能力培養等。

陳敬衡（2002）在高中資訊素養課程的研究中亦表示，資訊素養教育不僅在一個年齡層上的發展，同時也會在不同的階段有不同的訴求，因此格外需要培養學生運用資訊以及反省思辨的能力。

林佳旺（2003）在整理國內幾位學者對於現行資訊教育體制面臨的問題與實施的困境所做的研究後認為，資訊教育工作的推展至少存在以下幾點問題，仍須改善：

（一）課程推動缺少完善組織：例如缺乏人員管理維護設備等問題，導致正常教學受到影響。

（二）資訊課程未納入正式課程：資訊課程屬工具性入門課程之操作本質，同時具有明確的內容，並非有爭議之處，因此未納入正式課程而列為議題是徒增學校及教師的困擾。

（三）資訊課程安排偏重技能性學習：依課程綱要在資訊課程內涵節數的安排上，實際上仍著重於電腦網路知識、應用技能的訓練，但在正確電腦網路的使用態度、使用規範的養成教育上明顯不足。

（四）課程編排缺乏一貫性，教材內容差異大：九年一貫課程改革對於資訊融入各學習領域的方式，給予學校及教師相當大的彈性空間，各校的教學目標、課程的編排與教材內容均不一致，使學生的資訊素養能力受教與養成方面，缺少普遍性及公平性的原則。

綜上所述，可以得知目前資訊教育的現況缺乏明確的指標，不僅各級學校的重視程度不一，同時，課程的問題在九年一貫課程實施之後，也造成許多紛擾的

現象，由於國小資訊課程安排，學生學習的內容偏重技能取向，而中學生的資訊教育內容也多所刪減，此舉將使得學生對於科技的使用，更缺乏引領，而導致資訊科技的使用認知更為貧乏；另一方面，教材的多元化更使得學生受教的權益產生許多的影響；為了迎接新世紀網路資訊社會的來臨，對於資訊教育課程的妥善設計規劃，將是目前所要審慎評估與面對的要項之一。

二、資訊課程中的資訊安全

在九年一貫課程的規劃下，現有的資訊課程透過了解資訊科技的特性及其對個人與人類社會的影響，並針對不同領域學習所需之基本需求，分析出共通的資訊基本學習內涵，期能在認知、情意、技能上達成以下之教育目標(教育部，2003)。

（一）奠定學生使用資訊的知識與技能。

（二）導引學生了解資訊與日常生活的關係。

（三）增進學生利用各種資訊技能，進行資料的搜尋、處理、分析、展示與應用的能力。

（四）培養學生以資訊知能做為擴展學習與溝通的習慣。

（五）導引學生了解資訊倫理、電腦使用安全及資訊相關法律等相關議題。

（六） 培養學生正確使用網路的態度，善用網路分享學習資源與心得，培養合作、主動學習的能力。

（七）開展學生資訊科技與人文素養的統整能力，應用資訊科技提升人文關懷、促進團隊合諧。

上述為資訊教育欲達成的教育目標，就所提及安全內涵來說，可分二個階段，分別規劃在初級的認識電腦配件、操作環境、姿勢及環境可能造成的危害，以及在更深入的教導學生注意軟硬體的保養、備份資料等資訊安全概念。然而本研究者在檢視目前國中的教材內容，現有提及資訊安全的概念，都包含在「資訊倫理」的議題之下，而當中所提及的資訊安全見表 2-5-1，在所參考的三個版

本中，大多並未替資訊安全下一個明確的定義，同時在防範的措施上，也僅限於對電腦病毒防治的說明，除此之外，僅「南一版」在個人安全防護上，對於個人健康保健上有所涉獵，其餘大多付之闕如。

再如高中計算機概論所涉及的資訊安全內容，本研究者發現，目前僅有高職的「計算機概論二」當中的網路應用單元，出現資訊安全與保護的議題，同時所涵蓋的內容甚為狹隘且稀少，僅略微提及防火牆、密碼、資料加密解密、數位簽章等內容，且多數為教條式的陳列，此舉不僅使得教師在教學方面不知從何著手，同時也使學生對資訊安全相關議題缺乏學習動機，更遑論讓學生了解電腦使用安全以及擁有正確的使用電腦態度，準此而論，目前對資訊安全的議題日趨重視，但是在教材中對於資訊安全的介紹，卻相當地貧乏，實為目前推動資訊教育之一大缺憾。

表 2-5-1 現有資訊安全課程教材

出版社	適用年級別	資訊安全的意涵
旗立資訊	國中電腦二	泛指維護資訊系統正常運作的相關事項；例如電腦病毒的種類與防護以及電腦犯罪。
南一書局	國中電腦二	可分為硬體安全、軟體安全以及個人安全防護三點。
松崗	國中電腦二	危害資訊安全的原因以及資訊安全的防範措施如電腦病毒。
旗立	高職計算機概論二	電腦病毒、資料的加密解密、數位簽章、防火牆與防毒軟體。
金華	高職計算機概論二	防火牆、密碼、資料加密解密、數位簽章。

註：國中電腦二適用國中三年級、高職計算機概論二適用高職三年級

資料來源：本研究整理

第六節　教學設計

由於本研究的主要目的，在發展一套有關「資訊安全」的課程，最後經由實際教授的過程，檢視課程內容設計的適切性，以下將對本研究所採用的教學設計模式作一介紹。教學如同一套傳輸訊息的過程，因此在教學的過程中要不斷地加以改進與突破，張祖忻、朱純、胡頌華（1995）認為教學設計的過程有許多不同的模式，但大抵跳脫不出四個基本要素：

一、分析教學對象：即教學對象為何，並具備什麼特徵。

二、訂定教學目標：使學生在教學的過程中，能獲得哪些知識、技能或態度，並使用可供觀察、測量的行為表現來明確表述教學目標。

三、選用教學方法：如教與學的形式、媒體與活動的選擇等。

四、實施教學評量：藉此來評斷是否達到教學的目標，或作為教學修正之依據。

李宗薇（2000）在教學設計理論與模式的評析及應用的研究中，檢視許多教學設計模式，如 Heinich, Molenda & Russell 於 1982 年所提出的 ASSURE 模式以及 Dick & Carey 於 1978 年所提出的系統取向教學模式，還有 Kemp 等人 1993 年提出的環形模式，她認為教學設計模式是化繁為簡的工具，其功能的發揮將視使用者而定，每一種教學設計模式皆有其優點也有其限制，因此沒有一種所謂「最好的」模式能適用所有的情境，不同的模式適用不同特質的學習者與學習內容；本研究者在參考國內許多對資訊素養課程設計的研究之後，認為 Dick & Carey（1996）所主張的「系統化教學模式」(The systematic design of instruction)，不僅較為完備且詳盡，同時也提供教師較為明確且循序漸進的教學設計過程（林佳旺，2003；張芳綺，2002；龔裕民，2002）。在本模式中，一共包含了九個階段，分別為：確定教學目標、分析學習者、撰寫表現目標、發展標準參照測驗、

發展教學策略、發展及選擇教材、進行形成性評鑑以及總結性評量(見圖 2-6-1)。

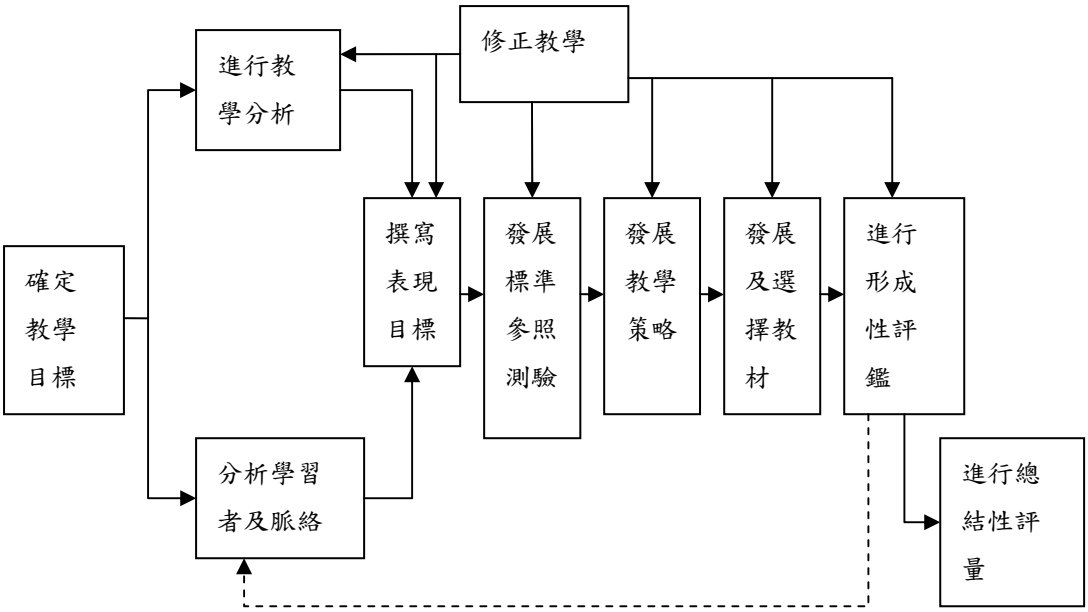


圖 2-6-1 Dick & Carey 的課程設計模式(Dick & Carey, 1996)

李宗薇(2000)提出該模式的四點特色，一是教學之前的分析工作，包括分析教學和學習者，這樣的步驟可說是一種需求性評估，經由分析的結果如果能產生或發展出新方向，那麼教學設計也須反映這種現實的需求。第二個特色在分析與教學歷程中，持續不斷地進行教學修正的工作，可以產生較好的結果。第三個特色是重視評量。有形成性評量及總結性評量，可應用到工作情境；如學習者未能在工作表現上顯示新知能，就可研判在前述的步驟未臻完善，需再做修正。第四個特色為教學目標的確定，不是由學科專家或組織機構之主管研擬，而是透過對組織任務、功能與目前狀況分析後的客觀理性決定。

盛群力、李志強(2003)認為，雖然這種「線性」設計模型近年來受到一些質疑與批評，但是該理論可以掌握住基本的教學設計程序和規範，並提供良好的基礎，同時也具有很強的實踐意義；而徐照麗(2000)以為，系統模式的應用，不論大至國家、地方或年級的整體課程規劃，或小至教師課堂較案的設計，都能夠加以應用；為期能在本研究中設計出一套適切合宜的課程規劃，因此本研究將參酌 Dick & Carey 的系統化教學設計模式進行資訊安全課程的規劃，以藉此達

成預期的教學目標。

教學設計的重點在引導教師有效的教學，而林進材（2000）在所提出的有效教學的意涵其中之一，便主張有效教學應該是多樣性的，也就是教師在教學歷程中應該使用豐富且多元化的教學活動、方法以及內容來達成預期的教學目標；而在教學的原則上，張添洲（2000）主張教材的選擇應切合學生的經驗基礎，便於學生的瞭解與接受，同時在評量上，可以採用較為多元的方式來實施。在劉玉玲（2003）對課程發展與設計的主張也提到，教師欲妥善經營課程，應該要注意以下幾點：

一、學生是主動學習並建構知識的：課程的規劃與教學的設計應重視學生的知識基礎、生活經驗與日常想法，以建立教學活動及其內容的生活關聯、社會關聯和知識的統整。

二、建立合作學習的環境：可以幫助學生積極建立良好的學習環境和避免不必要的學習干擾，而影響教室秩序。

三、教師提供創造思考機會的學習活動：學生是問題的探究者，教師在教學的過程提供適當的對話、相關補充材料及富有創造思考機會的學習活動。

四、鼓勵學生積極參與學習並養成主動探究、積極思考的學習態度。

五、採多元教學評量方式：傳統的紙筆測驗無法達成上述的學習模式，因此教學評量必須從學生的學習歷程來看，評量的重點應設定在學生知識概念的轉變與心理能力的提升。

由此可見，促進學生主動學習，並以分組合作的方式來實施活動，再配合多元評量的方式，將是目前教學設計的趨勢。據此，在教學的策略以及評量上，本研究的課程設計將參考謝淵任、周倩(2004)對中學生資訊素養課程所提出的設計理念，由下述幾點著手：

一、教學方法上：採用現有的資訊安全相關案例（如病毒對個人所造成的災害、信用卡的盜刷事件等），以貼近學生的生活經驗，並引起學生的注意與興趣。

二、教學媒體的運用：利用電腦多媒體的形式，以活潑的教學方式改善原本枯燥、死板的教學模式，同時也可以用來啟發學生的思考與討論。

三、活動的設計上：將設計生動活潑的學習活動，如遊戲的進行、小組辯論、角色扮演的方式，帶動學生的參與，讓學生在活潑的學習活動中吸收相關知識。

四、教學評量上：在每一單元的設計中，將會避免教師教條式的講述或使用傳統的紙筆測驗，而改以多元評量的方式來進行，例如實際的操作、口頭報告、成品賞析等，重視學生實際的行為表現。

綜括上述，本研究在教學設計上，將以系統化教學設計的理念為核心，不僅考量教學的對象、目標，同時在教學的策略上，將讓學生透過活動的參與，引發積極學習的動機；而在評量上，以多方蒐集學生的學習表現，並重視學生學習的過程，作為評量參照，以獲得較客觀之依據。

第三章　研究方法與實施

本章將探討本研究發展「中學生資訊安全」課程的研究步驟。以下將分為三節說明：第一節為研究的步驟與流程，第二節探討資料蒐集與分析的方法，第三節則為本研究之研究對象。

第一節　研究步驟與流程

本研究旨在發展一套「資訊安全」課程，因此課程內容的發展將是研究的首要工作。Posner & Rudnitsky（2001）認為，課程就類似一張建築藍圖，它的發展代表需要學生學習到什麼內容以達成教育的目標。本研究預計將研究流程分為六個階段，以下分別就各階段作一介紹：

一、課程內容的確立與實施理念

分析相關文獻資料，對資訊安全的意義與內涵加以確立，並歸結出「中學生資訊安全」課程所應包含的內容及教學所採行的設計模式與實施理念，以作為立論基礎。

二、需求分析以及學習者分析

研究者將藉由訪談現職的中學資訊教師，來達成研究的需求性評估，並根據專家對中學生「資訊安全」課程需要性的意見，確立教學目標並達成課程的規劃。此外將對目前的中學生發放「中學生資訊安全概念與態度」（附錄一）問卷，藉此檢視學生對資訊安全已有概念、知識與態度，獲得學習者具備的起點能力。

三、設計表現目標

由前述需求性的評估以及教學目標的確立，便可完成學習單元的設計，並撰寫學習者在此單元中的表現目標。

四、發展教材與教學策略

在本課程中的表現目標撰寫完成後，選擇合適的教學策略並設計適當的教學活動，以利學生對該課程內容的學習。

五、實施形成性評鑑

歐用生(1999)表示，課程的評鑑主要依循三個標準，分別為實施的可能性、方案的成效以及對學生是否有教育上的價值，而形成性評量（formative evaluation）的實施，是一種過程評價，目的是為了在教學歷程中改進教學並提高學習效果（施良方，1997；郭生玉，2000）；為能檢視本課程發展的可行性以及實施成效，同時也可以對課程有所改善與修訂的機會，本研究者將以發展之課程進行教學演示，並在教學完成後，對受教班級學生發放「課後意見調查表」(附錄二）問卷，以檢視學生對本課程的反應；此外，透過學者專家發放「專家評估調查表」(附錄三)，藉此獲得專家對該課程的意見，為本課程提供良好的修正與回饋。

六、結論與建議的提出

本研究者將藉由課程發展的歷程，以及課程評鑑的結果，提出本研究的結論與建議，瞭解本研究是否達成預設目的，及檢討反省此執行狀況和可改進的空間。本研究所採的研究流程，見圖 3-1-1。

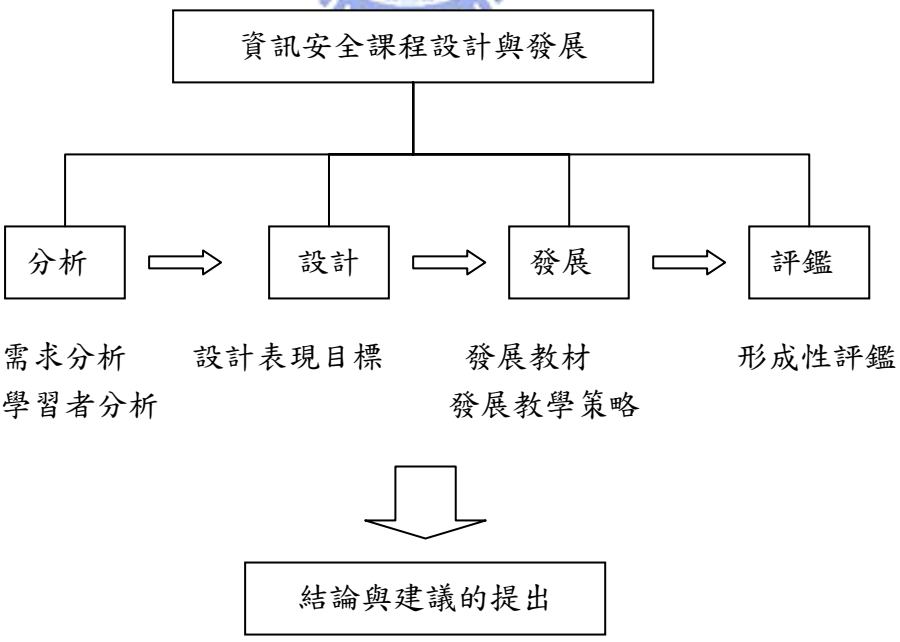


圖 3-1-1 本研究之研究流程

第二節　資料蒐集與分析的方法

本研究所採用的研究方式，除了採質化的觀察與訪談之外，也同時以量化的問卷調查方式來蒐集資料，期能對研究的發展有一客觀公正的標準。因此本節將說明資料蒐集的方式與分析過程。

一、資料的蒐集

（一）訪談法

在研究發展之初，為了解本課程設計之需求，研究者將針對五位在中學任教的資訊教師進行訪談，以了解本課程是否有其需求以及重要性。黃光雄、簡茂發（2000）表示，訪談的方式具有彈性以及可以獲得較佳、較為深入的第一手資料等優點，在被訪問者不了解問題時，調查者可以重述問題，以控制訪問的情境。本研究者蒐集資料所採取的步驟分別為：

1. 選取訪問對象：對象的選擇以具有代表性的訪問對象為主，本研究所探討的資訊安全議題，跟中學的資訊教師有較密切的關連，因此訪問的對象選定如擔任中學的資訊教師或系統管理師等人員。
2. 編制訪問表：研究者將採「半結構訪問」（semi-structured interview）的方式來進行，這種方式可以兼具結構與無結構訪問的優點（吳明清，2001），以下為研究者自擬的訪談大綱：

（1）從您的認知與角度來看，通常所謂的「資訊安全」所指為何？現有的資訊課程當中需要設計一套這類的課程嗎？如需要，約需多少時間？

（2）您認為「資訊安全」的課程當中，應該包含哪些相關的議題？如電腦病毒、駭客、垃圾信件、謠言等？

（3）目前學生對這類的知識是否充足，有需要加強或補充之處？

（4）學生的資訊能力與資訊安全的認知上是否有差異？

（5）目前課程當中較為迫切需要但卻缺乏的內容？

（6）建議該如何發展以及教授這類的課程，例如從教學活動上的進行或課程設計發展最能引起學生的興趣？

（7）教師對於課程有什麼樣的期許？

3. 訂定訪問行程：事先規劃訪問行程，將受訪者與訪問日期、時間作適當的安排與調配，使訪問工作得以順利進行。

4. 進行訪談：研究者拜訪受訪者，訪談的過程，均以錄音機記錄，並謄成逐字稿供分析之用。

（二）觀察法

研究者在教學過程中，也將進行教室的觀察，注意學生對教學的反應情形，此外，對上課情形全程錄影，利於事後對課程的進行加以分析比較，獲得較為全面的資料比對成效。

（三）問卷調查法

除了前述的訪談方式，本研究同時也採問卷調查的方式，使用的問卷為研究者自編之「中學生資訊安全概念與態度調查表」，對一般中學生進行學生起點知識與態度的調查，此外，在課程實施結束後對受教學生發放「課後意見調查表」，檢視參加本研究的學生，在課程結束後的看法與意見；最後，並對專家學者進行「專家評估調查表」的發放，藉由專家在評估表上的反應，對本課程提出相關的建議與改善。以下分別介紹此三種問卷。

1.「中學生資訊安全概念與態度調查表」：本問卷的目的在調查一般中學生在過去學習的資訊課程中，是否具備對資訊安全的基本知識，同時也調查學生對資訊安全有關的態度。

（1）研究問題：中學生對「資訊安全」的起點知識與態度為何？

（2）研究實施：問卷的發放以便利取樣為主，但盡量做到國高中及區域之平衡，研究者將對目前的國高中生，進行問卷的發放；同時對接受課程教學的學生，實施前後測的比較，以檢視學生們在經過此次課程之後，對資訊安全的認知及素養是否有實質的提升。

（3）問卷的編制：內容共分為三部分，第一部份為學生的背景資料，包括了性別、年級別、家中有無電腦、每週使用的電腦時數、上網的地點、上網的主要活動以及是否遭遇過電腦病毒或駭客的經驗等七項；第二部分則為學生對資訊安全的一些基本能力調查，題目的題型則包括是非、選擇以及問答等三種方式，內容涵蓋「電腦網路通訊安全」、「資訊的適切性」以及「個人保健」等三個主要議題共 36 題（附錄一），以下說明此三個議題：

a. 電腦網路通訊安全：在這一部份所強調的為學生對電腦網路使用上的安全認知，例如對電腦病毒與駭客的認識程度，以及相關防範措施，共 16 題。

b. 資訊的適切性：此處包括資訊的正確性、合理使用性以及個人資訊保護的了解，例如對網路謠言的認識、垃圾信件的防範以及在網路上洩漏個人資料等能力的調查，共 15 題。

c. 個人保健：題目的內容包括使用電腦所可能產生的傷害，例如對身體健康產生的影響，以及如何預防相關傷害的認知，共 5 題。

第三部份則針對學生對資訊安全的態度調查（附錄一），用來確認學生對資訊安全的態度調查，答題的方式為李克特式（Likert）四點式量表，共 22 題，分別為非常同意、同意、不同意以及非常不同意四個選項。

2.「課後意見調查表」：為研究者自編，對象是本研究受教學生在課程結束後所填寫對本課程的反應情形，問卷一共包括三部份，分別是有關課程內容、學生的學習以及綜合評價等三方面，答題的方式也採李克特式（Likert）四點式量表，分為非常同意、同意、不同意以及非常不同意四個等級，並加入一題開放式問題，供學生自由作答。

3.「專家評估調查表」：為課程設計完成後，本研究者對學科內容與課程設計專家所做的調查，期能對本課程的發展提供相關的建議，作為本研究者改善課程的方向與參考，答題的方式採李克特（Likert）五點式量表，分為非常同

意、同意、中立意見、不同意以及非常不同意等五個等級，同時加入一題開放性的問題，請專家提供對課程上的建議。

4. 問卷效度：在本研究中，由研究者自行發展之問卷，為提升問卷的內容效度，研究者在設計完成後，將請指導教授以及在需求評估階段所訪問的教師檢視，求取專家效度，並根據所提出的相關建議與回饋，進行問卷的修改與調整，以期研究工具能趨於完善。

二、資料的分析

（一）訪談法：針對訪談對象訪問的內容，研究者在事後將整理成逐字稿，作為分析之依據，同時在完成逐字稿後也請受訪者閱讀，對其加以修正以接近受訪者的原意。

（二）問卷調查法：本研究中一共使用三種問卷，第一份問卷為「中學生資訊安全概念與態度」調查表，研究者在問卷回收後，除了檢視學生所具備的資訊安全概念外，也將對不同學生特性與學生在資訊安全的概念與態度上做相關以及差異性的比較，同時在課程完成後，對參與課程的學生實施後測，進行成對樣本 t 檢定，檢視前後測是否有差異；此外，在「課後意見調查表」上，將所蒐集到的資料作百分比、平均數以及標準差的統計描述，以分析學生在對本課程的滿意度以及學生對課程的建議；至於在「專家評估表」的部份，研究者也將對所蒐集到的資料做簡單的描述統計，分析專家對本課程的反應與相關意見。

第三節　研究對象

本研究的研究對象，主要可分為訪談對象、問卷施測對象以及參加本研究課程教學等三種對象，以下分別介紹這三種研究對象。

一、訪談對象

本研究在評估需求的階段，將針對目前任教於中學的資訊教師以及資訊組長進行訪談，表 3-3-1 為研究者進行訪談之日期與受訪對象之基本資料。

表 3-3-1 訪談對象的背景資料

編號	職稱	性別	經歷（年）	訪問日期
A01	新竹市建功高中資訊教師	女	國高中教師 8 年 高中教務主任 2 年	93.2.19
A02	國立新竹高中資訊組長	男	高中教師 4 年	93.3.18
A03	國立中壢高商資訊教師	女	高職教師 7 年	93.3.24
A04	台北市立大同高中系統管理師	男	高中教師 7 年	93.3.30
A05	新竹市建功高中資訊教師	男	高中職教師 5 年	93.05.21

二、問卷施測對象

本研究中使用的三種問卷，分別為「中學生資訊安全概念與態度」調查表、「學生課程意見」調查表以及「專家評估」調查表三種工具。在「中學生資訊安全概念與態度」調查表的施測的對象，為目前就讀於國高中之學生，在現行教育政策的推動之下，多數的國高中生已經接受過相當時數的資訊課程教學，並具備一定的資訊操作與認知能力，因此本研究者將對台北、新竹、台中、屏東等四個地區的國高中生，一共十個班級，發出 398 份問卷，調查現有中學生對資訊安全的概念與態度。在「課後意見」調查表上，主要是針對在研究中參與教學課程的國高中生，一共三個班級來進行調查。至於在「專家評估」調查表上，本研究者主要以四位在學科內容、課程設計以及教學經驗豐富的學者專家為調查對象，表

3-3-2 為本研究中受訪的專家，獲得的結果將作為檢討本研究在課程設計上的修改依據。

表 3-3-2 專家評鑑的受訪者與背景資料

代號	專長	背景
E1	網路學習、電腦輔助學習、教學媒體、教育傳播	國立交通大學教育研究所教授 教育工學博士
E2	數位學習課程設計與評估、網路學習社群	國立交通大學教育研究所助理教授 資訊科學與學習科技博士
E3	資訊教育	新竹縣自強國中教師
E4	資訊教育	新竹市建功高中資訊教師
E5	資訊教育	台北縣五股國中資訊教師

三、課程實施班級

研究者受限於能力以及便利性上的考量，以新竹市建功高中以及台北市大同高中的三個班級為課程實施之對象，並利用班級的電腦課來進行教學，教授的單元以及教學的日期分別如表 3-3-3 所示。本研究者在大同高中進行的課程為「網路安全ｅ起來」以及「電腦健康百分百」，使用的時間各為一節課；至於在建功國中，則分別針對兩個不同班級進行「網路逍遙遊」以及「個人資料不露白」兩個單元的教學，使用的時間也維持在一節課。

表 3-3-3 課程實施對象

教學日期	學校	年級別	班級人數	教學節數	教學單元
93.06.08	台北市大同高中	高一	40	1	「網路安全e起來」、「電腦健康百分百」
93.06.23	新竹市建功國中	國一	39	1	「網路逍遙遊」
93.06.24	新竹市建功國中	國一	33	1	「個人資料不漏白」

第四章　研究結果與討論

本章主要探討研究過程中資料蒐集的分析與討論，以及根據資料分析的結果，進行課程發展的過程。一共分為三節來說明，分別是第一節的分析階段，進行需求性的分析以及學生起點能力的調查，第二節為課程的設計與發展，第三節則為課程的評鑑階段。

第一節　分析階段

一、需求分析

研究者訪談五位現職中學教師，進行課程需求性的評估，根據訪談內容的分析，主要分為「資訊安全意涵的詮釋」、「學生具備的知能」以及「對課程的建議」三方面來說明：

（一）資訊安全意涵的詮釋

訪談結果發現，每位教師對資訊安全之定義有不同的看法，對課程所應包含的內容也有差異。根據受訪過程的分析發現，不同的受訪者，對資訊安全的內涵，可以從許多不同的觀點去切入，但多數都表示，資訊安全與電腦硬體或是電腦系統上有很大的關聯，而這也是一般人認知中的資訊安全，可見資訊安全的內涵在電腦網路通訊上是息息相關的；再加以深入探討，資訊安全又可以分為一般的使用者跟管理者兩方面來加以說明；此外對於課程上的需求，多數的教師都傾向應該要包含這樣的一類課程，因為他們認為現有的資訊課程，內容有所不足，由此也可以發現多數資訊教師已經逐漸意識到資訊安全的需求與重要性。不過仍有一位受訪教師表示，資訊安全在現有的課程已約略提到相關資訊，因此沒有設計新課程的需要。

那資訊安全就是一個，電腦使用安全…這個是比較硬體部分的，就是說你看得到摸得到，還有比較能夠有具體概念的東西；然後另外一個是在核心能力的部分，比如說應該要怎樣保護自己，不要因爲網路而受到傷害，健康的概念也算，因爲那是身體

的…，像瞭解與實踐資訊倫理這個也是…然後另外一個是你心理上的安全。（受訪者 A01）

資訊安全…現在我們在做的資訊安全定義的話，第一個是不當的資訊，例如色情的防制…，第二個就是 e-mail 垃圾信件的處理，那第三個就是病毒啦…是不是需要，我覺得是需要啦！（受訪者 A02）

資訊安全的課程的話，我是覺得不需要再去有關這方面的課程，因爲現有的課程裡面都已經有了。（受訪者 A03）

第一個部份就是說個人隱私的保護，第二個就是…校務行政系統的一些資料，第三個部份大概就是說因爲現在有很多的不當資訊…那甚至交友的部份，那我想這個可能也可以把它列爲資訊安全的範圍的一部份，第四個部份就是說我們在資訊安全的過程當中…一些簡單文件的安全性，第五個層次就是說，現在很多學生在密碼的控管上，會有一些問題，那第六個部份，我是覺得說現在學生他們在使用電腦的時候，最常碰到的就是有關病毒的問題，大概可以分爲這六個部份，那我覺得現有的課程當中，是非常需要這類的說明跟這類的介紹，但是目前現有的課程這個部份是幾乎都沒有…我覺得你在切這些問題的時後，應該可以分成兩個層面就是資訊管理者跟一般 user。（受訪者 A04）

我個人的認知是兩個層面的問題，一個是使用者的習慣，因爲通常有許多的問題，是由使用者的習慣所造成的，那另外一個就是管理跟預防，對於這樣的一類課程我是覺得有需要！像我自己也有在上資訊安全的課程。（受訪者 A05）

（二）學生所具備的知能

1. 對資訊安全的知識

對於學生擁有的資訊安全相關知識上，多數的受訪者認為學生在這方面知識懂得很有限，而且，由於目前各校或各地區重視資訊教育的情形不一，也造成學生在能力上有很大的落差；此外，許多教師自己本身對相關的知識也不是很充足，所以在進行這方面的教學時候，甚至不知從何下手。

學生知識不完全很充足，而且經常會因爲知識不足造成錯誤的判斷，學生的起點能力差很多，像國小上來，電腦的基本能力差很多…而且老師方面也不太有人瞭解，不要說國小，連國中都很少有人瞭解，老師自己都很不清楚…。（受訪者 A01）

現在學生的資訊能力差異很大，甚至我有一些學生，他可以破解學校的行政電腦系統…他有這個能力去玩，把它當成一種挑戰…。（受訪者 A02）

我是覺得很不足，尤其很多學生在這方面的概念是相當弱，從電腦教室的管理或者是公用電腦的管理，可以發現到很多這種問題，不是只有學生而已，老師也是一樣…

有些學生資訊能力好的，他甚至可以當起駭客。（受訪者 A04）

…資訊安全相關的知識，學生知道的還是很有限，大部分的學生都是習慣操作，不喜歡維護。（受訪者 A05）

2. 學生在能力上與認知的差異

對學生在資訊能力跟資訊安全的認知上，有些受訪者表示，學生即使在資訊能力很不錯，但是對於資訊安全的概念卻有待加強，因為能力好的，這方面卻未必有很正確的認知或警覺，或者學生即使有相關的認知，但在能上卻不足；還有受訪者表示，認知跟能力間其實是沒有很大的相關性，因為很多學生即使知道這樣不好，可是仍然會抵不住一些外在的誘惑，所以這兩方面沒什麼太大的關係。此外，受訪者教師也提到另一個問題，那就是目前在資訊教育的課程中，一直很難扭轉學生對電腦的看法，因為學生一向把電腦當成是玩樂的東西，而不是將它視為是用來進行學習的工具，而這也是在推動資訊教育仍需持續努力的地方。

那資訊能力跟認知上面是不是有差異呢？我認爲有啦!（受訪者 A02）

即使他知道這樣有危險，他還是會去做，像個人資料外洩，學生當然知道會有怎樣的後果…可是你說這種情況，你要怎麼預防，無法預防啊！…所以即使你有那個認知，可是當比較有誘惑性的行爲或是東西出現的時候，他可能還是大於你的認知；所以這時候即使學生有認知也很難。所以我覺得認知跟行爲之間沒有太大關聯。（受訪者 A03）

…學生的認知跟能力上，當然是有很大的差異…像我自己有帶社團，學生參加社團的第一個目標就是要破解人家電腦，要入侵，有啦!他當然知道不對啦!可是他還是很喜歡去做!（受訪者 A04）

如果你心智發展不成熟，比方說國中生，通常會變成很糟糕的局面…幾乎所有的資訊課程都有一個共同的問題，就是學生學習意願很低，除非你壓的住他們，那很低的原因是他們從小養成習慣電腦是拿來玩的…我會認爲說，就像剛開始的問題，他們在資訊方面的認知還好，可是他們的能力還不夠。（受訪者 A05）

（三）對課程的建議

1. 課程中較為迫切需要的內容

根據訪談的內容顯示，不同的受訪者對於課程中較為迫切安排的內容也有不同的需求，可能是因為每位教師所接觸的學生族群不同，有些學生對象是國中

生，有些則是高中生，而不同的區域，也有可能存在某種差異，不過受訪者除了提到本研究在前述提及的三個面向之外，還提出其他需要教導的觀念，例如法律、購物上以及交友方面，這些都是目前教師認為相當重要而且應該安排在課程中的內容。

我覺得應該是對電腦一個正確的概念…現在比較缺的可能類似網路社會，怎樣跟網路裡面的人作人際溝通、互動、怎樣去判斷它的對或錯…，或是網路交友，可能是比較迫切的…像謠言這個部分就是蠻需要的，很多人會信以為真…然後接著就演變出垃圾信件的問題，…這是比較缺的…還有跟資訊相關的法律部分，可是現在的國中生似乎也不是那麼清楚。（受訪者 A01）

目前課程是否有迫切或缺乏的內容，大概就是 e-mail 的部分跟電腦中毒的部分，大概就是他們比較會使用的…。（受訪者 A02）

目前比較缺乏的，就是我剛剛提的那六點，我覺得應該都可以把它一併的加進來，那加進來之後我覺的說如果你有一個基本學理的介紹，可以強化學生這方面的能力…那包含一些尊重智慧財產權或者尊重個人隱私，這些都可以一併考慮…另外一個就是說，對學生比較常碰到就是說現在網路消費很多，就是一個安全的網路消費行為，這可能是一個將來會常碰到的一些問題。（受訪者 A04）

…我會覺得第三個部分比較重要，就是個人安全的部分，主要是學生對這方面比較欠缺，而且最主要是學生不一定聽的下去…另外還有一個就是說，現在很流行的就是網路購物，像網路購物、拍賣，其實在資訊教育部份，我們特別擔心的是網路安全，這網路安全有一個很嚴重的問題就是說，現在青少年流行網路交友…這個東西都是你要花時間去跟他們溝通。（受訪者 A05）

2. 對於發展這類課程的建議

在發展課程的建議上，幾乎所有的受訪者都認為設計活動來帶學生進行的方式，比較可以引起他們的學習興趣，如果加上可以讓學生來實地演練，並讓學生可以在競爭的情境之下，比較能有參與感，這樣的預期效果可能比較大；此外，多運用生活實例的方式，讓學生來探討或瞭解，也可以使學生有較貼近自己生活經驗的感覺，因此對於相關新聞案例的蒐集與整理，也是課程發展的過程中，所不可或缺的必備工作。另外，在課程時間的安排上，受訪教師認為設計這樣一套的課程，時間的安排上不要太長，才不會擠壓到其他的上課內容，所以在課程時間的設計上不宜過長，每單元以一至二小時為限。

…可能是作遊戲或活動競賽，…要找出跟他生活很有關係的，可能就是他身邊發生的一些例子，從那個地方去上課，或者是用競賽叫他們比賽…（受訪者 A01）

我的建議是可能的話設計一個小時到兩個小時，那一個小時到兩個小時的話，其實大慨就是去針對某一個向度…。（受訪者 A02）

其實網路上的案例還真的蠻多的，…你講這些案例的時候，他會覺得比較新奇，多一些案例還是比較吸引人，他會覺得比較有趣，我相信而且非常肯定這在引起學生興趣啊…。（受訪者 A03）

那我覺得這些課程的設計上面當然是以教學活動設計，用活動式的方式，比較可以引起學生的興趣，這是一個，另一個可能就是平常可能就要把這些內容納進來，就比如說學生交的作業它一些檔案的規範，平常就是要要求等等…你可以用一些活動討論甚至可以作一些簡單的遊戲，讓學生對這樣的議題有更深入的認識…課程所需的時間，應該用兩個小時來介紹是差不多，十個百分比左右，佔一成的時間應該是足夠。（受訪者 A04）

課程的設計方面，最好的方式就是給他們看實例，…然後還是要讓他們動手去做;另外,教學活動設計方面…設計搶答這一類的活動他們會有興趣,要不然就是說…像辯論，像網路安全跟網路交友都可以有正反兩方面的辯論，給他們分組、編組…。（受訪者 A05）

根據以上訪談內容的結果，可以歸納出幾點結論：

1. 資訊安全的範圍：每位教師的取向都不太一致，有的教師較偏向技術取向，有的老師可以兼顧科技與人文，還有老師是以實用為取向，或是偏人文關懷取向，可見，資訊安全涵蓋了許多不同的面向，不論是技術面或心理認知層面都包括在其中，也證明了安全的需求與我們的生活息息相關。此外，許多受訪教師會提到資訊安全跟一般的使用者以及管理者兩方面,因此要對資訊安全有效的掌握，應該是使用者跟管理者雙管齊下才能兼顧各方面的需求。
2. 目前最迫切需要的課程：由於老師的學生群體不同，所以在課程上會有不同的偏重。不過研究者發現，除了本研究所整理的電腦網路通訊安全、資訊的合宜性以及個人安全等三方面的需求之外，對於交友、法律或網路購物等議題，也是需要發展的課程內容，然而本研究者受限於自身能力，以及時間規劃上的限制，因此在本研究中，只能針對前述提及的三個面向來進行課程的規劃。
3. 教師本身所具備的知識：本次受訪教師表示，有時候連老師自己本身都不清楚許多資訊安全的知識，更遑論教導學生來保護自己，可見目前教師對這方面的

知識也有加強的需要，才能在課堂上導入學生正確的觀念。

4. 學生的資訊能力：由於資訊教育目前在九年一貫課程中屬於六大議題之一，不同的學校、地區，也會有不同的重視程度與教學取向，因此學生自國小畢業升入中學之後，能力間的落差會逐漸出現，這點也是相當值得加以正視的問題。

5. 學生的資訊能力與資訊安全的認知：誠如許多老師所提到的，學生的資訊能力強，對於應有的安全認知卻沒有同步的成長，可見過去在資訊教育的教學過程，可能較著重於資訊能力的訓練，卻忽略了在道德安全上基本認知的培養，讓學生即使可以輕易在電腦網路中穿梭，卻不曉得自己的行為其實是不安全不適當的，甚至有可能是違法的。

6. 對課程設計的建議：根據受訪的教師表示，設計活動讓學生來參與，或是透過競賽的方式來實施，可以引起學生很大的興趣。此外，多運用實例的融入，也可以讓學生覺得貼近自己的生活經驗，因而從中學到教訓，可能會有較佳的學習成效。

二、學習者分析

針對學習者起點能力的分析，本研究者以自編的「中學生資訊安全概念與態度量表」來進行調查，研究的對象為台北、新竹、台中以及屏東等四個地區的國高中生，其中台北市的大同、新竹市的建功以及台中市的惠文高中，三所學校皆為完全中學，所發出問卷的數量與地區之分配見表 4-1-1。本研究一共發出 398 份問卷，回收 375 份，回收率為 94.22%，剔除無效問卷份 42 份，共 333 份有效問卷。

在本研究的受訪學生中，國高中生以及男女生的比例大致相同，國中生佔了 51.2%，高中生則佔了 48.8%，在性別的比例上，男生佔了 46.8%，女生則為 52.6%；受訪對象家中有電腦的比率相當高，為 88.6%，可見電腦的普及化，幾乎已經是家中基本配備；而學生曾經遭遇過電腦病毒以及駭客的經驗，則為 45.4%，見表 4-1-2a，也就是有將近一半的學生表示曾經有電腦病毒或駭客騷

擾的遭遇，這或許也是電腦普遍、平民化所產生的結果，至於學生每週花在使用電腦的時間，則大約在 12 個小時左右，表 4-1-2b。

表 4-1-1 問卷發放情形一覽表

發放地區	學校名稱	發放份數	回收份數	回收率（%）	廢卷	人數比率（%）
屏東	恆春工商	40	39	97.5	7	20.7
	恆春國中	41	41	100.0	4	
新竹	新竹建功高中	80	80	100.0	22	38.1
	建功國中部	76	73	96.0	4	
台中	台中惠文高中	40	31	77.5	0	18.6
	惠文國中部	40	36	90.0	5	
台北	台北大同高中	41	41	100.0	0	22.5
	大同國中部	40	34	85.0	0	
總計		398	375	94.2	42	100.0

表 4-1-2a 受訪學生背景描述

背景	類別	人數	百分比(%)
年級別	國中	170	51.2
	高中	162	48.8
性別	男	156	46.8
	女	175	52.6
家中有無電腦	有	295	88.6
	無	34	10.2
有無遭遇電腦病毒或駭客的經驗	有	142	45.4
	無	171	54.6

表 4-1-2b 受訪學生每週上網時數

每週上網時數	平均數	標準差	最大值	最小值
	12.96	22.59	99	0

三、研究結果與討論

由於本研究所使用的工具「中學生資訊安全概念與態度調查表」，除了受訪者的背景資料外，還分為兩部份，一部份為學生對於資訊安全的起點能力調查，另一部分則為學生對資訊安全的態度，以下將依照此二部份來討論。

（一）學生資訊安全概念

在資訊安全概念中，研究者所欲探討的是學生是否具備對資訊安全的基本概念，亦即檢視學生對基本的資訊安全知識的瞭解程度，以確認學生起點能力，雖然在問題類型中包括了開放式問答題，但由於受試者漏答過多，因此不列入分析之考慮，以下主要分析有幾點：

1.試題的難度

所提到的難度分析的是指每個題目的難度，根據郭生玉（2000）表示，就實用觀點來說，難度用正確答對該試題人數的百分比作為指標是適當的，該百分比稱為「難度指數」(item difficulty index)，其公式為 P＝R/N，其中 P 為項目的通過率，而 R 則為答對該題的人數，N 為所有參與測驗的人數，其數值愈大，表示題目愈容易，數值愈小，題目就愈難。所獲得的各題難度見表 4-1-3。

由表 4-1-3 可發現 33 題之難度介於.90 到.08 之間，難度在.70 以上的題目有十七題，所佔比率為 51.51%，難度在.3 至.7 中間的題目共有十二題，所佔比率為 36.36%，至於在.3 以下的，則共有 4 題，分別為第 3 題，其難度為.25，第 27 題，難度為.15，以及第 32 題，難度為.08，與第 33 題，難度為.13，4 題佔總題數的比率為 12.12%，表示這些題目對於受試者來說過難，學生幾乎完全不知道有關這方面的資訊；一般對試題難度的 P 值，以.50 者為佳，然而不可能找到所有題目的 P 值都接近.50，因此有的學者主張以.40 到.70 範圍為選擇題的選擇標準，亦有學者主張以.30 到.70 為試題難易適中的標準，本研究的試題，難度在.70 以上佔 50%以上，而在.3 以上的則總共佔了 87%左右，可見試題的難度偏易（余民寧，1998；郭生玉，2000；葉儒智，1998）。

表 4-1-3 各項目的難度

試題內容	答對率（%）
1.電腦一旦安裝防毒軟體後，就不會中毒。(x)	90.4
2.發現電腦中毒應立即關閉電源，尋求解毒的方法，這樣可以防止病毒繼續破壞。（○）	51.5
3.電腦病毒與電腦蠕蟲其實是指同一種惡意的電腦程式。(x)	25.8
4.駭客原本被定義為「一群高度熱中於寫程式的人」，他們相信透過軟體之間的分享，可以促進資訊與資源的快速流通。(○)	51.4
5.個人重要檔案應加密保護，以防他人偷窺或竄改。(○)	94.0
6.防護性較差的電腦，有可能會變成駭客入侵其他機器的跳板，這樣入侵者可以迴避自身責任。(○)	57.8
7.我國為推動電子化政府，建置政府憑證管理中心（GCA)，一般民眾必須從網路下載數位簽章的製作軟體。(○)	73.5
8.數位簽章製作軟體會產生兩個金鑰，公開金鑰是使用者自己保管，私密金鑰是在外流通。(x)	68.8
9.公開金鑰基礎建設（PKI）是以「密碼學」為基礎的安全技術，可以確保資訊在網路作業中不被竊取或盜用。(○)	78.1
10.網路連線安全機制如 SSL，通常具備了私密性與完整性的功能，但無法做到身份的驗證。(○)	59.6
11.「謠言」通常是指未經加以證實的事物，為了避免聽信不實的網路謠言，應該要對網路上的消息加以懷疑。(○)	74.2
12.因為討厭某位老師，故意在網路上散佈有關他的不實言論，這樣的行為並不會違法。(x)	88.9
13.將個人常使用的信箱與公開或註冊用的信箱作區隔，可以有效的防範一些廣告信件的發生。(○)	80.8
14.使用郵件規則或者過濾軟體，可以有效的防範垃圾信件，但也有可能會漏收了自己親朋好友所寄來的信件。(○)	72.3
15.網路是一個虛擬的世界，只要我不使用真實姓名，應該沒人知道我在作什麼。(x)	82.9
16.網站上的隱私保護政策的作用，主要是在保護該網站的隱私安全。(○)	75.0
17.cookies 中譯「網路餅乾」，通常會蒐集有關登入該網站使用者的資訊，同時也會使個人與網站的互動更為密切。(○)	75.6
18.密碼的設定要以簡單好記為原則，所以個人出生年月或是家裡電話是設定密碼的最佳來源。(x)	72.3
19.印表機只是用來列印文件，不太可能對個人的健康產生影響。(x)	69.1
20.電腦的螢幕，應該擺在臉部的右前方，這樣正前方可以放置所需的東西，方便電腦的操作，也讓眼睛跟電腦螢幕保持適當距離。(x)	46.8

試題內容	答對率（%）
21.「電腦駭客」通常是指下列哪種人？（非法入侵電腦系統的人）	83.0
22.電腦病毒的傳染途徑，可經由許多方式來達成，但以下何者為非？（使用者沒有保持個人衛生習慣）	82.3
23.電腦中毒後所可能造成的情形有很多，以下何者為非？（電源供應器燒壞）	83.4
24.關於防制電腦駭客與病毒的方式，以下何者有誤？（不要將電腦連上網路）	66.3
25.要對網路上的消息有所確認，通常有幾種方式，但下列選項何者為非？（不斷轉發，讓其他人來判斷真偽）	57.5
26.網路上的謠言之所以能夠大量的散佈，除了網路訊息散佈快速的特性之外，主要還具備了什麼要素？（可能會發生、跟現實有關、恐懼感）	79.3
27.大量的廣告信，不只會讓個人產生困擾，還可能產生許多影響，但何者不是可能產生的結果？（電腦病毒橫行）	15.1
28.要防止不要的廣告信件，通常可採取幾種方式，以下何者有誤？（回覆信件，表示不想再收到類似消息）	52.6
29.在網路上常見的個人資料外洩，通常有幾種方式？（註冊、cookies、算命或贈品）	77.8
30.在網路上洩漏個人資料，將會導致許多情形發生，但下列何者有誤？（增加中獎機率）	70.1
31.電腦可能透過哪些部分影響個人健康？（螢幕、鍵盤、滑鼠）	41.4
32.傳統電腦螢幕（CRT）輻射線最強的地方是哪一區？我們應該盡量避免在該區域工作。(正後方)	8.5
33.下列何者是代表電腦螢幕的安全標準？（TCO）	13.0

2.學生具備的資訊安全概念

「資訊安全概念量表」所調查的是學生對資訊安全概念的基本知識，研究者將資訊安全的項目分為三個面向，分別為「電腦網路通訊安全」、「資訊的適切性」以及「個人保健」等，總題數為 33 題，答對一題以一分計算，受訪者在三個面向所獲得的答對率分別為 68.9%、69.7%以及 36.0%，整體答對率則為 58.2%，受訪者在個人保健的答對率有明顯的偏低，見表 4-1-4。

表 4-1-4 資訊安全概念量表反應情形

	問卷總題數（33 題）	電腦網路通訊（14 題）	資訊適切性（14 題）	個人保健（5 題）

有效人數	309	323	329	319
答對率（%）	58.2	68.9	69.7	36.0
平均分數	21.7	9.7	9.6	1.8
標準差	4.7	2.3	2.5	0.9

3.家裡有無電腦的學生在資訊安全概念量表成績上的比較

根據 t-test 的結果，家中有無電腦的學生，在資訊安全概念的得分上有顯著的差異，家中有電腦的學生在資訊安全概念的平均得分顯著高於家中沒電腦的學生（t=6.7，p=.000），見表 4-1-5。

4.有無遭遇電腦病毒或駭客的經驗在資訊安全概念量表成績上的比較

根據 t-test 的結果，是否曾遭遇過電腦病毒或駭客的人在資訊安全概念量表上的得分有顯著差異，由表 4-1-5 可看出有經歷過電腦病毒或駭客的經驗在資訊安全概念量表上的得分顯著高於沒有經驗的學生（t=3.4，p=.001）。

表 4-1-5 有無電腦與有無遭遇病毒駭客在安全概念量表 t 檢定

	組別	平均分數	標準差	T值
家中電腦	1（有）	21.70	4.33	6.7***
	0（無）	16.28	4.29	
病毒與駭客	1（有）	22.03	4.44	3.4**
	0（無）	20.15	4.76	

***p<.001

5.家裡有無電腦與有無遭遇電腦病毒或駭客的經驗的獨立性考驗

根據卡方考驗的結果，家中有無電腦的比例為 89.3%跟 10.7%，而有無遭遇電腦病毒或駭客的經驗的比例為 45.4%與 54.6%，兩個變項所構成的列聯表達顯著水準（X^2 (1)=6.99，p=.008<.01），表示兩個變項之間有顯著的關聯性存在，見表 4-1-6。

表 4-1-6 有無電腦與有無遭遇病毒駭客之獨立性考驗摘要表

變項	類別	百分比（%）	X^2 數值	自由度
有無電腦	有	89.3	6.99*	1
	無	10.7		
有無經驗	有	45.4		
	無	54.6		

*P<.01 **p<.001

6.不同區域在資訊安全概念成績上的比較

由於本研究的施測對象，一共有台北、新竹、台中以及屏東等四個不同區域，根據單因子變異數（ANOVA）分析的結果，組間效果達顯著，見表 4-1-7，表示不同的地區在資訊安全概念的得分確有差異。進行事後比較的結果（採 Scheffe 法），顯示屏東在得分上顯著低於其他地區，至於台北、新竹、台中三個地區之間，並沒有顯著的差異性。

表 4-1-7 不同區域在資訊安全概念上之單因子變異數分析摘要表

變異來源	SS	df	MS	F
組間	1014.07	3	338.02	18.15***
組內	5680.36	305	18.62	
全體	6694.43	308		

***p<.001

（二）學生對資訊安全的態度

本量表所要探討的是學生對資訊安全的態度，所採的為 Likert 四點量表，採 1 到 4 計分，依序為非常不同意、不同意、同意以及非常同意，總題數為 22 題，量表的得分越高代表受訪者對資訊安全越有警覺，也較為重視，在此所要討論的主題有下述幾點：

1.不同區域對資訊安全的態度比較

研究者以四個不同區域在資訊安全的態度量表下的比較，根據單因子變異數分析的結果，組間效果達顯著，見表 4-1-8。事後比較的結果，發現新竹顯著低

於其他三個地區。

表 4-1-8 不同區域在資訊安全態度上之單因子變異數分析摘要表

變異來源	SS	Df	MS	F
組間	1.88	3	.63	5.61*
組內	33.01	296	.11	
全體	34.88	299		

*p＜.05

2.有無電腦在態度上的差異

受訪者家中有無電腦在態度量表上的比較上，t-test 檢驗的結果發現，家中有電腦的學生與沒電腦的學生在得分上有顯著差異（t＝2.61,p＝.01），見表 4-1-9。

表 4-1-9 有無電腦與有無遭遇病毒駭客在安全概念量表 t 檢定

	組別	平均分數	標準差	t值
家中電腦	1（有）	3.04	.33	2.61*
	0（無）	2.87	.38	
病毒與駭客	1（有）	3.06	.33	2.14*
	0（無）	2.98	.35	

*P<.05

3.有無遭遇病毒與駭客的經驗與資訊安全的態度上是否有差異

表 4-1-10 也顯示，是否曾遭遇過電腦病毒或駭客的人在資訊安全概念量表上的得分有顯著差異（t=2.136，p=.034），有經歷過電腦病毒或駭客的經驗在資訊安全概念量表上的得分顯著高於沒有經驗的學生。

4.學生的資訊安全概念與資訊安全態度是否有相關

根據 Pearsons r 檢驗的結果顯示，學生具備的資訊安全概念與他們對資訊安全的態度有顯著正相關，其相關係數為.30（p=.000）。

（三）討論

根據以上調查的結果，可以參見表 4-1-11 整理。

表 4-1-10 不同變項的比較表

變項	資訊安全概念量表	資訊安全態度量表
家中有無電腦	有>無	有>無
有無遭遇經驗	有>無	有>無
地區別	台北、新竹、台中>屏東	台北、台中、屏東>新竹

據此有幾點的發現，可以分別加以討論：

1.學生對資訊安全方面的概念仍待加強

由難度分析得知，本問卷難度偏易，但根據受訪學生在研究中所訂定之資訊安全三個面向的答對率，發現「電腦網路通訊安全」與「資訊的適切性」答對率未及七成，在個人保健方面的答對率更是偏低，可以反應出目前學生對如何正確使用電腦的相關知識普遍缺乏或不重視，也顯見這方面的知識內容有待加強。

2.家中有無電腦以及有無遭遇電腦病毒與駭客的經驗

根據研究的結果顯示，家中有無電腦的學生與有無遭遇電腦病毒與駭客的經驗兩者間有相關，同時在資訊安全概念的量表表現上也有顯著性的差異，可見隨著電腦的普及化，家中有電腦的學生在使用越來越頻繁的情形下，遭受電腦病毒與駭客影響的機會也就越大，另外，如果使用者曾經遇到電腦病毒與駭客的經驗，他們對資訊安全的態度也顯得更具有警覺性。

3.不同地區的差別

在研究的四個地區中，屏東地區在資訊安全概念的表現上明顯的低於其他三個地區，這樣的結果很有可能是由於城鄉之間的差異，顯現出數位落差的情形在這個面向上確實是存在的。另外在資訊安全態度上，新竹地區的學生呈現較另三

個區域較低的態度，研究者推測大概有幾個原因，其中一個原因可能是新竹地區的學生家長多從事資訊產業或與其相關行業，學生若遭遇相關的問題皆為家長代為處理，因此會對這方面的知覺較低，認為與資訊安全相關的資訊應該由專門的人來負責，自己不需太過擔心，另一個可能的原因是新竹地區的受測學生為國一生，在受訪的對象當中屬年紀最小的，接觸電腦的經驗較其他受測者來說相對較少，因此會對資訊安全缺乏警覺；上述為本研究者自行推論的可能原因，至於確切的原因，可能要再深入加以研究與探討。

4. 資訊安全概念與資訊安全態度的相關性

在此可以討論的是學生對資訊安全概念與資訊安全態度之間的關係，統計結果顯示兩者間有顯著的正相關，可見越瞭解資訊安全有關的知識，對於資訊安全的態度越正向，反之亦然。

以上討論的結果，也產了許多在課程設計上的啟示：

1. 根據難度分析，多數題目的難度在中等難度或偏易，然而學生答題情形，並不理想，表示學生在這方面的概念有加強的必要，尤其對個人保健知識的提升，更列為課程設計中的重點。
2. 對於曾經遭遇電腦病毒與駭客經驗的人，在安全概念量表之間也有差異，因此課程的設計上，可安排曾經有該經歷的學生來作自身的經驗分享，相信更能夠引起學生的共鳴並貼近其生活經驗。
3. 由於屏東地區在資訊安全的概念上顯著低於受訪的其他三個地區，有可能是城鄉差距造成的學生在相關概念上的不足，因此今後對偏遠地區的資訊課程，在基礎資訊概念上，應再予以加強；而新竹地區的受訪者，在資訊安全的態度上，較其他三個地區低，顯示學生雖然具備基本資訊安全的概念，但是在態度上卻顯得較為輕忽，因此在課程設計上，對學生態度上的調整，應特別予以注意；綜上所述，不同地區學生的反應情形也不一，今後對於相關課程的安排，宜針

對學生的特性，做適當的設計與調整。

4. 根據統計的結果顯示，資訊安全概念與資訊安全態度彼此之間有顯著的正相關存在，可見在課程的設計安排上，不論是加強學生對安全上的概念，或資訊安全態度的提升，都能適當喚起學生對資訊安全的重視，同時不論是對概念或態度，也都是不可偏廢的課程安排。

第二節　課程的設計與發展

一、課程規劃

本研究者經過文獻的整理分析以及訪談分析的結果，同時也考量研究者本身的能力與時間上的規劃，將本研究中的「中學生資訊安全課程」一共分為三個面向四個單元來發展，分別名為「網路安全ｅ起來」、「電腦健康百分百」、「網路逍遙遊」、「個人資料不露白」，其中「網路安全ｅ起來」，包括了對電腦病毒以及網路駭客的瞭解與防範，屬於電腦網路通訊安全，而「電腦健康百分百」，則包含了使用電腦的健康守則與須知，屬於個人安全防護，另外「網路逍遙遊」介紹的是網路上流竄的不實訊息，「個人資料不露白」，所傳達的是讓使用者不輕易在網路上留下有關個人的資訊，降低各種可能產生的危險，上述二個單元，則都屬於網路資訊的合宜性。表 4-2-1 為各學習單元以及所屬的資訊安全面向。由於教學單元內容較為龐雜，因此將其列為本研究之後的附錄部分（見附錄四），在此不加贅述。

表 4-2-1 教學單元與所屬資訊安全的面向

資訊安全面向	教學單元
1. 電腦網路通訊安全	「網路安全ｅ起來」
2. 資訊的合宜性	「網路逍遙遊」、「個人資料不露白」
3. 個人安全防護	「電腦健康百分百」

二、教學媒體設計

（一）媒體設計理念與表現類型

探討資訊安全相關的議題，往往被人認為過於專門而顯得生硬，因此在從事教學活動時，首先應調整學生對相關課程內容之觀感；透過教學媒體可以允許學生作有彈性的學習，尤其對一成不變的講解方式而言，無疑是一種有趣的變化(張玉燕，1994)，因此本研究在教學媒體的運用上，不僅希望藉此讓學生對學習的內容有初步的認識，同時也能引起學生對學習內容的學習動機與興趣，而在媒體的設計規劃上，主要透過視覺媒體的表現來進行，因為透過影像來作為知覺的傳遞媒介，不只可以讓觀賞者容易意會，也同時增加了訊息的吸引力；在視覺媒體的設計上，林麗娟（2000）表示，設計者可以採用學習比較熟悉的情境作為界面構圖的題材，如此可以激勵學習者引發相關的聯想，激發必要的互動。

本研究者在「網路安全ｅ起來」的部份，所採用的是漫畫的型態呈現，製作了「小明日記Part I&II」等兩則漫畫（附錄五）。由於漫畫屬於視覺藝術，一般商業漫畫有時充滿色情暴力意識，但卻深受歡迎，可見漫畫近來已經逐漸成為青少年生活世界中的顯性文化，也是青少年現實生活中不可或缺的文化消費（何洵怡，2002；譚光鼎，2000）。

徐照麗（2000）以為卡通、漫畫等插圖的運用，在討論較嚴肅、敏感或沉悶的話題時，有助於提振氣氛，她並認為圖象的媒體可以將抽象的表徵具象化；此外，盧姿里（2000）主張以漫畫型態為主的影像教學法，除了能幫助學生對學習材料的瞭解之外，更能使教學的活動進行的生動有趣。

根據以上所述，以漫畫為主的教學媒體，已經逐漸受到教學研究者的重視，同時也是一種可以有效吸引青少年注意的教學媒體，由於在電腦網路通訊安全的課程中所要探討的電腦病毒與電腦駭客的入侵，多半被視為一種較高層次的電腦使用技巧，也屬於抽象的概念，不太容易讓學生由外在感受到電腦病毒的設計或入侵系統的情形，因此透過學生比較容易接受的方式、較簡單的圖象設計，讓學生可以逐漸受到引領而進入教學的內容，並產生學習的興趣。

在「電腦健康百分百」單元中，由於所探討的主題為使用電腦的健康概念，也就是避免因為操作電腦的不當而受到傷害，因此本研究者在教學媒體中，一方面期望在視覺上讓學生體會到大自然萬物的美景，另一方面在聽覺上配合音樂的播放，刺激學生在視覺與聽覺上的雙重感受，領略個人身體健康的重要性；媒體的製作上，本研究者運用簡報軟體，以及所蒐及到的相關風景圖片，製作成投影片，而在音樂的選擇上，主要以輕柔之鋼琴作為配樂，之後再順勢帶入本教學單元主題。

在「網路逍遙遊」與「個人資料不漏白」兩個單元中，分別介紹了網路的謠言以及網路的個人隱私，本研究者在教學媒體的製作上，主要是以自編的兩齣狀況劇「都是美白惹的禍」以及「是誰告的密」(附錄六、七)，作為引起學生的學習動機以及帶動學生討論的工具，其內容見後述。表 4-2-2 為課程單元與使用的教學媒體一覽表。

表 4-2-2 學習單元與教學媒體一覽表

	學習單元			
	網路安全 e 起來	電腦健康百分百	網路逍遙遊	個人資料不露白
教學媒體	小明日記 Part I&II	風景圖 ppt 音樂 cd	都是美白惹的禍 ppt	是誰告的密 ppt

（二）教學媒體的發展

1.漫畫

（1）小明日記 Part Ⅰ

此則漫畫主要在敘述小明看到新聞報導，描述駭客隨意進出別人的電腦，覺得這種行為很特別而且似乎可以藉此表現自己的能力，遂興起見賢思齊的意圖；一般大眾往往在媒體的渲染之下，對於入侵系統的行為一知半解，因此藉由這樣的例子，教師可以對學生進行機會教育，告知學生電腦駭客所指為何，同時也讓

學生知道隨意進出他人電腦是不對的行為。

（2）小明日記 Part II

這一則內容是屬於近來常見的電腦病毒中毒方式，由於小明對於轉寄電子郵件的好奇心，一時不察而讓自己的電腦受到病毒的侵害，損失了寶貴的資料；透過這樣的案例，教師可以藉此詢問同學是否有相同的經驗，並請學生來分享自身的遭遇，讓學生間彼此對病毒有所警覺。

2 狀況劇

狀況劇一共有二則，分別為「都是美白惹的禍」以及「是誰告的密」，以下分別介紹之：

（1）都是美白惹的禍

這是一則探討網路謠言的狀況劇，主角小琳是個愛漂亮的女孩，她很注重打扮，然而她有一個很大的困擾，那就是她的皮膚比一般人都還黑，一次在同學的介紹下，她用了一個網路上謠傳具有美白效果的產品，沒想到卻讓她的臉上產生了一大堆的紅斑，讓她懊悔不已。由於網路上有很多似是而非的言論，有許多甚至會危及到個人健康，因此透過這樣的戲劇傳達了網路不當訊息所可能產生的危害，教師可以請同學討論是否曾在網路上有相近的例子，或是否曾經聽過網路上有什麼不實的謠言，藉此告訴大家如何對網路上的訊息作出合理的判斷。

（2）是誰告的密

本則案例在說明網路隱私的重要性;劇中小龍在學校學會了如何在網路上註冊，擁有免費的電子信箱，他同時也發現網路上有很多好用的資源等待他去發掘，可是後來他卻發現很多的網站都要註冊，才能享受會員的免費服務，於是他想了一個好方法，那就是一次將所有需要註冊的網站都登錄，這樣以後使用上就便利許多，然而就在他完成這件工作之後不久，卻給他們家帶來許多的困擾，最後連他隱瞞媽媽考試不佳的事情都東窗事發。本劇所要傳達的即是個人在網路上的資料要特別謹慎，千萬不可隨意註冊，而讓自己的資料落入有心人士的手中，並使自己與的家庭都因而受到威脅。

第三節　課程的評鑑

本節主要用來說明課程評鑑的部分。在課程的評鑑上，主要依據學生在「中學生資訊安全概念」量表的後測表現，以及學生在上完課後所填答的「課後意見調查表」分析，並配合研究者教學過程中課堂上的觀察，輔以專家所填答的「專家評鑑表」，綜合歸納出本課程實施的有效性以及相關檢討與改進之處。

一、學生的前後測差異以及「課後意見調查表」分析

本研究者在進行教學之後，對受教學生依不同單元的「資訊安全概念」，實施後測，所獲得成績再與前測進行「配對樣本 t 檢定」，該統計方式通常用於具有前後測的研究設計中（邱皓政，2000），以檢驗在完成教學活動之後，學生在資訊安全概念成績上是否有進步，此外，學生在課後的意見調查與研究者在課堂上的觀察也為課程實施成效的指標之一；以下分別對四個學習單元來進行討論。

（一）網路安全 e 起來

本問卷題數共十題，一題以一分計，滿分為十分，根據表 4-3-1 顯示，所獲得的 t 值為-3.77，考驗效果達顯著，顯示後測的成績較前測有些許的提升。可見學生在經過課程的安排之後，成績有所進步。

表 4-3-1 網路安全 e 起來前後測比較

組別	平均分數	標準差	t值
前測	8.08	1.15	-3.77**
後測	8.96	1.02	

**p<.01

而在課後意見調查表上，見表 4-3-2，在 31 位受測者中對課程內容的安排方面，除了對課程內容豐富並吸引人的比率稍低，認為「非常同意」與「同意」的人在 77%左右，其餘認為「非常同意」與「同意」的學生幾乎都在 93%以上；

在學習方面，認為課程可以引起學習動機，表示「非常同意」與「同意」的學生所佔的比率略低，約在74%左右，其餘認為可以從課程中學習新知、認為課程的設計可以有效幫助學習、以及將所學運用到日常生活，表示「非常同意」或「同意」的都在92%以上；綜合評價方面，「非常同意」與「同意」整體課程所帶來的幫助與成效的都在92%以上，「不同意」的皆為6.5%。

本研究者在教學過程中，發現教學媒體的呈現，可以引起多數學生的注意，也有學生願意跟其他同學大方分享自己遭遇電腦病毒的經驗，但有學生在課後意見調查表上表示，過去曾上過有關電腦病毒的課，因此會認為本課是老生常談，這方面或許可以說明課程意見調查表上，在內容豐富並吸引人以及認為課程可以引起學習動機兩個選項上，所獲的同意率較低，表示課程還有調整與修改的空間。

表4-3-2 網路安全e起來課後意見調查表

	非常同意（%）（人）	同意（%）（人）	不同意（%）（人）	非常不同意（%）（人）
一、課程內容				
1.課程內容豐富並吸引人。	6.5（2）	71.0（22）	22.6（7）	0（0）
2.課程的安排恰當、難易適中。	19.4（6）	77.4（24）	3.2（1）	0（0）
3.課程設計讓我對電腦與網路的瞭解更多。	12.9（4）	80.6（25）	6.5（2）	0（0）
4.上了本課程後，我會更加注意資訊的安全。	16.1（5）	80.6（25）	3.2（1）	0（0）
二、學生的學習				
5.可以從課程中學習到新知。	16.1（5）	80.6（25）	3.2（1）	0（0）
6.課程內容能引起自己的學習興趣。	12.9（4）	61.3（19）	25.8（8）	0（0）
7.課程中的活動設計可以有效的幫助學習。	12.9（4）	80.6（25）	6.5（2）	0（0）

8.我會將所學應用在日常生活中。	6.5 （2）	90.3 （28）	3.2 （1）	0 （0）
三、綜合評價				
9.上完這個課程，對我有很大的幫助。	9.7 （3）	83.9 （26）	6.5 （2）	0 （0）
10.上了本課後，我會更適當使用電腦與網路。	12.9 （4）	80.6 （25）	6.5 （2）	0 （0）
11.整體來說，在本課程中所帶來的成效不錯。	9.7 （3）	83.9 （26）	6.5 （2）	0 （0）
受試者：31 人				

（二）電腦健康百分百

根據表 4-3-3 可以得知，獲得的 t 值為-10.45，考驗效果達顯著，顯示後測的成績較前測有顯著的提升。表示學生在課程的實施之後，成績有顯著的進步。

表 4-3-3 電腦健康百分百前後測比較

組別	平均分數	標準差	t值
前測	2.42	1.03	-10.45***
後測	4.54	0.65	

***p<.001

課後意見調查表上，見表 4-3-4，28 位受訪者中，對課程內容的安排上，認為「非常同意」或「同意」的人都在 80%以上，其中對課程內容安排恰當以及上了課程後，會更加注意安全表示「非常同意」、「同意」的人，更在 92%以上；在學習方面，除了對課程可以引起學習興趣方面，表示「非常同意」與「同意」的人稍低，約佔 82%左右，其餘像學習新知、幫助學習以及將所學應用至生活上，認為「非常同意」、「同意」的人都接近 90%或超過；綜合評價方面，有 92%左右的人在「會更適當使用電腦與網路」的選項上表示「非常同意」與「同意」，而在「上完該課程有很大幫助」以及「整體來說，在本課程中所帶來的成效不錯」兩方面，認為「非常同意」與「同意」的人也都在 85%以及 89%左右以上。

本研究者在教學的過程中，覺得課程之初所使用的音樂配合投影片的播放，可以有效吸引學生的注意，尤其在課程實施前，適逢學生的午休時間，學生的精神較為渙散，此舉對振奮學生精神有不錯效果；而課程進行中，學生在分組討論的表現上，展現豐富的想像力，也為課程增添許多趣味性，例如學生在討論電腦工作站設計不良，對人體可能產生的傷害以及如何防止傷害的造成，學生可以具體的說出他們認為可能的觀點。

表4-3-4 電腦健康百分百課後意見調查表

	非常同意（%）（人）	同意（%）（人）	不同意（%）（人）	非常不同意（%）（人）
一、課程內容				
1.課程內容豐富並吸引人。	3.6（1）	82.1（23）	14.3（4）	0（0）
2.課程的安排恰當、難易適中。	10.7（3）	85.7（24）	3.6（1）	0（0）
3.課程設計讓我對電腦與網路的瞭解更多。	0（0）	82.1（23）	17.9（5）	0（0）
4.上了本課程後，我會更加注意資訊的安全。	10.7（3）	82.1（23）	7.1（2）	0（0）
二、學生的學習				
5.可以從課程中學習到新知。	7.1（2）	82.1（23）	10.7（3）	0（0）
6.課程內容能引起自己的學習興趣。	3.6（1）	78.6（22）	17.9（5）	0（0）
7.課程中的活動設計可以有效的幫助學習。	3.6（1）	89.3（25）	7.1（2）	0（0）
8.我會將所學應用在日常生活中。	3.6（1）	85.7（24）	10.7（3）	0（0）
三、綜合評價				
9.上完這個課程，對我有很大的幫助。	3.6（1）	82.1（23）	14.3（4）	0（0）
10.上了本課後，我會更適當使用電腦與網路。	10.7	82.1	3.6	3.6

	(3)	(23)	(1)	(1)
11.整體來說，在本課程中所帶來的成效不錯。	7.1 (2)	82.1 (23)	7.1 (2)	3.6 (1)
受試者：28 人				

（三）網路逍遙遊

表 4-3-5 的結果顯示，前後測的比較並沒有顯著上的差別，很有可能是在網路謠言的部分題數不多，總題數四題，總分為四分，因此學生在前後測的表現差異不明顯，雖然前測所獲得的平均數為 2.83，後測則為 2.92，但兩者在統計分析上無法判別其差異。

表 4-3-5 網路逍遙遊前後測比較

組別	平均分數	標準差	t值
前測	2.83	.97	-.62
後測	2.92	.87	

課後意見調查表上，見表 4-3-6，38 位受訪者中，對課程內容的安排，認為「非常同意」與「同意」的比率，皆在 92%以上；學習方面，除了認為課程可以引起學習興趣以及有效的幫助學習上，表示「非常同意」與「同意」的人在 83%與 89%左右之外，其餘如學習新知、並應用到日常生活的，在「非常同意」與「同意」上的比率皆在 92%以上；綜合評價方面，學生表示「非常同意」與「同意」上完課程有很大幫助上，所佔百分比為 89%左右，而在適當使用電腦與網路以及認為整體成效不錯上，表示「非常同意」與「同意」的人更在 92%以上。

本研究者在教學過程中，發現所製作的狀況劇播放，可以引起學生很大的興趣，有助於課程內容的引入，同時運用具有圖片的謠言案例，更能激發學生對網路謠言的認識；但學生在小組討論的部分稍有不足，可能是國一學生在分組活動進行方面，需要多方面來引導。

表4-3-6網路逍遙遊課後意見調查表

	非常同意（%）（人）	同意（%）（人）	不同意（%）（人）	非常不同意（%）（人）
一、課程內容				
1.課程內容豐富並吸引人。	28.9（11）	65.8（25）	5.3（2）	0（0）
2.課程的安排恰當、難易適中。	42.1（16）	55.3（21）	2.6（1）	0（0）
3.課程設計讓我對電腦與網路的瞭解更多。	42.1（16）	50.0（19）	7.9（3）	0（0）
4.上了本課程後，我會更加注意資訊的安全。	52.6（20）	39.5（15）	7.9（3）	0（0）
二、學生的學習				
5.可以從課程中學習到新知。	47.4（18）	47.4（18）	5.3（2）	0（0）
6.課程內容能引起自己的學習興趣。	47.4（18）	36.8（14）	15.8（6）	0（0）
7.課程中的活動設計可以有效的幫助學習。	44.7（17）	44.7（17）	10.5（4）	0（0）
8.我會將所學應用在日常生活中。	50.0（19）	42.1（16）	7.9（3）	0（0）
三、綜合評價				
9.上完這個課程，對我有很大的幫助。	36.8（14）	52.6（20）	10.5（4）	0（0）
10.上了本課後，我會更適當使用電腦與網路。	50.0（19）	47.4（18）	2.6（1）	0（0）
11.整體來說，在本課程中所帶來的成效不錯。	47.4（18）	44.7（17）	7.9（3）	0（0）
受試者：38 人				

（四）個人資料不露白

表4-3-7的結果，顯示在個人隱私的部分，經過教學之後，學生在這方面的概念有顯著的改變，後測獲得的平均分數8.86，顯著高於前測所獲得的平均分數

6.69。

表 4-3-7 個人資料不露白前後測比較

組別	平均分數	標準差	t值
前測	6.69	1.63	-8.41***
後測	8.86	1.16	

***p<.001

課後意見調查表方面，見表4-3-8，35位受訪者中，在課程內容的安排上，認為「非常同意」與「同意」的人，佔91%以上，其中認為課程設計可以對電腦與網路的瞭解更多方面，所佔人數比更高達97%左右；至於學習方面，覺得課程可以讓自己獲得新知、並有效幫助學習兩個選項上，表示「非常同意」與「同意」所佔的人數比高達97%左右，其餘選項表示「非常同意」與「同意」的人也都在91%以上；綜合評價方面，認為「非常同意」與「同意」整體課程所帶來的幫助與成效比例為都在91%以上，認為「不同意」的不超過9%。

由此可以看出，學生對於課程內容、學習上以及整體的評價上，都有不錯的反應，這方面可與本研究者在教學過程中，所觀察到的學生學習情形相符合，課程進行中，學生對課程的進行以及小組的討論上，皆有不錯的表現，整體互動性不差。

表4-3-8 個人資料不露白課後意見調查表

	非常同意（%）（人）	同意（%）（人）	不同意（%）（人）	非常不同意（%）（人）
一、課程內容				
1.課程內容豐富並吸引人。	11.4（4）	80.0（28）	8.6（3）	0（0）
2.課程的安排恰當、難易適中。	22.9（8）	68.6（24）	8.6（3）	0（0）
3.課程設計讓我對電腦與網路的瞭解更多。	28.6	68.6	2.9	0

	(10)	(24)	(1)	(0)
4.上了本課程後，我會更加注意資訊的安全。	34.3 (12)	60.0 (21)	5.7 (2)	0 (0)
二、學生的學習				
5.可以從課程中學習到新知。	34.3 (12)	62.9 (22)	2.9 (1)	0 (0)
6.課程內容能引起自己的學習興趣。	17.1 (6)	74.3 (26)	8.6 (3)	0 (0)
7.課程中的活動設計可以有效的幫助學習。	25.7 (9)	71.4 (25)	2.9 (1)	0 (0)
8.我會將所學應用在日常生活中。	31.4 (11)	62.9 (22)	5.7 (2)	0 (0)
三、綜合評價				
9.上完這個課程，對我有很大的幫助。	22.9 (8)	68.6 (24)	8.6 (3)	0 (0)
10.上了本課後，我會更適當使用電腦與網路。	28.6 (10)	68.6 (24)	2.9 (1)	0 (0)
11.整體來說，在本課程中所帶來的成效不錯。	22.9 (8)	74.3 (26)	2.9 (1)	0 (0)
受試者：35 人				

二、專家評鑑

在專家評鑑方面，本研究者選定5位在資訊教育以及教學領域方面經驗豐富、學養兼備的學者教師作為受訪對象，分別為兩位在網路學習以及教學科技領域的專家，以及在三位中學任教並擁有豐富教學經驗與課程規劃之專家。

評鑑的工具為研究者自編之「專家評鑑調查表」，一共分為兩部份，第一部份是針對所有課程的五個面向來做評估，分別為「課程規劃」、「課程目標」、「課程內容」、「教學」以及「評鑑的實施」等五方面，並採Likert五點式量表，依序從「非常不同意」、「不同意」、「中立意見」、「同意」到「非常同意」等五個等級，採1到5計分，第二部份則為開放式問題，請受訪專家針對課程提供相關建議或需改進之處。

根據專家對本課程實施評鑑的結果顯示，多數專家教師對四個單元的課程設

計上，不論是內容的豐富度以及活動的發展方面，都有不錯的評價，因此除了少數項目所獲得的平均分數在4以下之外，大部份評估項目所獲的平均分數皆在4以上；然而，每個單元在「計算課程所需時數準確」評估項目上，獲得的平均分數跟其他項目表現相較之下，顯著的偏低，可見在課程規劃方面，單元時間的計算無法符合課程的需求，因此針對這方面，有需要再加以改進。表4-3-9為各單元在專家評估問卷中所獲得的平均分數，以下分別依單元來說明。

表 4-3-9 專家評估結果

評估面向	內容細則	網路安全ｅ起來	電腦健康百分百	網路逍遙遊	個人資料不露白
課程規劃	1.需求性評估妥適	4.60	4.40	4.40	4.40
	2.能將評估的結果應用在課程設計上	4.40	4.20	4.20	4.20
	3.計算課程所需時數準確	**2.60**	**3.40**	**3.40**	**3.60**
	4.能列出相關參考資源	5.00	4.80	4.80	4.60
	5.教學資源包含在課程中或容易取得	4.80	4.80	4.80	4.40
課程目標	1.清楚的陳述課程目標	4.20	4.80	4.60	4.40
	2.課程目標可以傳達課程的意涵	4.40	4.40	4.60	4.40
	3.目標能配合課程目的與內容	4.40	4.40	4.20	4.40
課程內容	1.內容生動，可吸引學生的動機與興趣	4.40	**3.80**	5.00	4.60
	2.課程內容難易適中	4.00	**3.60**	4.60	4.20
	3.課程實用性高	4.80	4.20	4.60	4.80
	4.內容能與學習者的生活經驗結合	4.20	4.20	4.80	4.80
	5.課程內容可以對學生有實質的幫助	4.60	4.80	5.00	4.80
教學	1.教學能配合學生需求	4.40	4.20	4.60	4.60
	2.教學內容可引起學生共鳴	4.40	4.00	4.80	4.80
	3.教學的順序與步驟適當	4.60	**3.60**	4.80	4.40
	4.教學策略包含主動與合作性的學習	4.60	4.40	4.40	4.40
評量實施	1.評量是有效、可信的	4.40	**3.80**	**3.80**	4.00
	2.清楚說明評量的方式	4.20	4.20	**3.80**	4.00
	3.評量方式與課程目標相配合	4.40	4.40	4.00	4.20

（一）網路安全ｅ起來

根據表 4-3-9 專家評估的結果，可以發現受訪的專家教師中對本研究所設計的課程內容與教學流程大部分都持肯定且正向的態度，因此所獲得的平均分數多在 4 分以上，不過在「計算課程所需時數準確」的選項上，所獲得的平均分數較低為 2.60，多數專家表示從教案中不容易正確估算所需時數，同時有專家建議在本單元中，由於難度較深，因此這方面應增加教學時數的安排，如此才能讓學生容易吸收到該單元的內容。

而在開放式的題目中，幾個較為具體的建議為：

1. 多數受訪者都認為本課程的內容豐富有趣，可以引起學生的興趣。
2. 對案例的建議上，可以將案例中的時間確切標示年月日，或是其中提到電腦病毒所造成數百萬的損失，可再具體讓學生了解到底造成多大的傷害。
3. 建議在講述電腦病毒與網路駭客時，帶一點網路犯罪的法律討論，這樣一來可以避免讓學生因不瞭解事情的嚴重性，而在無意間觸法。
4. 建議可以請學生事先蒐集相關資料，教師可以站在輔助說明的角色。

（二）電腦健康百分百

本單元中，幾個較低分的項目除了「計算課程所需時數準確」獲得3.4分之外，其餘分別為「內容生動，可吸引學生的動機與興趣」、「內容難易適中」、「教學的順序與步驟適當」以及「評量是有效可信的」等四個項目，所獲得的平均分數分別為3.8、3.6、3.6、3.8。在開放式的問題方面，幾個較為重大且具體的建議為：

1. 許多專家表示在開始的引起動機和教學活動之間的連貫較弱，因此在中間應該再增加連接，例如在教學設計中，教師可以讓同學思考，如果因為使用電腦而導致健康問題，無法再享受過去曾擁有的美好生活，是否會感到很後悔。
2. 此外，有專家表示本單元在分段能力指標上是用於國小三四年級，但教學設計卻針對國高中，因可能需考量其適用性或再多加一些學習內容說明。

（三）網路逍遙遊

本單元中，評估的專家皆表示課程的進行能運用實際案例及趣味性，頗能引起學生的學習動機。幾個較低分的項目除了「計算課程所需時數準確」獲得3.4分之外，其餘兩項分別為「評量有效可信」以及「清楚說明評量方式」，獲得的平均分數皆為3.8。在開放式的問題方面，幾個較為重大具體的建議為：

1.學習單的內容可加入一些案例，讓學生設法去查詢相關資料，以辨別事件的真偽，同時也可親身體驗辨別資訊的可用性與有效性。

2.可將學習單的內容納入評量的項目之一。

（四）個人資料不露白

本單元中，多數的教師專家表示課程活動有趣，同時教學資源也很豐富。因此除了時數的分配所獲得的分數較低為3.6分之外，其餘平均分數都在4以上，而幾個較為具體的建議為：

1.在課前準備上，可以請學生幫教師找好相關資料。

2.對於侵犯他人網路隱私全會有怎樣的處罰，可就法律面或道德面稍做說明。

三、小節

本節主要在說明對課程的評鑑階段，研究者所採的評鑑依據主要有三，分別為學生在資訊安全概念的前後測表現、課程意見調查表並配合研究者上課的觀察以及專家的評估，對課程提出相關建議作為修改之依據。

學生在前後測的表現上，四個單元中，有三個單元可以看出學生在經歷過教學課程後，有明顯的進步，至於「網路逍遙遊」，由於用於受測的題目不多，因此較無法看出其與前測的顯著差別；而在課程意見調查表上與研究者課堂觀察上，可以發現多數學生在課程當中的反應都不錯，藉此證明本課程的實施成效不差；至於專家評估課程的部分，多數的受訪者表示本課程在設計的內容上、豐富度以及趣味性都不錯，並提出相關的建議，以作為本研究者對課程加以修改、檢

討之依據。以下為本研究者整理專家評估對本課程所提出的建議：

1. 本課程的設計主要是以教師引導為主，未來在發展上，應可以調整不一樣的學習型態，讓學生擔任自學的角色，例如對網路謠言進行科學驗證性的活動，而教師只擔任輔導者的角度。
2. 教學所需的時數不足，教師應針對學生的程度參酌使用，由於不同的教師會有不同的教學喜好與取向，同時學生的接受狀況也不一，因此在教學時數的分配上，教師可依所掌握的情況對內容加以取捨。
3. 在「網路安全e起來」以及「個人資料不露白」兩單元中，宜導正學生觀念的偏差，適當的矯正學生偏頗的心態並輔以法律常識的介紹，避免學生因輕忽與認知上的缺乏而導致無可承受之後果。

第五章　結論與建議

本章共分為三節來討論，第一節為本研究的結論，第二節則為本研究的限制，第三節則為本研究者對未來相關研究提出的建議。

第一節　結論

本研究主要針對所探討的資訊安全議題，發展出一套適合中學生的資訊安全課程，課程發展的過程，主要經過分析、設計、發展與評鑑的階段，因此在研究的結論也希望由課程發展的不同階段所獲得的結果，並以第一章中提出的研究問題來加以說明。

一、資訊安全的定義與內涵

傳統的資訊安全，最簡要的定義便是利用各種方法或工具來保護靜態或動態的資訊，本研究者認為凡涉及與資訊有關的安全防護或傷害，都可將其歸於資訊安全所探討的議題中，然而研究者受限於時間與能力上的限制，在此將資訊安全的議題分為三方面加以探討：

（一）電腦網路通訊安全：（例如駭客入侵、病毒、以及相關的安全機制等），由於牽涉到較高的技術層次，因此過去被認為是一般人較無法觸及的領域，近來隨著便利工具的充斥，資訊的普及導致取得容易，讓從事破壞網路通訊安全的專業門檻因此降低，造成不斷衍生的資訊犯罪問題，再加上社會的轉型持續擴張，學校也漸漸成為散佈的溫床。

（二）資訊的正確、合宜與私密性：由於網路的資訊流通快速，因此不實以及不當的言論或訊息在網路上散播，讓人不勝其擾，同時個人資料的外洩，更使個人隱私在網路上無所遁形。

（三）確保個人安全：在此主要探討個人操作電腦所應具備的基本保健常識，例如長時間或不正確的姿勢使用電腦，會使人體的健康受到損害，而造成個人的不便或終生的傷害。

二、「資訊安全」課程的需求性評估

根據文獻分析的結果，本研究所探討的資訊安全範圍主要分為「電腦網路通訊安全」、「資訊的適切性」以及「個人保健安全」三個面向，為了確認資訊安全課程是否有發展的需求性，本研究者親身訪談五位目前任教於中學的資訊教師；訪談的結果，多數的受訪教師都認為現有的學生接觸電腦與網際網路的機會大幅增加，但在目前的資訊課程中，有關資訊安全方面的規劃卻明顯不足，因此發展相關課程內容有其必要性，而課程中所應包含的內容除了前述的三個議題，如電腦網路通訊安全、資訊的合宜性以及個人安全防護之外，還包括了網路交友、法律或網路購物以及智慧財產權等內容，但本研究者基於時間以及能力上的限制，因此只將針對前述的三個議題進行研究。

此外，研究者以自編之「中學生資訊安全概念與態度」量表，一共發出 398 份問卷，對台北、新竹、台中、屏東等四個地區的國高中生，進行學生的資訊安全起點能力與態度調查，調查結果顯示，學生整體所具備的資訊安全概念仍有所不足，其中學生在個人保健部份的基本概念更為缺乏，實有加強的必要；至於不同區域的比較上，屏東地區的學生，在資訊安全概念上的表現顯著低於其他地區，顯見偏遠地區學生在資訊安全概念上與都會區的差異，而在資訊安全態度的部分，新竹地區較其他地區來得低，研究者提出兩點可能的解釋，其中一個可能的原因為，新竹地區的學生其家長較多從事資訊產業的人員，學生遭遇到相關問題的機會較低，另一個原因，則是因為新竹地區的受測者較其他地區來說，年級層較低，接觸電腦的經驗尚不如其他年級層高的學生來得多，因此遭遇相關問題的頻率也相對較少。

三、「資訊安全」課程的發展

根據文獻分析的結果，本研究將資訊安全一共分為三個面向四個學習單元來發展，其中四個學習單元分別為「網路安全ｅ起來」、「電腦健康百分百」、「網路逍遙遊」、「個人資料不露白」。「網路安全ｅ起來」單元中，包括了對電腦病毒以

及網路駭客的瞭解與防範，「電腦健康百分百」，則包含了使用電腦的健康守則與須知，而「網路逍遙遊」所介紹的內容，為教導學生如何辨別網路上流竄的不實訊息，最後，在「個人資料不露白」一單元中，所傳達的是提醒使用者不輕易在網路上留下有關個人的資訊，降低各種可能產生的危險。

在教學策略上，本研究者主要採用大量實際的案例運用，藉以貼近學生生活經驗，同時配合教學媒體的製作，以引起學生的學習動機與興趣，為此本研究主要運用視覺媒體的設計規劃，開發了「小明日記 PartI&II」，運用連環漫畫的方式來呈現，內容敘述網路上橫行的駭客與到處肆虐的電腦病毒，此外並設計了「都是美白惹的禍」、「是誰告的密」兩齣狀況劇，內容為針對網路謠言以及網路個人隱私的情境模擬；在課程的安排上，則以小組討論、角色扮演的活動方式讓學生參與，使學生從活潑的學習過程中，習得相關知識。

四、「資訊安全」課程的評估

本研究者選定位於台北市與新竹市地區的兩所中學、三個班級為課程實施的對象，在教學完成後，對學生進行學習單元的後測，以及課後意見的調查，藉以檢視學生在接受課程的教學後，對相關概念是否有顯著的提升，同時，也調查學生對課程的反應情形；根據前後測的差異比較，顯示學生接受課程的教學之後，在電腦網路通訊安全、個人保健以及網路隱私的部分，都有顯著性的差異，但在網路謠言的部分，由於用於測試的題目數不多，因此其前後測的差異較不明顯，整體來說，學生在接受本研究課程後，對相關概念與知識的增長，都有顯著的成長。

在不同單元的課後意見調查表反應上，除了在「網路安全ｅ起來」單元中，學生在內容豐富並吸引人以及認為課程可以引起學習動機兩個選項上，所獲的同意率稍低之外，認為「同意」與「非常同意」的人數比約在 74%與 78%左右，其餘單元學生普遍認為課程的實施成效不差，因此對課程的意見在「同意」與「非

常同意」所佔的人數比都在 80%以上，顯見學生認為本課程的實施，不僅可以帶給他們新知，對於日後應用於日常生活中，也有所幫助，而研究者藉由教學中的觀察，也可以明顯感受到多數學生在此次的教學活動中，對課程的進行有相當高的投入。

此外，本研究者針對具有學科內容、教學設計以及對中學資訊課程具有豐富教學經驗的專家教師，以研究者自編之「專家評鑑表」進行調查，研究的結果顯示多數的專家認為課程的設計方面，不論是在課程活動的設計安排上以及資源運用方面，都相當有趣而且豐富，除此之外，也提出幾點較為重大具體的建議，分別為對課程時間的安排上、引導學生正確的觀念以及教學的取向上，相關的建議，本研究者都納為課程修改的重要依據。

第二節　研究限制

本研究因時間與人力上的限制，因此所探討的範圍僅以文獻所載與所蒐集的資料為限，無法涵蓋所有與資訊安全有關的議題；此外，在研究上有下述幾點的限制：

一、受測者抽樣的限制

學生對資訊安全的概念與態度，因所處區域的差異以及社經背景的不同，也會產生許多的差異性，例如數位落差（Digital Divide）的問題，產生了區域間資訊能力的差異（林逢慶，2003），由於本研究所採的抽樣方式為便利取樣，因此在研究結果的推論上有其限制性。

二、課程導向的限制

本研究課程的取向上，多數活動皆由教師主導，雖然活動的進行中，學生可以分組參與討論以及發表意見，同時也產生許多互動關係，但教師大部分皆為課程中的主角，距以「學習者為主」的課程取向仍有段距離。

三、課程的安排

由於本研究的進行，受限於進行教學的班級，單一教學單元只能針對一個班級進行教學，無法比較不同班級在同一單元內的表現是否有不同的結果，而在課程的規劃方面，對預設的教學時間上，無法做較長時間的設計，此舉也將是影響學生學習成效的因素之一。

四、研究者自身的限制

本研究者由於在研究中擔任課程的設計與教學者的雙重角色，在過程中可能會產生無法預期的盲點，缺乏較廣泛的角度來進行課程的發展規劃，同時研究者本身對活動設計較缺乏創新概念，因此無法提供更為有效的學習活動發展，對學校教室情境的掌握，也有所不足，這些都將是影響課程實施成效的原因。

五、課程涵蓋的範圍

雖然本研究者在進行需求性評估時，許多訪談的教師表示，目前資訊安全較為重要的議題，除了本研究所提及的三個面向之外，其餘如網路交友、線上購物以及網路法律等也都是迫切需要加入的內容，但是本研究者基於自身的能力限制，無法將其納入本研究的研究議題。

六、態度方面缺乏後測

研究者基於課程時間的安排，對資訊安全態度方面並沒有進行後測，因此在學生的態度上無法看出是否產生改變，僅能由教師在教學的過程中，觀察學生的反應情形來加以判斷。

第三節　建議

本研究者於課程發展的過程中，獲得許多發現，在此，提出對未來從事相關研究的幾點建議：

一、增加相關課程內容

藉由需求訪談可以發現，教師對於資訊安全有關的議題，除了本研究的討論範圍之外，其他如網路交友、網路購物，也是教師們認為亟待對學生引導與加強

的內容，或者可將網路法律的內容與本課程作連結，讓學生不僅知法同時也不會因此而觸法。建議未來對於資訊安全課程的設計上，可以規劃納入這些內容。

二、減少區域間差異

根據本研究者進行「資訊安全概念與態度」的調查，可以發現不同的區域間，學生在資訊安全概念與態度上確實有差異存在，因此今後對不同的地區，可以透過不同的課程設計取向，減少學生在相關概念或態度上的差異性。

三、增加教學班級

由於本研究者在取樣上的限制性，因此在實地進行教學的班級數不多，建議未來可以對不同的班級或不同年級的學生進行同一單元的教學與比較測試，相信可以獲得更多的研究成果。

四、讓學生擁有更多自主學習經驗

未來在這類課程的安排上，宜多採取讓學生自主學習的課程設計，教師一方面可以減輕負擔，另一方面也可養成學生獨立學習的習慣，例如讓學生自己親身操作，遭遇電腦病毒時的處置情形，或是讓學生可以自行分組尋找網路謠言的相關佐證資料，甚至讓學生在個人隱私的課程中，可以在網路上尋找自己所熟悉的對象資料，如此一來更能激發學生在學習上的主動性。

科技的發展促進了人類文明的昌盛，今日的社會，更由於網際網路的連結，帶動了一連串前所未有的數位革命，然而隨著對科技的依賴越深，許多令我們無法預期的狀況也因然而生。雖然科技在技術上不斷的有所突破，但各種可能的資訊安全危機也持續的在產生，然而，目前並沒有一種可以完全有效遏阻這類傷害機制的存在。因此，透過基礎教育著手，讓學生建構培養基本的資訊安全防護概念，保護自己也保護他人，相信是最根本而且有效的作法，也是本研究之初衷，希望本研究可收拋磚引玉之效，期待有更多的研究者投入。

參考文獻

中央警察大學資訊密碼暨建構實驗室（2003）。誰偷了我的網路身份資料？網路通訊（147），22-25。

台灣微軟（2001）。電腦使用健康指南。2003.12.27 取自 http://www.microsoft.com/taiwan/Hardware/ergo/position.htm

尹玫君（2000a）。國小老師的網路教學素養與培育。資訊與教育（79），13-19。

王正豪（2004，7 月）。SPAM 防治技術探討。論文發表於中央警察大學，國立台灣大學主辦之「2004 年：資訊科技與人文管理教育論壇」數位內容、數位教育與管理政策研討會，台北。

向電腦傷害說不（n. d.）。2003.12.11 取自 http://webs.sups.tp.edu.tw/computer/rule/hurt/hurt.htm

行政院「資訊教育基礎建設計畫」擴大內需方案實施作業計畫(1998)。2003.09.16 取自 http://www.ey.gov.tw/planning_old/pe871203-1.htm

沈中偉（1999）。國小資訊教育的省思與理念。資訊與教育（71），52-57。

李正吉、林詠章、黃明祥(2002)。電子檔案之安全技術。檔案季刊，1(2)，48-57。

余民寧（1998）。教育測驗與評量:成就測驗與教學評量。台北：心理。

汪志堅、駱少康（2002）。網路上流傳謠言類型與特性研究。2004.05.20 取自 http://mozilla.hss.nthu.edu.tw/iscenter/conference2002/

李安德（1992）。超個人心理學：心理學的新典範。若水譯。台北：桂冠。

何志中（1999）。台灣中部地區國民小學教師網路素養之研究。國立臺中師範學院國民教育研究所碩士論文。中華博碩士論文，88NTCTC576012。

李怡志（2000）。有趣的網路流言。2003.11.30 取自 http://www.richyli.com/hondoni/20000404.htm

李怡志（2003）。兒童選媒體網路排第一。2003.09.08 取自 http://tw.news.yahoo.com/2003/09/08/leisure/ctnews/4243011.html

吳明清（2001）。教育研究-基本觀念與方法之分析。台北：五南。

李忠憲（2001）。增進校園網路安全。教師天地（111），40-45。

李宗薇（2000）。教學設計理論與模式的評析及應用：以師院社會科教材教法為例。國立臺灣師範大學教育研究所博士論文。中華博碩士論文，88NTNU0331026。

李建平（2003）。黑客：游俠還是罪犯？2003.10.24 取自 http://it.sina.com.hk/it_news/2003/0313/51269.html

吳美美（1996a）。資訊時代人人需要資訊素養。社教雙月刊（73），4-5。

吳美瑩（2001）。網路成文規範與使用者行為之初探—以台大椰林風情BBS政治版為例。國立交通大學傳播所碩士論文。中華博碩士論文，89NCTU0376007。

何洵怡（2002）。談中文科漫畫教學。國文天地 17（8），83-88。

宋振華、楊子翔、樊國楨(2001)。資訊系統入侵與偵防。資訊安全通訊，7(2)，

91-97。
邱皓政（2000）。量化研究與統計分析。台北：五南。
何榮桂（1998）。從教育部之資訊教育推展策略看未來中小學資訊教育的願景。資訊與教育（68），2-13。
李維倫（2003）。駭客入侵-淺談個人電腦網路安全。資訊與教育（94），93-99。
吳賢明（2000）。腦系統談校園網路防駭之道。資訊與教育（78），29-41。
林佳旺（2003）。國小網路素養課程系統化教學設計之行動研究-以「六年級網路互動安全課程」為例。國立嘉義大學教育科技研究所碩士論文。中華博碩士論文，91NCYU0620005。
邱俊吉（2003）。台灣垃圾郵件一年耗600億。中時電子報。2003.10.26取自http://news.chinatimes.com/Chinatimes/
林珊如、劉旨峰、袁賢銘（2001）。技術學院資訊相關科系學生的電腦病毒之迷思概念研究。資訊與教育（86），51-61。
林修遠（2003）。電腦病毒於3D電腦動畫視覺化之研究。中原大學商業設計研究所碩士論文。中華博碩士論文，91CYCU5317006。
林進材（2000）。有效教學-理論與策略。台北：五南。
林逢慶（2003）。消弭數位落差：政府的責任與對策。國家政策季刊2(1)，29-52。
林詠章、黃明祥（2000）。資訊系統之安全技術。資訊與教育（78），15-28。
施良方（1997）。課程理論。高雄：麗文。
林麗娟（2000）。電腦視覺設計：動態性因素與學生特質探討。台北縣：輔仁大學出版。
孫中英（2003，11月19日）。花旗洩密 消金負責人將親自處理。聯合報，C02版。
病毒/蟲-看不見的敵人（n. d.）。2003.10.04取自http://www.symantec.com/region/tw/homecomputing/article/virus.html
徐照麗（2000）。教學媒體：系統化的設計、製作與運用。台北：五南。
高麗玲（2003，10月10日）。打電腦過勞易傷手腕。蘋果日報，A10版。
麻少華（2003）。信用卡網路安全機制探討。國立臺灣大學商學研究所碩士論文。中華博碩士論文，91NTU00318112。
陳文進（2000）。我國資訊教育之演進與未來發展。資訊與教育（80），78-89。
郭生玉（2000）。心理與教育測驗。台北，精華。
張玉燕（1994）。教學媒體。台北：五南。
葉芳如（1999）。如何保護兒童網路隱私安全？資訊與電腦（231），129-131。
教育部（1998）。國民中小學教師資訊基本素養指標。2003.09.23取自http://wwwnet.tmps.tp.edu.tw/edu/teacher/teacher1.htm
教育部（2001）。中小學資訊教育總藍圖初稿。台北：教育部。
教育部（2003）。國民中小學九年一貫課程綱要-重大議題。台北：教育部。
許怡安（2001）。兒童網路使用與網路媒體素養之研究--以台北縣市國小高年級

學童為例。國立政治大學廣播電視學碩士論文。中華博碩士論文，89NCCU0472013。
張芳綺（2002）。中學生網路素養課程設計與發展之初探。國立交通大學傳播研究所碩士論文。中華博碩士論文，90NCTU0376012。
陳長榮、崔友經（2002）。公開金鑰基礎建設之應用與議題。通訊雜誌（108），36-39。
陳則黎、蘇偉慶（2000）。SSL 及 SET 之分析比較。資訊安全通訊，6(3)，58-78。
康春枝（1999）。培養中小學師生資訊素養之實際—以高師大附中為例。2003.10.02 取自 http://www.ntnu.edu.tw/ace/new/2-7.htm。
張春興（1996）。教育心理學-三化取向。台北：東華。
陳炳男（2002）。國小學生網路素養及其相關因素之研究。國立屏東師範學院國民教育研究所碩士論文。中華博碩士論文，90NPTT1576028。
許秋芬(2001)。資訊時代的資訊倫理課題。台北市立圖書館館訊，18(3)，56-64。
張郁蔚（2003）。從資訊素養標準探討我國小學資訊教育課程。國立中央圖書館臺灣分館館刊，9（2），58-72。
陳泰安(2002)。九年一貫課程教師資訊素養能力之探究。資訊與教育(91)，50-59。
張祖忻、朱純、胡頌華編著（1995）。教學設計—基本原理與方法。台北：五南。
張添洲（2000）。教材教法-發展與革新。台北：五南。
陳清芳、趨勢科技「紅色警戒小組」(2002)。電腦病毒紅皮書。台北：趨勢教育。
陳朝平（2003）。國民小學資訊教育基礎課程之商榷。國教天地（151），89-96。
曹雅芳（2002）。國民小學教育學程資訊教育相關課程設計之需求評估。淡江大學教育科技研究所碩士論文。中華博碩士論文，90TKU00620008。
陳敬恆（2002）。資訊素養在高中國文科教學中的應用研究。輔仁大學圖書資訊研究所碩士論文。中華博碩士論文，90FJU00448006。
盛群力、李志強（2003）。現代教學設計論。台北：五南。
莊道明（1998）。從台灣學術網路使用調查解析網路虛擬社群價值觀。資訊傳播與圖書館學，5（1），52-61。
張德群（2001）。網際網路與電子商務之安全與認證。絲織園地（37），35-41。
張黎文(2003)。眼科醫師建議小孩 10 歲之後再學電腦。中時電子報。2003.10.07 取自 http://news.chinatimes.com/Chinatimes/
葉儒智（1998）。虛擬實境學習環境之教學設計研究。國立台南師範學院資訊教育研究所碩士論文。中華博碩士論文，87NTNTC395001。
黃光雄、簡茂發（2000）。教育研究法。台北：師苑。
黃宏宇（2003）。以認知行為理論建構病態網路使用與網路敵意模式之研究—以北部三所綜合型大學為例。國立交通大學教育研究所碩士論文。中華博碩士論文，91NCTU0331004。
黃貞芬、許孟祥和林東清（2000a）。資訊時代中倫理導向之決策制定架構。2003.10.09，取自

http://140.109.196.10/pages/seminar/infotec1/ethic.htm.
黃淑珠（2000）。高職學生電腦網路態度、素養及使用現況之調查研究。淡江大學教育科技研究所碩士論文。中華博碩士論文，88TKU00620008。
黃淑靜（2002）。高中職商科教師應用資訊科技於教學之研究。國立彰師大工業教育學系碩士論文。中華博碩士論文，90NCUE0037028。
黃翠玉(2002)。國小電腦使用環境與人體傷害之探討。資訊與教育(92)，111-120。
資訊保安自衛術（n. d.）。2003.11.06 取自
http://www.infosec.gov.hk/chinese/about.htm
電腦使用保健（n. d.）。2003.11.20 取自 http://www.howard2c.com/rsi/
經濟部（2001）。推動電子簽章法計畫。2003.11.27 取自
http://www.esign.org.tw/default.asp
廖述惟（2002）。Spam mail 常見問題集。2003.12.08 取自
http://spam.gsnmm.gov.tw/
榮泰生(2002)。資訊科技一日千里，資訊倫理跟上了嗎？管理雜誌(33)，54-59。
廖肇祥（2001）。瓶中貓／玩笑驚動 FBI 網友連署抗議。2003.11.20 取自
http://www.ettoday.com/2001/06/14/521-490111.htm
劉一賜（1999）。關注自己的網路隱私權。網路通訊（94），65-71。
線上國語辭典。2003.10.01 取自 http://140.111.1.22/mandr/clc/dict/
歐用生（1999）。課程發展的基本原理。高雄：復文。
劉玉玲（2003）。課程發展與設計。台北：桂冠。
劉志明（1998）。向電腦傷害說不。2003/12/11 取自
http://webs.sups.tp.edu.tw/computer/rule/hurt/hurt.htm
蔡均璋（2002）。常見資訊安全機制（二）-病毒防護、安全掃描、入侵偵測。資訊與電腦（261），112-115。
鄭美枝（2000）。台灣電子付款機制之發展與消費者偏好結構調查。國立臺灣大學商學研究所碩士論文。中華博碩士論文，88NTU00318027。
劉莉秋(2002)。散佈電子郵件謠言因素研究-以電腦中介人際互動觀點分析。國立中正大學電訊傳播研究所碩士論文。中華博碩士論文，90CCU00438006。
劉國昌、劉國興（2000）。資訊安全。台北：儒林。
蔡敦仁（2002）。安全議題。資訊種子學校教師團隊培育課程。
歐陽宜珊（2003）。美眾院通過反垃圾郵件法案寄垃圾郵件將罰鍰判刑。
2003.11.23 取自 http://www.ettoday.com/2003/11/23/752-1547879.htm
蔡靚萱（2002）。從「衛生棉長蟲」案談 BBS 討論區的謠言傳播現象。國立臺灣大學新聞研究所碩士論文。中華博碩士論文，90NTU00383005。
盧姿里(2000)。卡通行，漫畫也可以-影像教學法在性侵害防治教育教學的應用。兩性平等教育季刊（13），85-89。
盧鄂生、吳啟文(2001)。電子認證與網路安全管理。研考雙月刊，(25)1，21-29。
謝清俊（1997）。資訊科技人文社會影響計畫。2002.12.27 取自

http://www.sinica.edu.tw/~cdp/article/origin36.htm
謝淵任、周倩（2004，4 月）。中小學資訊安全課程之內涵與設計原則。論文發表於國立屏東師範學院 2004 數位學習研討會，屏東。
譚光鼎（2000）。青少年次文化與人格發展-流行漫畫讀物的分析。中等教育 51（4），11-31。
關淑尤（2002）。台中市國民小學行政人員資訊素養之研究。國立台中師範學院國民教育研究所碩士論文。中華博碩士論文，90NTCTC576049。
龔裕民（2002）。國中學生網路課程學習研究－以九年一貫課程為基礎。淡江大學資訊與圖書館學系碩士論文。中華博碩士論文，90TKU00447001。
Aftab, P. (2000). The parent's guide to protecting your children in cyberspace. Berkshire, England: Mcgraw-Hill.
Aidman, A. (2000). Children's online privacy. Educational leadership, 58(2), 46-47.
Anderson, J. M., (2003). Why we need a new definition of information security. Computers and Security, 22(4), 308-313.
Andy, B. & Geraldine, S. (2000). Some human dimensions of computer virus creation and infection. International Journal of Human-Computer Studies, 52(5), 899-913.
Baird, R. M., (2000). Cyberethics. NY : Prometheus Books.
Chou, C., & Hsiao, M. C. (2000). Internet addiction, usage, gratifications, and pleasure experience – The Taiwan college students' case. Computers & Education, 35(1), 65-80.
Cohen, F. (1999). Managing network security: Security education in the information age. Network security(10), 7-10.
Dick, W., & Carey, L. (1996). The systematic design of instruction. NY: Harper Collins College Publishers.
Doyle, C. S. (1994). Information Literacy in an Information Society. ERIC Digest. Retrieved October 9, 2003, from http://search.epnet.com/direct.asp?an=ED372763&db=eric&lang=zh-tw
Duncan, L. (1995). Practical computer ethics. Berkshire, England: Mcgraw-Hill.
Dwan, B. (2000). The computer virus-From there to here. Computer Fraud & Security, 2000(12), 13-16.
Florence, O. (2002). Fed up with spam. Chronicle of Higher Education, 49(5), 47-49.
Gilbert, B. (2000). Teaching information literacy and computing ethics:Are they the same thing？ International Information & Library Review, 32(3-4), 473-483.
Hester, D. M., & Ford, P. J. (Eds.). (2001). Computers and ethics in the cyberage. Upper Saddle River, New Jersey: Prentice Hall.
Himanen, P. (2001/2002). The hacker ethic, and the spirit fo the information age. 劉瓊云（譯）。駭客倫理與資訊時代精神。台北：大塊。
Hinde, S. (2003). Spam : The evolution of a nuisance. Computers and Security, 22(6),

474-478.
Hinde, S. (2003). Careless about privacy. Computers and Security, 22(4), 284-288.
International Society for Technology in Education (2002). National educational technology standards for teachers: Preparing teachers to use technology. Eugene, OR: Author.
Johnson, D. G. (2001). Computer ethics. Upper Saddle River, New Jersey: Prentice Hall.
Kang, J. (1999). Cyberspace privacy：A primer and proposal. Human rights：Journal of the Section of Individual Rights & Responsibilities, 26(1), 3-6.
Louis, S. (1995). Beware don't stare. NEA Today, 13(9), 19.
Mason, R. O. (1986). Four ethical issues of the information age, MIS Quarterly, 10(1), 5-12. Retrieved October 2, 2003, from http://www.misq.org/archivist/vol/no10/issue1/vol10no1mason.html
McClure, C. R. (1994).Network Literacy: A Role for Libraries? Information Technology and Libraries, 13(2), 116-117.
Plotnick, E. (1999). Information Literacy. ERIC Digest. Retrieved October 9, 2003, from http://search.epnet.com/direct.asp?an=ED427777&db=eric&lang=zh-tw
Pendleton, S. C. (1998). Rumor research revisited and expanded. Language and Communication, 18(1), 69-86.
Poftak, A. (2002). Net-Wise TEENS: Safety, Ethics, and Innovation. Technology & Learning, 22(12), 36-49.
Posner, G. J., & Rudnitsky, A. N. (2001). Course design : A guide to curriculum development for teachers. New York : Longman.
Richard, B. (2001). Hackers profiled — Who are they and what are their motivations? Computer Fraud & Security, 2001(2), 14-17.
Schwartau, W. (2001). Internet and computer ethics for kids. Seminole, Florida : Interpact Press.
Senicar, V., Jerman-Blazic, B., & Klobucar, T. (2003). Privacy-enhancing technologies—Approaches and development. Computer Standards and Interfaces, 25(2), 147-158.
Spam Categories.(2004). Retrieved July 29, 2004 from http://www.brightmail.com/spamstats.html
Spinello, R. A. (2003). Cyberethics-morality and law in cyberspace. London: Jones and Bartlett.
Stephen, B., Heather, G., Ira, S., Steve, R., & Andrew, P. (2003). Where danger lurks. Business Week(3846), 114-118.
Shaw-Mcminn, P. G. (2001). CVS. Review of Optometry, 138(8), 78-85.
Thomas, S. G. (1999). Kid wrists at risk. U.S. News & World Report, 127(1), 62-63.

Top ten ways to protect your privacy online.(n. d.). Retrieved December 22, 2003, from http://www.cdt.org/privacy/guide/basic/topten.html

Willard, N. E. (2002). Computer ethics etiquetty & safety. Danvers, MA : Insternational Society for Technology in Education.

附錄一

中學生資訊安全概念與態度調查表

親愛的同學，您好：

這份問卷是用來瞭解你使用網路的行為以及對於網路的認識，所得的資料除了作為研究之用外，不作其他用途，請你放心，本問卷分為三部分一共二頁，所需回答時間約為 15 分鐘，請務必仔細回答全部的題目。非常謝謝你。

國立交通大學教育研究所教授　周倩

研究生　謝淵任

壹、基本資料

1. 性別：□男 □女
2. 年級：□國一；□國二；□國三；□高一；□高二；□高三；
3. 班級____班；座號____號
4. 家裡有無電腦：有□；無□
5. 每週上網約____小時
6. 常上網的地方（可複選）：□家裡 □學校 □網咖□圖書館 □朋友家裡 □其他____
7. 上網的活動主要是（可複選）：□玩線上遊戲 □找資料 □收發 e-mail 電子郵件 □跟其他人聊天 □玩討論區或 BBS □看文章或新聞 □上教學網站□網路購物 □其他____
8. 在使用電腦時，是否遭遇到電腦病毒或駭客的經驗：有□;無□

貳、以下請同學填答對電腦或網路的了解

一、是非題（請打○或×）

1. （ ）電腦一旦安裝防毒軟體後，就不會中毒。
2. （ ）發現電腦中毒應立即關閉電源，尋求解毒的方法，這樣可以防止病毒繼續破壞。
3. （ ）電腦病毒與電腦蠕蟲其實是指同一種惡意的電腦程式。
4. （ ）駭客原本被定義為「一群高度熱中於寫程式的人」，他們相信透過軟體之間的分享，可以促進資訊與資源的快速流通。
5. （ ）個人重要檔案應加密保護，以防他人偷窺或竄改。
6. （ ）防護性較差的電腦，有可能會變成駭客入侵其他機器的跳板，這樣入侵者可以迴避自身責任。
7. （ ）我國為推動電子化政府，建置政府憑證管理中心（GCA），一般民眾必須從網路下載數位簽章的製作軟體。
8. （ ）數位簽章製作軟體會產生兩個金鑰，公開金鑰是使用者自己保管，私密金鑰是在外流通。

9. （ ）公開金鑰基礎建設（PKI）是以「密碼學」為基礎的安全技術，可以確保資訊在網路作業中不被竊取或盜用。
10. （ ）網路連線安全機制如 SSL，通常具備了私密性與完整性的功能，但無法做到身份的驗證。
11. （ ）「謠言」通常是指未經加以證實的事物，為了避免聽信不實的網路謠言，應該要對網路上的消息加以懷疑。
12. （ ）因為討厭某位老師，故意在網路上散佈有關他的不實言論，這樣的行為並不會違法。
13. （ ）將個人常使用的信箱與公開或註冊用的信箱作區隔，可以有效的防範一些廣告信件的發生。
14. （ ）使用郵件規則或者過濾軟體，可以有效的防範垃圾信件，但也有可能會漏收了自己親朋好友所寄來的信件。
15. （ ）網路是一個虛擬的世界，只要我不使用真實姓名，應該沒人知道我在作什麼。
16. （ ）網站上的隱私保護政策的作用，主要是在保護該網站的隱私安全。
17. （ ）cookies 中譯「網路餅乾」，通常會蒐集有關登入該網站使用者的資訊，同時也會使個人與網站的互動更為密切。
18. （ ）密碼的設定要以簡單好記為原則，所以個人出生年月或是家裡電話是設定密碼的最佳來源。
19. （ ）印表機只是用來列印文件，不太可能對個人的健康產生影響。
20. （ ）電腦的螢幕，應該擺在臉部的右前方，這樣正前方可以放置所需的東西，方便電腦的操作，也讓眼睛跟電腦螢幕保持適當距離。

二、選擇與填充題

1. （ ）「電腦駭客」通常是指下列哪種人？（a）販售不法軟體的人（b）非法入侵電腦系統的人（c）竊取電腦的人（d）破壞電腦硬體設施的人。
2. （ ）電腦病毒的傳染途徑，可經由許多方式來達成，但以下何者為非？（a）電子郵件（b）複製檔案（c）作業系統的漏洞（d）使用者沒有保持個人衛生習慣。
3. （ ）電腦中毒後所可能造成的情形有很多，以下何者為非？（a）儲存在電腦裡的資料不見(b)作業系統損毀(c)使用電腦時會當機或拖慢速度(d)電源供應器燒壞。
4. （ ）關於防制電腦駭客與病毒的方式，以下何者有誤？（a）裝設防火牆（b）時時注意更新軟體公司發佈的最新檔案（c）加強對電腦駭客與病毒的認識（d）不要將電腦連上網路。
5. （ ）要對網路上的消息有所確認，通常有幾種方式，但下列選項何者為非？（a）信賴知名的網站（b）不斷轉發，讓其他人來判斷真偽（c）上網查證相關事項（d）對任何事情都保持合理的懷疑。
6. （ ）網路上的謠言之所以能夠大量的散佈，除了網路訊息散佈快速的特性之

外，主要還具備了什麼要素？（a）謠言似乎可能會發生（b）謠言跟現實有關（c）謠言具有恐懼感（d）以上皆是。

7. （ ）大量的廣告信件，不只會讓個人產生困擾，還可能產生許多影響，但以下何者不是廣告信所可能產生的結果？（a）電腦病毒橫行（b）浪費企業資源（c）網路公司需要購買更大的伺服器（d）拖慢網路速度。

8. （ ）要防止不要的廣告信件，通常可採取幾種方式，以下何者有誤？（a）利用郵件規則來封鎖（b）將信箱做區隔（c）回覆信件，表示不想再收到類似的消息（d）保護自己的信箱不要公開。

9. （ ）在網路上常見的個人資料外洩，通常有幾種方式？（a）透過註冊成為會員的方式（b）透過 cookies（c）透過算命或接受贈品的方式（d）以上皆是。

10. （ ）在網路上洩漏個人資料，將會導致許多情形發生，但下列何者有誤？（a）個人資料遭盜用，從事不法行為（b）增加被他人騷擾或跟蹤的機會（c）疾病史的公開，使人覺得難堪（d）增加抽獎中獎機率。

11. （ ）電腦可能透過哪些部分影響個人健康？（a）電腦螢幕（b）鍵盤（c）滑鼠（d）以上皆是。

12. （ ）傳統電腦螢幕（CRT）輻射線最強的地方是哪一區？我們應該盡量避免在該區域工作。(a) 正
前方（b）正後方（c）左右兩邊（d）上下方。

13. （ ）下列何者是代表電腦螢幕的安全標準？（a）EPA（b）ISO（c）TCO（d）以上皆是。

14. 請寫你（妳）知道或聽過的電腦病毒的名稱或種類（至少兩種以上）：

_____

15. 隨意開啟來路不明的電子郵件可能有哪些危險？（請寫出二項以上）

_____

16. 請寫出二項可以保護你（妳）個人網路隱私的方式？

_____

參、對資訊安全的態度

＊以下題目，請在符合你自己意見或想法的選項上打勾。

題目	非常同意	同意	不同意	非常不同意
1. 我認為在電腦上的資料隨時都有洩漏或遭到損壞的可能。	□	□	□	□
2. 我覺得隨意侵入他人電腦是不應該的行為。	□	□	□	□

3. 駭客只是因為好奇心驅使，入侵電腦網路系統，但沒有造成任何破壞的舉動，這樣的行為是可以被允許的。	□	□	□	□
4. 我覺得裝了防毒軟體之後，可以完全預防電腦病毒。	□	□	□	□
5. 我覺得自己不會這麼倒楣遇到電腦病毒或駭客的攻擊。	□	□	□	□
6. 我覺得電腦病毒非常可怕。	□	□	□	□
7. 我覺得製作電腦病毒的人很缺德。	□	□	□	□
8. 我覺得使用電腦的人，每天都活在電腦病毒的威脅恐懼中。	□	□	□	□
9. 我認為平常多充實對電腦病毒的知識，可以有效的防範電腦病毒的危害。	□	□	□	□
10. 在課堂中，老師教授電腦病毒或駭客的內容對我來說是很無聊的事。	□	□	□	□
11. 我很重視網路購物的安全性。	□	□	□	□
12. 我覺得網路上的資料或訊息有很多是不正確的。	□	□	□	□
13. 我認為網路上的消息大部分是可以完全相信，不需經過查證。	□	□	□	□
14. 對於那些寄廣告信的人，我常覺得束手無策。	□	□	□	□
15. 胡亂寄送廣告信件的人，讓我覺得很討厭。	□	□	□	□
16. 我覺得公開有關個人的身份資料沒什麼大不了。	□	□	□	□
17. 個人的身份資料如果可以在網路上輕易的被他人看到，會使我覺得很不安。	□	□	□	□
18. 在一些需要註冊的網站，我會很小心的填寫有關個人的資料。	□	□	□	□
19. 我認為電腦應該不會對個人健康造成任何影響。	□	□	□	□
20. 我覺得不論使用電腦姿勢的正確與否，適當的休息是很重要的。	□	□	□	□
21. 我覺得長時間不正確使用電腦，會使個人的健康產生問題。	□	□	□	□
22. 我認為自己使用電腦的習慣很正確，應該不會有問題。	□	□	□	□

問卷到此結束，謝謝你的合作！^o^

附錄二

◎ 學生課後意見調查表（請同學勾選你對本課程的看法）

本問卷一共分四部份，前三部份總共十一題,最後一部份則請同學就自己的觀感寫下你對課程的意見。

	非常同意	同意	不同意	非常不同意
一、課程內容				
1.我覺得課程內容豐富並吸引人。				
2.我覺得課程的安排恰當、難易適中。				
3.我覺得課程設計讓我對電腦與網路的瞭解更多。				
4.我覺得在上了本課程後，我會更加注意資訊的安全。				
二、學生的學習				
5.我認為可以從課程中學習到新知。				
6.我認為課程內容能引起自己的學習興趣。				
7.我認為課程中的活動設計可以有效的幫助學習。				
8.我會將所學應用在日常生活中。				
三、綜合評價				
9. 我覺得上完這個課程，對我有很大的幫助。				
10.我覺得在上了本課之後，我會更適當使用電腦與網路。				
11.整體來說，我覺得在本課程中所帶來的成效不錯。				

四、請同學寫出覺得課程中較特為特別或有趣的地方，同時也可以寫下你對本課程的建議或意見！

附錄三

課程發展之專家評估調查表

一、學習單元的評估

評估面向	內容細則	非常不同意	不同意	沒意見	同意	非常同意
課程規劃	1.需求性評估妥適	1	2	3	4	5
	2.能將評估的結果應用在課程設計上	1	2	3	4	5
	3.計算課程所需時數準確	1	2	3	4	5
	4.能列出相關參考資源	1	2	3	4	5
	5.教學資源包含在課程中或容易取得	1	2	3	4	5
課程目標	1.清楚的陳述課程目標	1	2	3	4	5
	2.課程目標可以傳達課程的意涵	1	2	3	4	5
	3.目標能配合課程目的與內容	1	2	3	4	5
課程內容	1.內容生動，可吸引學生的動機與興趣	1	2	3	4	5
	2.課程內容難易適中	1	2	3	4	5
	3.課程實用性高	1	2	3	4	5
	4.內容能與學習者的生活經驗結合	1	2	3	4	5
	5.課程內容可以對學生有實質的幫助	1	2	3	4	5
教學	1.教學能配合學生需求	1	2	3	4	5
	2.教學內容可引起學生共鳴	1	2	3	4	5
	3.教學的順序與步驟適當	1	2	3	4	5
	4.教學策略包含主動與合作性的學習	1	2	3	4	5
評量實施	1.評量是有效、可信的	1	2	3	4	5
	2.清楚說明評量的方式	1	2	3	4	5
	3.評量方式與課程目標相配合	1	2	3	4	5

二、請寫下任何您對本課程的寶貴意見！

附錄四　教學單元介紹

（一）網路安全ｅ起來

單元名稱		網路安全ｅ起來	適用年級	國高中	教學節數	1 節
學習先備條件		1.對電腦有基本的概念 2.學生能簡單的操作電腦 3.懂得網路的基本運用				
教學方法		講述、問答、示範、範例操作、小組討論				
教學資源		1.參考資源：旗立資訊、南一書局、松崗國中電腦（二） 2.教具：notebook、單槍投影機				
分段能力指標	核心能力	1.資訊科技概念的認知 5.資訊科技與人文素養的統整				
	學習內涵	1-2-3 電腦使用安全（二）－教導學生注意軟硬體的保養、備份資料等資訊安全概念。 5-3-3 認識網路隱私權相關法律，保護個人及他人隱私。 5-4-1 認識網路犯罪－了解網路犯罪型態，避免誤觸法網及受害				
教學目標	單元目標	1.瞭解電腦惡意程式的意義與差別。 2.瞭解電腦惡意程式所造成的影響。 3.瞭解相關損壞發生的經過，以及維持電腦正常運作的預防工作。 4.瞭解製作惡意程式行為的合理性。 5.了解電腦駭客行為的適切性。				
	具體目標	1-1 能分辨電腦病毒、蠕蟲以及木馬程式。 2-1 能說出電腦惡意程式所產生的影響。 3-1 能判斷電腦的運作是否正常。 3-2 能展現網路安全的基本防護技巧。 4-1 製作惡意程式行為的合理性。 5-1 能判斷入侵電腦的不法性。				

教學活動	教學資源	教學方法	教學評量
壹、準備活動 一、課前準備 教師對相關的電腦惡意程式如電腦病毒、蠕蟲等資訊有基本的了解，並尋找相關案例，製作成投影片，供上課使用。			
二、引起動機 播放製作的「小明日記」連環漫畫，並詢問是否曾經遭遇過病毒的學生，邀其向全班分享自身的經驗。	單槍、notebook	示範	學生能對所學習的單元產生興趣。
貳、發展教學活動 活動一、 1.教師講述何謂電腦惡意程式如電腦病毒、木馬程式及電腦蠕蟲。 2.舉例不同的惡意程式所產生的影響（圖例介紹）。 活動二、 進行學習活動，將學生分為六組（最輸的人必須表演活動）。 1.教師提供相關案例（例如電腦病毒造成的損壞以及損失），請同學找出惡意程式所可能產生的破壞情形以及如何來防護等資訊，以兩組分別相互競賽，看誰能最快找出。 2. 假設自己是負責電腦系統的人，你要如何來防治惡意程式的破壞，各組尋求相關的防治之道，不可與他組重覆，同時可由前述案例尋求解答（各組進行搶答）。	單槍、notebook 粉筆、黑板	講述法 分組討論 範例操作 分組討論	學生可以分辨不同的電腦惡意程式以及所可能產生的影響。 學生能了解病毒的徵狀，並懂得基本的防護守則。
參、綜合活動 教師提供電腦病毒作者以及電腦駭客	單槍、	講述	學生對行為的判斷

教學活動	教學資源	教學方法	教學評量
的案例說明，最後讓學生分組討論製造病毒、入侵他人系統或植入程式等，其行為情節的輕重，將其排序。教師在本活動中，宜特別注意導正學生的觀念，使學生認知入侵電腦與製造病毒所可能導致後果的嚴重性，避免因為輕忽或抱持好玩有趣的態度，造成無可收拾的局面。	notebook	法與分組討論	是否合宜以及製作病毒的作者或是電腦駭客所可能遭受的懲罰。

教學參考

（一）何謂駭客

最早的駭客是一群在麻省理工學院（MIT）的學生，他們主要的興趣是在了解電腦系統內部的運作，所寫的程式可以開放分享給一般大眾使用，同時也尋求更進一步的交流與發展；根據駭客們透過網路共同編纂的「行話檔」(jargon file)，駭客被定義為「一群高度熱中於寫程式的人」，他們「相信資訊的共享是一種力量強大的美德，並且認為，盡可能藉由撰寫自由軟體（free ware），以及促進資訊及電腦資源的自由流通，以將他們的專業分享給其他人，這是他們的道德義務。」這就是所謂的駭客倫理（hacker ethic）。然而因為時代的遷移，過去主張駭客所應具備的倫理價值觀已經逐漸受到挑戰，並顯得不合時宜了（Duncan, 1995）；今日所謂的駭客，大抵都帶著負面的涵義，用來指那些使用電腦從事不法行為，特別是未經許可擅入電腦系統並竊取軟體的人。

雖然許多人對駭客的定義或分類有所不同，但是大致可以將其歸納為三種，分別為：

1. 好奇心的駭客：只是為了滿足自己對他人相關資訊的好奇心。
2. 耍小聰明的駭客：為了證明自己的能力。
3. 有目的性質的（不論好或壞）駭客：包括報復或為了自己與他人的便利性甚至為了利益入侵，但也有人是為了找出系統的安全漏洞。

即使上述的分類都是針對駭客的入侵動機而言，但並非所有駭客的入侵行為都是不好的具有破壞性的，有些人只是為了滿足自己的好奇心，才會挺而走險，甚至有些人是為了測試系統的安全性，避免讓有心份子有機可趁，釀成更鉅大的傷害或損失，這些都可以讓人重新省思駭客的意涵。

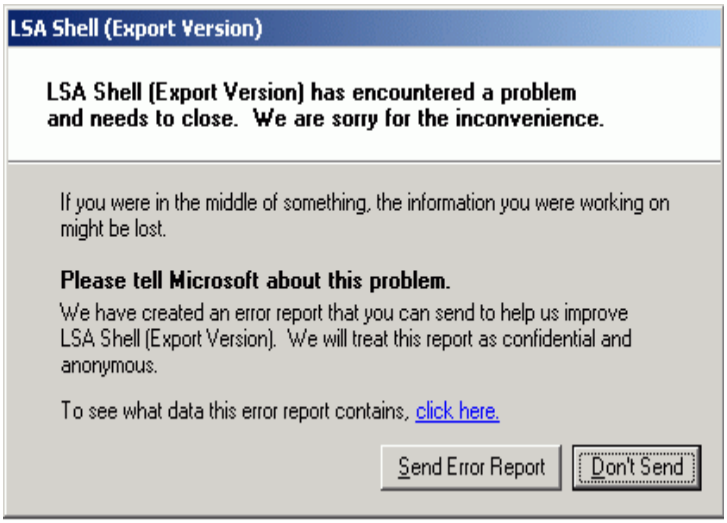
（二）電腦惡意程式的介紹

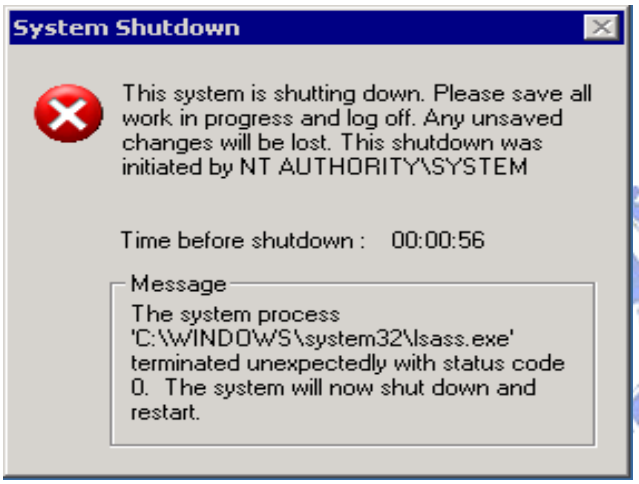
1. 電腦病毒：其實就是用電腦語言所寫的程式，它可以經由複製並造成破壞。
2. 電腦蠕蟲：與電腦病毒最大的不同，便是其可以自行繁殖，例如Ｉ love you，就是透過電子郵件傳送到通訊錄上的每個人。
3. 木馬程式：其實也是一種電腦程式，它會偷偷的放到你的電腦裡頭 ，可以偷取你電腦的密碼、移除電腦中的程式或是監視你在電腦上的一舉一動，通常也會偽裝成吸引人的東西如圖檔、影片等，以電子郵件附件方式傳送到使用者手中。

根據趨勢科技表示，未來的趨勢，是上述三種程式，逐漸的被有心人士整合在一起，變成破壞威力十分驚人的惡性程式，讓個人或是機關、公司蒙受不少的損壞。

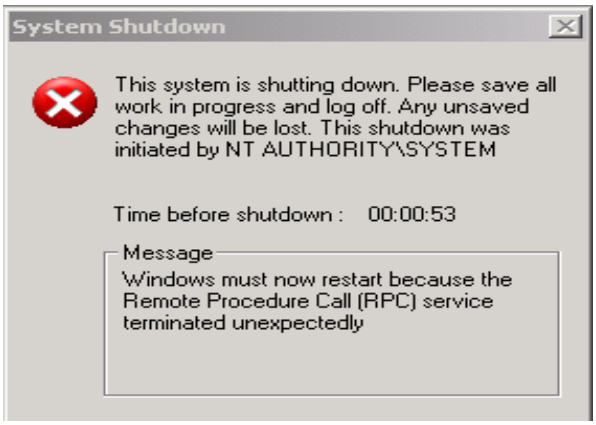
（三）病毒圖示

1.殺手病毒（WORM_Saser_A）

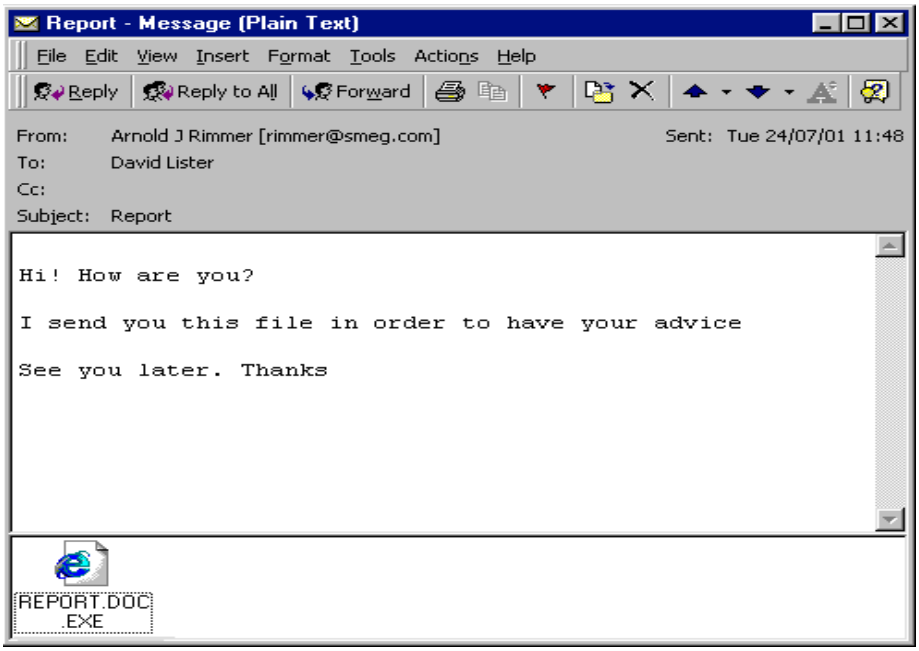




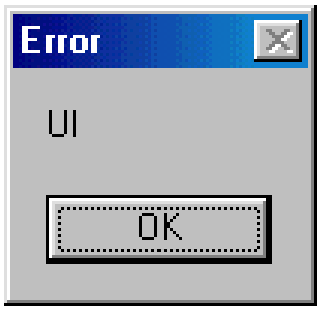
2.疾風（W32/Blaster-A）

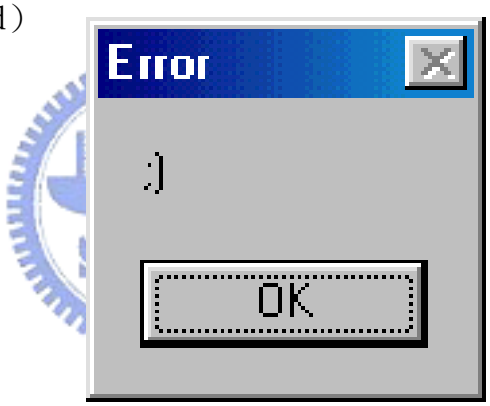


3.思坎（ W32-Sircam-a ）



4. 娜坦病毒（Worm-Navidad）





5.老大病毒 Sobig-F Worm

（圖示取自 http://www.sophos.com/pressoffice/imggallery/virusimg/ ）

（四）電腦惡意程式所可能造成的破壞

1.電腦資料的遺失，例如硬碟遭格式化

2.電腦硬體的損壞，例如主機板 Bios 損毀

3.電腦軟體的損壞，例如電腦軟體的某個檔案損毀

4.電腦系統的不穩定，例如不斷的重開機

5.電腦執行效能降低，例如網路變慢或電腦執行速度緩慢

6.個人的資料外洩，例如電腦遭植入木馬程式

（五）如何防止電腦惡意程式

1.資料備份：定期的對自己電腦上的資料加以備份，並分散儲存，同時做好檔案管理，以將災害降至最低。

2.不隨便下載檔案：免費或公眾軟體，很有可能遭有心人士的變造，植入病毒或木馬程式，因此對這類的軟體，使用者應保持警覺性，此外，在開啟來路不明的檔案時，也應有所警覺所可能產生的後果。

3.使用合法軟體：來路不明的軟體，對於品質的控管不夠嚴謹，不僅在穩定度上有疑慮，也有可能成為他人散布惡意程式的來源。

4.安裝防毒軟體並定期更新：多數的人懂得安裝防毒軟體，但卻缺乏定期更新消息的認知，此外，作業系統的安全漏洞，也是電腦遭受攻擊的來源之一，因此應隨時注意使用軟體的原創公司所發布的各種更新程式。

5.安裝防火牆:個人防火牆的安裝,可以保護電腦降低被攻擊或植入程式的機會。

6.建立基本的電腦常識以及對相關新聞的注意，同時儘量保持冷靜：電腦網路的發達，惡意程式的進化一日千里，因此隨時注意有關的消息或增加相關知識，也是讓自己的電腦遠離災害的方式之一。

電腦病毒案例摘要

名稱	發作徵狀/造成影響	如何感染	如何防止
CIH	格式化硬碟、破壞主	檔案感染	不隨意複製或下

	機板 BIOS。		載檔案或軟體
TaiWan NO.1	自動開啟文件檔	檔案感染	不隨意複製或下載檔案或軟體
13 號星期五病毒	電腦A磁碟機燈不斷亮起，刪除檔案。	檔案感染	不隨意複製或下載檔案或軟體
諾瓦病蟲	癱瘓網路。	隨意開啟不明檔案	不隨意開啟檔案
I Love You	植入木馬程式。	隨意開啟不明檔案	不隨意開啟檔案
疾風	作業系統不斷重新開機。	作業系統安全漏洞	下載軟體更新檔
假好心	植入木馬程式，癱瘓網路。	作業系統安全漏洞	下載軟體更新檔
熊熊蟲	植入木馬程式，資料外洩。	隨意開啟不明檔案	不隨意開啟檔案
Fun love	癱瘓windowsNT作業系統。	檔案感染	不隨意複製或下載檔案或軟體
求職信病毒	移除電腦中的防毒軟體。	預覽電子郵件	關閉郵件軟體中的預覽功能

案例一

電腦安全專家提出警告，一種名為「CIH1.2」的病毒將在二十六日發作，個人電腦硬碟內的所有資料可能被殺掉，甚至無法啟動程式。

自從CIH病毒出現後，二十六日就成為電腦族聞之色變的重要日子。尤其是這個月二十六日，CIH1.2及1.4版同時發作，除了會格式化硬碟，毀掉所有資料外，更可怕的是會破壞主機板上的BIOS，造成無法彌補的損害。

趨勢科技專業講師張嘉太表示，CIH病毒從去年六月起開始流行，專門針對三十二位元的視窗系統下手，也就是WINDOWS98及NT等作業系統。CIH1.2版是四月廿六日發作，CIH1.3版是六月廿六日發作，兩者都會在發作日當天格式化硬碟；CIH1.4則是每月二十六日發作，而且會破壞BIOS，讓電腦壽終正寢，最快的解決之道只有更換主機板一途！

案例二

巨集病毒

9月開始，電腦族要當心！將有不少電腦病毒入侵，「台灣第一」(TaiWan NO.1)就是其中之一。9月13日是第一個發病日期，當天13號星期五與台灣第一都會發病，真是黑色星期五。

根據美國國家電腦安全協會(National Computer Security Assoication)統計，文件巨集病毒已是電腦環境頭號殺手，有 36%的受訪公司曾遭受感染，而且高居感染事件的一半；根據調查，有 20%的病毒感染事件源自網路下載資訊及電子信箱文件傳送。

趨勢科技客戶服務部統計病毒的情況，「台灣第一」(TaiWan NO.1) 已連續四個月高居申訴排行榜冠軍，這隻文件巨集病毒在每月 13 日發病時，會出現四位數字以上的心算畫面，若答錯便會自動開啟 20 個文件檔，甚至還有一種名為亞特蘭大的變種病毒。

案例三

如果你的電腦 A 磁碟機燈一直在亮燈狀態，或是電腦螢幕上出現「 We hope we haven't inconve-nienced you 」這樣的客套話，就可能中了「 13 號星期五病毒」。13 號星期五病毒不會常駐記憶體、也不會攔截中斷向量，只感染 .COM 文件，發病當天若執行中毒文件，將會被刪除。

另外一隻變種稱為耶路撒冷病毒，也以 13 號星期五做為發病條件，但是其感染後遺症卻比前者嚴重。「耶路撒冷病毒」屬於記憶體常駐病毒、會攔截中斷向量，所以感染力較「13 號星期五」強。感染「耶路撒冷」時，.EXE 和.COM 文件長度都會增加，而且會出現系統執行速度變慢的現象。每逢 13 號星期五會在螢幕左下方出現黑色視窗，並會刪除正在執行的程式。

案例四

又見電腦病毒 小心悲慘命運 又名「過期病毒」，也叫「諾瓦病蟲」，主旨顯示 Hi、Hello、Test 或「退信通知」

電腦病毒在猴年和電腦族一起「開工大吉」，三家電腦防毒軟體公司昨天都緊急通知用戶嚴重病毒警訊，有電子郵件主旨說「Ｈｉ」、「ＨＥＬＬＯ」、「ＴＥＳＴ」或奇怪的英文，千萬別開啟附件檔。

此病毒的傳播速率驚人，防毒業者呼籲電腦用戶在收信時，切勿打開不明收信人有附加檔案的信件，並立即更新防毒軟體病毒碼。如果收件匣還具有自動預覽信件功能者，一定要立即進入「檢視、版面配置、預覽窗格」中予以取消，不明寄件者的信件應一律刪除。

案例五

「我愛妳！」是情人間浪漫的對話，不過如果網友這幾天發現即時通訊軟體 MSN Messenger 的對話框，出現「I Love You!!!我愛你!!! 」的訊息，千萬別高興得太早，因為這不是網友傳來的綿綿情話，而是你已經中了「我愛你(I Love You) MSN 網路版病毒」！

這個針對 MSN 即時通訊軟體 MSN Messen-ger 的網路版病毒，是透過「WIN.SCR」或「I Love You!!!.SCR」螢幕保護執行程式，以 email 偽裝誘導使用者開啟這樣的檔案，然後病毒趁機植入木馬程式，透過 MSN Messen-ger 散播「我愛你」的訊息給網友，而這次的「I Love You」病毒也是從去年來第 7 個針對即時通訊軟體的電腦病毒。

由於近年來網友使用即時通訊軟體越來越普遍，其中國內網路使用者普遍採用的 MSN Messenger，更成為駭客攻擊的大宗，從去年至今專門透過即時通訊軟

3.知名駭客米特尼克緩刑期滿

世界最知名的電腦駭客米特尼克曾因非法侵入他人網站而繫獄五年，本周即將緩刑期滿，他打算重回當年觸法的遊樂場——網際網路。

39 歲的米特尼克 21 日緩刑期滿，當天他將在科技產業報導頻道 TechTV 的現場節目 Screen Savers（螢幕保護裝置或螢幕救星）上重登睽違八年的網路。同時出現該節目的還有音樂下載網站 Napster 的創辦人范寧及蘋果電腦創辦人之一沃茲尼亞克。

米特尼克 18 日接受路透訪問時說：「比較困難的是說服企業安全單位，讓他們知道許多關於我的報導都不是真實，至於真實的部分，我覺得很抱歉……我已向社會付出代價，現在我正嘗試做些積極正面的事，我無法改變過去。」米特尼克是第一批遭起訴的駭客之一，他曾被貼上「電腦恐怖分子」的標籤。美國聯邦調查局當初費時三年才找到許多電腦網路遭闖入，以及昇陽電腦、網威和摩托羅拉等軟體公司遭竊的元凶，米特尼克也名噪一時。

他在 2000 年 3 月坦承犯下網路及電腦詐欺及攔截通信等罪案，此後雖獲釋，但旅遊、就業及科技的使用皆受監督及限制。他獲准使用行動電話及電腦，但不可連上網路。米特尼克說：「我很期待能使用電子郵件，我的朋友和家人都因常幫我檢查與列印郵件而覺得煩透。」對於可以使用個人數位助理，他也非常興奮，那是女友送給他的緩刑期滿禮物，一台可無線上網的 Black-berry。他還說：「我已浪費許多時間，錯失許多教育及研究。」

線上資源

網軍入侵，現代木馬屠城記
http://www.iii.org.tw/INCmagzine/147/147_1.htm
趨勢科技病毒教室
http://www.trend.com.tw/endusers/security/primer.htm#1
電腦病毒發作的徵狀
http://www.sophos.com/pressoffice/imggallery/virusimg/
研究電腦病毒網站
http://geocities.com/hotdogcom/index00.html
病毒知識
http://www.rising-hk.com/tradition/antivirus/virus_main.htm
電腦病毒的相關新聞
http://virus.thu.edu.tw/news/news.htm
資訊安全網-防毒常識
http://www.infosec.gov.hk/chinese/general/virus/general.htm
電腦病毒、特洛依以及蠕蟲的不同
http://service1.symantec.com/SUPPORT/INTER/traditionalchinesekb.nsf
聯合知識庫：http://udndata.com/library/

網路安全ｅ起來學習單

一、畫出你心目中「惡意程式」的代表圖樣。

二、寫出你認為最有趣的電腦病毒名稱，並說明其特性。

三、假裝自己是一個遭受電腦病毒破壞的使用者，寫一封約 50 字的信給製造該病毒的作者。

（二）電腦健康百分百

單元名稱		電腦健康百分百	適用年級	國高中	教學節數	1 節
學習先備條件		1. 對電腦有基本的概念。 2. 認識電腦的主要組成原件。 3. 對身體健康資訊有基本瞭解。				
教學方法		講述、問答、示範、範例操作、小組活動				
教學資源		教具：notebook、單槍投影機				
分段能力指標	核心能力	1. 資訊科技概念的認知				
	學習內涵	1-2-2 電腦使用安全（一）：正確規劃使用電腦時間及與電腦螢幕安全距離等資訊安全概念				
教學目標	單元目標	1. 瞭解不當的使用電腦，將會對人體造成傷害。 2. 認識不當使用電腦所可能產生的傷害有哪些。 3. 建立正確使用電腦的習慣。				
	具體目標	1-1 學生能說出不當使用電腦的意義。 2-1 懂得使用電腦不當對人體各部位所可能產生的傷害。 3-1 學生能說出基本的電腦保健知識。				

教學活動	教學資源	教學方法	教學評量
壹、準備活動 一、課前準備 教師事先準備一個電腦工作站圖片，包括電腦主要的組成原件、周邊（如印表機）以及操作電腦所需的桌椅。			

教學活動	教學資源	教學方法	教學評量
二、引起動機 播放教師所製作的風景圖片，同時配合輕鬆音樂，讓學生擁有視覺與聽覺的雙重享受，接著讓同學閉上眼睛，想像如果哪天自己再也無法去到各地去旅行，看不到那些美景，聽不到清脆悅耳的聲音，會有什麼感觸，請同學發表自己的想法。	單槍、notebook	示範	學生能對所學習的單元產生興趣。
貳、發展教學活動 活動一、驚天動地九十秒 教師發一張電腦工作站的圖，讓學生分組討論工作站設計不良所可能引發的各種人體的傷害，各組並派出一人將可能的情形寫出，本活動的進行要在限定三分鐘內完成，教師並在隨後進行補充。	粉筆、黑板	小組討論	學生能指出工作站設計不良，對人體所可能產生的危害。
活動二、搶救健康大作戰 針對剛剛各種可能引起的病變，尋求解決之道，各小組討論之後回答。 **參、綜合活動** 1. 教師講解有關電腦的規格 2. 請同學想像自己是一位從事販售電腦工作站的業務員，該如何來說服家長購買你所促銷的產品，各組	粉筆、黑板 單槍、notebook	小組討論 講授、小組討論、演示	學生能說出操作電腦應注意之事項，以避免各種傷害。 學生能運用老師上課所提及的相關內容，進行實地演練。

教學活動	教學資源	教學方法	教學評量
討論結束後，找出一人來演示。			

教學參考

（一）電腦使用不當可能造成的傷害

1. 姿勢不良：包括不當使用鍵盤、滑鼠以及坐姿不良等，產生如頭痛、頸肩部僵硬酸痛、脊椎神經的傷害，多數是因為缺乏活動筋骨或坐姿不正確而造成身體上的不適。
2. 缺乏休息所受的傷害：眼睛的過勞是電腦族群中最普遍的疾病，包括眼睛疲勞、視力模糊衰退等使用電腦所引起的視力徵候群，而持續長時間的工作，對於身體骨骼與肌肉的傷害也是主因之一。
3. 電腦輻射的傷害：學家在某些研究中，輻射線會對一些動植物產生某種程度上的傷害，一些研究甚至提出對電器產品與癌症或流產之間的關注。
4. 環境的傷害：造成傷害的另一個原因，很多時候也是由於設備所引起的，據調查學生在學校所使用的電腦桌椅等設備多數是為成人所設計的，學生們不得不遷就設備而採用不良的姿勢。

（二）避免不正確或不當使用電腦

1. 要有充足的休息：每小時休息 10 分鐘，每日使用不宜超過 4-6 小時。甚至只要覺得身體不舒服就休息。
2. 避免暴露在電腦螢幕下的時間過久：研究指出，螢幕後方的輻射量是最高的；此外與螢幕的距離最好保持七十五公分以上（一個手臂的距離）。
3. 養成良好習慣並充實保健常識：良好的擺設位置以及正確的操作姿勢是亟待建立的觀念，此外，許多電器產品的安全規格，對人體所可能產生的影響都有一定的檢測標準，因此對產品安全規格等相關知識的了解，將可以有效的預防電腦所引起的傷害。

（三）電腦螢幕規格認識

1.能源之星（為美國環保署 EPA 之註冊商標 ）

（取自中華民國能源之星
http://www.energystar.org.tw/Chtml/OUTLINE.HTM）

由美國環保署所發起的一連串自發性資源汙染防治以及節省能源的計劃，擁有該標誌代表該產品可以符合節省能源的功能。

2.MPRII

MPRII 為由瑞典科技檢驗局（SWEADAC)所制定的，有關電磁輻射量的規範；只要是符合 MPRII 的規就表示這台顯示器的輻射量與辦公室其它的電器產品相較之下要低得多。

3.TCO-95、TCO-99、 TCO’ 03

（取自 TCO Development http://www.tcodevelopment.com/）

由瑞典職業公會低輻射標準，較 MPRII 更為嚴格的低幅射量要求，TCO-99 除包含 TCO-95 所有的規範之外，還有更嚴格的人體工學，環保標準之規定，而且除了電腦、顯示器和鍵盤，也有越來越多印表機、傳真機和影印機產品加入它的審核認證。

（四）人體工學

1. 人體工學就是瞭解性別上、年齡的不同在工作遊戲以及休憩時必須注意的各種設計要素。人體工學包括人們在操作機器、工作於各種環境中的能力，同時也考慮到使用者和操作元的安全、舒適和生產力。
2. 廠商在進行工業產品設計時，依循人體工學因素設計出來的產品，讓消費者在使用其產品時，真正能感覺到操作的方便和舒適感，以提高工作效率。

線上資源：

電腦工作桌椅尺寸建議值-勞工局
http://www.iosh.gov.tw/data/f12/e7.htm

印表機會散發臭氧？
http://www.ettoday.com/2004/02/11/517-1584927.htm

電腦操作人員健康手冊
http://www.klhpb.gov.tw/new_page_25.htm
RSI 大綱
http://www.howard2c.com/rsi/overview.htm
TCO’03 認證
http://www.beareyes.com.cn/2/lib/200306/14/20030614131.htm
HealthyComputing
http://www.healthycomputing.com/
TCO Development
http://www.tcodevelopment.com/

電腦健康百分百學習單

一、請你找出下述的電腦工作站如果設計不良或使用不當，對人體所可能引發的傷害。

二、針對上述的傷害，你要如何去改善？

（三）網路逍遙遊

單元名稱		網路逍遙遊	適用年級	國高中	教學節數	1 節
學習先備條件		1. 對電腦有基本的概念。 2. 對網路的基本特性有所瞭解。 3. 學生能利用網路資訊。				
教學方法		講述、問答、示範、範例操作、小組討論				
教學資源		教具：notebook、單槍投影機				
分段能	核心能力	5.資訊科技與人文素養的統整				

力指標	學習內涵	5-3-1 了解與實踐資訊倫理,遵守網路上應有的道德與禮儀。 5-3-3 認識網路隱私權相關法律，保護個人及他人隱私。 5-4-2 適時運用資訊科技，透過網路培養合作學習、主動學習的能力。
教學目標	單元目標	1.瞭解網路謠言的特性。 2.瞭解謠言所可能產生的影響。 3.確保網路資訊的可靠性。
	單元目標	1-1 學生能說出謠言的意義。 1-2 學生懂得網路訊息散布的特性。 2-1 學生對謠言所產生的衝擊能有所警覺。 2-2 學生懂得查證網路訊息。

教學活動	教學資源	教學方法	教學評量
壹、準備活動 一、課前準備 教師蒐集具有特色的網路謠言案例，製作成投影片，作為學生上課討論用。			
二、引起動機 播放教師製作的狀況劇，並詢問學生是否有類似的經驗，請同學跟大家分享。	單槍、notebook	示範	學生能對所學習的單元產生興趣。
貳、發展教學活動 活動一、 1.教師講述何謂謠言，謠言具有哪些特性使人相信。 （講述完後請同學就老師所發的學習單，對第一題進行討論） 2.舉例不同的謠言所產生的影響（圖例介紹）。 活動二、 教師提供一些網路謠言，讓	單槍、notebook 粉筆、黑板 單槍、	講述法 範例操作 分組討論 分組討論	學生懂得謠言的意義，並知道網路謠言成功散布的因素。 學生瞭解謠言的可怕，是經由有心人士根據事

教學活動	教學資源	教學方法	教學評量
學生猜測事件的真假。 （接著請同學對學習單內的第二題做答） 活動三、 老師讓學生分組討論，如何對網路訊息的有效性加以確認，最後進行補充。(之後進行學習單第三題做答） **參、綜合活動** 進行分組活動，教師將學生分為六組，並由老師出題目，讓學生由前傳到最後的人，最後的人說出答案，是否與最初相同，本活動的進行，可以讓學生了解訊息以訛傳訛的可怕。	notebook	講述法與分組討論	實加以改編。 學生能掌握基本的資訊查證技巧。 學生在活動過程中，藉由人與人傳遞的方式，瞭解維持資訊正確性的困難。

教學參考

（一）何謂謠言

1. 在群眾間針對某個對象、事件或是符合大眾興趣的問題，而流傳開的一種說明或未經証實的解釋便稱為「謠言」(rumor)，謠言藉由網路的媒介流傳，便稱為「網路謠言」。

2.據美國 UCLA 大學的調查，在 12 到 17 歲的網路使用者中，有超過一半的人認為網路上的訊息大部份甚至是全部可信的。

（二）成功或一般流通謠言散布的特性

1.多數成功的謠言具備的三種特性，分別為

（1）謠言是有可能會發生的（例如新版算命程式會讓自己的身份資料外洩）。

（2）謠言涉及到某些我們所知道的或認為是真實的事件（例如經由器官的移植而感染到愛滋病）。

（3）謠言被加入恐懼感（例如熱桔茶會溶解塑膠杯）。

2.一般流通的謠言所具備的要素有：

一般流傳的謠言通常具下列的要素：

（1）與現實有關的訊息：謠言是一種訊息，傳遞的是與時事或現實相關聯的訊息，也就是說謠言所傳播的訊息是大眾有興趣的現實事件。

（2）未經証實：謠言是一種未經証實其真實性為何的訊息。

（3）使人相信：謠言的目的在於使人相信，通常具備了強而有力的說服訊息。

（4）口耳相傳：藉由人際之間的溝通來傳遞資訊，而且通常人與人之間所交換的資訊，常常是沒有真實或確切的證據來支持，而謠言往往也是在人際階段散布的最快。

（三）有趣的網路謠言

1.加拿大的跨海大橋

謠言內容：有人表示，已經收過這封 Mail 很多次了，每次收到都直接刪除，也沒再轉寄出去，因為他從頭到尾都不相信真有這麼長的橋……」；照常理判斷，一座蓋在海上，長達 13 公里的大橋，聽起來就很跨張，再看照片，怎麼看都像是合成的。

查證結果：但實際上真有這麼一座橋，地點位於加拿大。

2.竹籃子公司

這是 1 家製作竹籃子的公司，總公司蓋成 1 個竹籃子的形狀，位在美國的俄亥俄州，堅持將公司蓋成這付模樣的是該公司的創辦人；當時他提出要將辦公大樓外型蓋成竹籃子的想法時，無論是僱員或是建築師，大家一致認為這只是個玩笑話，但他最後還是完成了這個大夢；不過這樣的一棟建築物，照片一放到網路上，就讓大家開始猜測，到底這是真是假。

3.在伊拉克發現的怪蟲

謠言內容：

它們是跑時時速可達 10 英里,跳可高達 3 呎的夜行性蜘蛛，除非它們處在陰暗的地方,不然只會在晚上出來活動，當它咬你時,你會被注入一種麻醉劑,

因此你會很快的陷入麻痺,失去知覺，當你在睡覺時,你甚至會不知道你被咬了,所以你醒來的時候會發現自己某部分的腿或者手臂已經不見了,因為已經被蜘蛛們整晚慢慢的啃斷掉了。

查證結果：

圖上的動物並不是什麼未知的大蜘蛛，就算在沙漠中看到了，也不用擔心你會跑不贏牠，更不用擔心這種小動物有能力吃掉你，或是讓你中毒。牠是屬於蛛形綱（aracnida）避日目（solifugae），夜行性，沒有毒線，龐大的大顎是用來咀嚼（好像是）獵物的。

4.澳洲巨貝島

謠言內容：

真令人震撼..大自然的鬼斧神工!!

國家地理協會(National Geographic Society) 日前在澳洲大堡礁東南方64 海浬 處上空拍攝到這座無人島嶼的照片。小島實際上是沉積成型在一枚已經鈣化的遠古巨硨磲蛤(Hippopus)的上殼。目前紀錄上所發現最大的活體巨硨磲蛤殼長約僅為十五公尺(1997 年於菲律賓外海)，科學家表示，這枚巨硨磲蛤

至少已有三千五百萬年以上歷史。
查證結果：這是一張合成照片

5.中台禪寺的多啦A夢

網路上流傳著埔里中台禪寺有尊多啦A夢小叮噹雕像，這真的讓人感覺很神奇，怎麼莊嚴的佛殿會突然出現漫畫裡的小叮噹？真的有嗎？會不會戲謔了點？中台禪寺見允法師說，是的，有的，就在中台山的菩提公園「鹿野園」裡，而且有2尊。

6.千萬不要點熱桔茶

謠言內容：

今天下午有人點了熱桔茶23杯及珍珠奶茶22杯，送到後同仁發現所有盛裝熱桔茶的保麗龍杯都被桔茶的強酸所腐蝕，有的甚至到了穿孔的地步！
與店家反映的結果，老闆另行補送23杯珍珠奶茶，並解釋該店產品因為使用新鮮桔汁與檸檬汁，故酸性較強，目前無法找到可以足以抗其酸度的免洗杯。
查證結果：很有可能是溫度過高才導致腐蝕的現象發生，而並非原作者所言是因為裝了桔茶的關係。

7.這是我們的自來水管？

謠言內容：

這是我們的自來水管,A 驚死人!今年挖到水管.....150mm,我看到這張照片我不敢喝水.....我們的自來水管?在全省&南部高雄還有六成以上的管路二十年沒有更換，因此建議雖然高雄水質有改善..但是..水還是不能生飲的。

查證結果：圖片中的水管是否真為自來水管，目前無法證明，但推測比較像是下水道的污水管。即便是如此，自來水還是燒開了再飲用比較不會有衛生上的顧慮。

（以上網路謠言摘自東森新聞網路追追追 http://www.ettoday.com/etrumor/index.htm）

8.SARS 期間的綠豆謠言

第一個版本:
這是剛剛發生的事!
我妹妹打電話來跟我說~
他同事的妹妹剛剛生下了一個寶寶
嚇人的事發生了
寶寶一出生就開口說話告訴媽媽
這次的非典型肺炎會死很多人
要大家凌晨 12 點以前去煮綠豆湯
但是不能加糖絕對不能加糖
說完寶寶就死了不要不相信.
這是真的我妹還看過那個孕婦喔我真的嚇呆了
第二個版本:
我外公告訴我媽媽
我媽媽告訴我

澎湖有個剛出生的嬰兒
一出世 就喊著 黑糖 & 綠豆
第三個版本:
不管你信不信...喝綠豆湯可防 sars
因為我姐夫家是開中醫的...
有個病患跟他們說...長庚有個病患..他是個啞巴
但在今天他說了一句說"喝綠豆湯可防 sars"...說完就死了....
醫院在場的人都嚇到了..因為那個人一生出來就是啞巴
你可以不相信...但這是真的...反正綠豆也很好吃
如果不信我想可以去長庚問問...如果我知道那個病房的病患
再告知大家...
第四個版本:
一位 103 歲的乙八喪..掛掉後..過三天
他爬起來說要吃綠豆湯...抗 sars
他說..閻羅殿.已淪陷..他被派回來居家隔離....

（四）辨別網路訊息的真偽

1. 信賴知名的網站：可以引導學生透過學校或圖書館許可的連結來搜尋資料，或是瀏覽搜尋引擎所提供的目錄連結
2. 謠言查証網站：例如國內外有幾個知名的網路謠言查証網站，來防止謠言的無限擴張。
3. 透過可信度較高的大眾媒介進行追蹤報導。
4. 網路討論區的自律：例如在 BBS 討論區內另可以觀察到網友提供闢謠資訊，同時 BBS 站內的管理機制也同時運作
5. 對任何事物都保持合理的懷疑。

（五）與衛生保健相關的報導

1.點選醫療網站 認明榮譽標章

「止汗劑導致乳癌？」「百分之九十的人臉上有寄生蟲？」「B 型肝炎疫苗與禿頭有關？」這些聳動的標題都來自醫療網站，但你能分辨它們的真偽嗎？衛生署昨天公布廿八個優良醫療網站名單，即日起這些網站的首頁都將標示由衛生署頒發的優良榮譽標章，可讓民眾在瀏覽醫療資訊時有所保障，不被錯誤訊息誤導。全部得獎優質醫療網站名單可至 http：//awards.doh.gov.tw：8080/網站瀏覽。

衛生署長涂醒哲表示，網路是現代人重要資訊來源，但如何讓民眾在閱讀資料時更有保障，不因錯誤訊息而恐慌，也不受到商業網站誤導，政府有必要從目前參與評選的兩百一十三個醫療網站中每年定期評選優良網站，並授予認證標章，以提供民眾選擇。這次獲獎的網站分四大類，分別為個人組、教學醫

院組、與醫療有關的基金會及學會組、商業性網站組，其中以一己之力架設網站並能獲獎者共有八人。

台大醫院小兒科主治醫師李秉穎在八十八年架設「GQ 的兒科小棧」網站，當時完全憑著一股提供民眾正確醫療知識熱忱，利用公餘時間摸索二、三個月才架設成功。李秉穎說，網路上有很多文章是假造的，背後可能有商業利益，很多患者常拿網路下載來的資料質疑他的診斷，或者詢問他「羊奶、蜂膠是否可改善氣喘」等在網路上廣為散播的訊息，尤其 BBS 站上的言論，更常有人蓄意傳播錯誤訊息，民眾如果無法分辨，很容易受到誤導。李秉穎強調，很多醫療網站提供問答服務，但只能解答一般原則，絕不能下診斷甚至開處方，因為每個個案都有特殊性，醫療網站只能諮詢，絕不能取代醫師眼見為憑的診斷。

開業皮膚科醫師陳衍良和同為皮膚科醫師的太太賴碧芬，共同創設「輕鬆美膚網」，創下每天一、二萬人次點選率的超人氣，訂閱電子報人數高達二、三萬人，也讓他的診所成為台北公館地區新地標。陳衍良說，他的網站有一個「解密網路謠言」專區，專門破解錯誤的醫療訊息，另外每天限定十位網友提問，並保證在廿四小時內回答的服務，也很受歡迎。夫妻兩人每天花在回答問題、更新內容的時間超過三、四小時，非常辛苦，但能夠獲得衛生署肯定，他感到很值得。

【2003-02-18/聯合報/11 版/生活】

2.西醫：晨喝冷飲 好嗯嗯

很多人相信，早晨喝冰飲吃寒食會傷胃，有網路傳言說，早上喝冰咖啡、生機飲食果汁等冷飲，是感冒、皮膚不好甚至致癌的凶手。但胃腸科醫師不以為然，甚至建議有便秘困擾的人，早晨起床後不妨喝杯冷水，可讓腸胃加速蠕動有助排便。

網路傳言說，早餐應吃熱豆花、熱豆漿、芝麻糊、山藥粥或廣東粥等。如果老是吃不結實，或是大便老是稀稀的，或是皮膚越來越差，是喉嚨老是隱隱有痰不清爽，時常感冒，小毛病不斷，都可能和冰冷冷的飲料有關，還會造成胃黏膜、胃壁組織之僵化、硬化等等，並說很多小女生從小冰品、可樂、紅茶不斷，結果導致月經不來、子宮急速老化、18 歲更年期就到了；或說骨癌的小女生戒除冰品後，癌症痊癒。

台北榮總胃腸科醫師黃以信說，早晨起床後喝冷飲會傷胃的說法，在西醫找不到關聯性，且喝冰水不會增加胃酸，最多是消化不良。馬偕醫院肝膽胃腸科醫師王蒼恩表示，早晨喝冷飲造成腸胃不適，可能與個人體質有關。黃以信和王蒼恩反而主張，便秘的人早晨喝杯冷開水，可以刺激腸胃道蠕動有助消化，但如果喝了不舒服，就不要喝。個人飲食習慣比較重要，不必刻意避免冰冷飲食。許多西方孩子早晨起床後，習慣喝一杯冰鮮奶或冰果汁，長期以來也沒有證據顯示，西方人腸胃因此比較差。

黃以信提醒說，水不可以喝多，以免造成「水中毒」，因為腎臟功能差的

人，如果喝太多水，有可能一時排不出去，造成「水中毒」。
【2004-05-03/聯合晚報/11 版/身・性・靈】

3.試用化妝品 恐怖乙

口紅、眼影拿了就塗 好像一把牙刷大家用

母親節檔的化妝品熱賣季又來了。但不少女生最近都收過一封「小心免費試妝」的電子郵件，呼籲女人最好少用化妝品櫃檯或賣場的開放性試用品。台大皮膚科主治醫師蔡呈芳說，過去確實有共同化妝品及器材致嚴重細菌感染的病例。

這封網路消息引用中國大陸的報導指出，在 10 分鐘內一支口紅就畫了近 20 名顧客，營業員稱，一支口紅可以試畫近 300 名顧客。眉筆、睫毛膏等產品同樣是大家混用。還有工作人員用相同的器械工具和化妝品，為三個人做了全套化妝，連洗手的水都沒有換。

報導中並有醫師說法，說混用化妝品會導致口腔疾病、皮膚病、肝病、愛滋病等疾病， 並說這形大家共同一把牙刷般不衛生。蔡呈芳說，雖然不少網路傳言常危言聳聽，不過這封算是頗具參考價值的。因為共用化妝品特別是眼睛周遭的眉筆、眼影或是睫毛膏等，最是危險，過去就曾有人感染綠膿桿菌或黴菌。

不過蔡呈芳說，依他的觀察，知名品牌的化妝品櫃檯已注意到試妝的衛生，會建議消費者在手背上試，或用拋棄式的試妝棉棒等。不過有些開架式的化妝品試用品，如口紅、眼影等，仍有消費者拿起來就往臉上塗。尤令人擔心的是，有些消費者權充彩妝模特兒，但化妝大師的化妝器材顯然是重覆使用，衛生條件恐多不佳。不僅試用的化妝品，很多人習於在家中姊妹或母女共同化妝品、化妝粉撲、蜜粉刷、唇筆或睫毛膏等，同樣有交叉感染的可能。
【2004-04-19/聯合晚報/11 版/身・性・靈】

線上資源：

網路追追追
http://www.ettoday.com/etrumor/index.htm
網路謠言、都市傳奇、紅豆泥研究院
http://www.richyli.com/hondoni/index.htm
網路謠言與都會傳奇
http://www.wei1105.idv.tw/comp/journal/rumor-1.htm
輕鬆美膚網-解密網路謠言
http://www.ezskin.com.tw/

網路逍遙遊學習單

一、你覺得電腦網路、電視、廣播、書本、雜誌、報紙等媒體，哪個所提供的訊息比較正確，請依你覺得最正確的排到較不可靠的。

二、找出你覺得最有趣或讓你印象最深刻的網路謠言，並試著分析其散布的原因。

三、想一想，如果你收到或聽到某些資訊，但又無法確定其真假，通常你的反應為何？有沒有比較好的處理方式？

（四）個人資料不漏白

單元名稱		個人資料不漏白	適用年級	國高中	教學節數	1 節
學習先備條件		1. 對電腦有基本的概念。 2. 對網路的基本特性有所瞭解。 3. 學生能利用網路資訊。				
教學方法		講述、問答、示範、範例操作、小組討論				
教學資源		教具：notebook、單槍投影機				
分段能力指標	核心能力	5. 資訊科技與人文素養的統整				
	學習內涵	5-2-1 認識網路規範，了解網路虛擬特性，並懂得保護自己。 5-3-1 了解與實踐資訊倫理，遵守網路上應有的道德與禮儀。 5-3-3 認識網路隱私權相關法律，保護個人及他人隱私。 5-4-2 適時運用資訊科技，透過網路培養合作學習、主動學習的能力。				
教學目標	單元目標	1. 瞭解個人隱私為何，並懂得在網路上洩露個人隱私的潛在危機。 2. 能建立保護個人隱私的基本認知。				
	單元目標	1-1 學生能說出個人隱私的意義。 1-2 學生能舉出個人資料外洩所可能遭致的後果。 1-3 學生能知道什麼是垃圾郵件。 2-1 學生懂得保護網路上有關個人資訊的基本技巧。				

教學活動	教學資源	教學方法	教學評量
壹、準備活動			

教學活動	教學資源	教學方法	教學評量
一、課前準備 1.教師蒐集網路上註冊所需登錄的個人資料細項，作為學生討論之主題。 2.教師尋找有關洩漏個人資料並遭受損失的案例，作為投影片供學生參考。			
二、引起動機 播放教師所製作的狀況劇，並詢問學生所認知的個人隱私為何？並讓學生討論是否有類似的劇中的經驗。	單槍、notebook	示範	學生能對所學習的單元產生興趣。
貳、發展教學活動 活動一、 1.教師講述隱私的意義，強調在網路上個人資訊的重要性。 2.舉例個人資料洩漏所可能產生的影響(ex.從垃圾信件的氾濫，到自己的身分遭盜用、竄改或從事犯罪行為等)。	單槍、notebook	講述法 範例操作	學生懂得個人隱私的意義，以及在網路上洩漏資料所可能造成的後果。 學生知道什麼是垃圾郵件，以及可能產生的影響。
活動二、 1. 老師將所準備的個人資料細項，分為三類，分別為個人身分資料、個人通訊資料以及家人資料等，並讓學生分六組討論，討論其中可以公開或不能公開的項目，小組跟小組間可以互相對不同的主張提出疑問。 2. 教師進行最後的結論。	單槍、notebook	分組討論 講述法	學生了解個人隱私的詳細內容，並對其重要性加以分辨。

教學活動	教學資源	教學方法	教學評量
活動三 由前面的活動，學生了解在網路上個人隱私的意義，而本活動的進行，所討論的是在網路上如何保護個人資料的外洩。老師給予提示，讓全班分組來進行搶答，以回答最多的一組為優勝。 **參、綜合活動** 教師講解學習單的內容，並請同學儘量將上課所學予以發揮。	粉筆、黑板	講述法與分組討論	學生懂得如何保護個人資料的方法。 學生能運用上課所學的內容表達出來

教學參考

（一）網路上的個人隱私

網路的普及化，讓個人隱私逐漸為人所重視，一般來說，隱私包含了兩個要素，分別為「有能力掌握自己的資訊」以及「能完全掌握有關自我的價值」，第一個因素存在現有的法律條文中，個人可以對自己的訊息作交代，至於第二個要素就比較難達成，尤其目前的電子交易盛行，許多人在還沒察覺中就不經意的洩漏出自己的資料，一些公司甚至很少提出保護消費者隱私的相關措施。

（二）網站所提供的個人化服務

根據網站上的主張，個人化服務對使用者可能有兩個好處：

1. 節省時間：讓使用者可以快速找到所需的資訊，節省使用者的時間。
2. 拓展視野：使用者可以有機會得到行家的建議，或是獲得跟他生活形態相近的人所接觸的資訊。

但事實上，使用者在填寫個人資料之後，卻無法確保其是否會遭他人洩露或濫用。

（三）常用蒐集資料的方式

一般公司在蒐集資料的方式，大約可以將其分為直接或間接兩種方式：

1. 個人資料會透過如免費郵件空間、線上購物、網路社群、網路徵才、線上算命、冒牌網站以及醫療網站等管道曝光，歸納其共通處，都是提供一些服務來吸引使用者註冊，其中尤以免費電子信箱最能吸引大量使用者，是目前相當普及的服務，使用者的人數相當多。
2. 間接資料的蒐集，是藉著在電腦上放一些小程式，稱做 Cookies，它可以用來作為網站伺服器與使用者電腦相互溝通的工具，並在使用者的電腦中儲存某些資訊，但使用者可以自行設定取消與否，並選擇是否接受 cookies。

（四）個人資料外洩可能帶來的後果

如 1. 被他人冒用身份，來從事不法行為，使得個人承擔很多的責任。
2. 增加被騷擾與跟蹤的機會：例如家中通訊資料被他人獲得，將很有可能遭不明人士的搔擾，或不斷的收到不必要的資訊，如垃圾電子郵件。
3. 個人的私密資料遭公開：例如個人疾病史被他人得知。

（五）垃圾信件所指為何？它會產生什麼影響？

1. 用來指將一份內容相同的電子郵件，未經收信人許可，大量寄給很多人而其內容多數是與收信人不相干的商業廣告，一般用「Spam」來稱呼；Spam 原本是指一種流行在二次大戰期間但是卻在六十年代被大家所排斥的一種豬肉罐頭，因為多數人都認為這種速食罐頭沒什麼營養，久了就把 Spam 跟沒營養的東西、氾濫成災、喧賓奪主、剝奪他人選擇權利的行為聯想在一起，近來隨著網路普及，慢慢的把垃圾郵件叫做 Spam。
2. 垃圾信件會產生什麼影響？

（1）佔用網路的頻寬：此舉可能會耗費郵件伺服器的處理效率，使公司不得不多花經費購買更大伺服器以維持一般的工作運作。

（2）造成個人困擾：例如侵犯了個人的隱私，也佔用使用者的硬碟空間，更糟的是，據調查，百分之四十九的美國人每週必須多花超過四十分鐘來刪除垃圾信件，他們每週刪除垃圾信件的次數比他們所做的其他活動還多出許多。

3.如何防止垃圾信件的產生

（1）利用「郵件規則」封鎖或使用過濾軟體：多數的郵件軟體都有該功能，只是也要小心避免將一些私人信件被過濾掉了。

（2）保護自己的郵件位址：通常是最為人所熟知的方式，使用者應該儘量對所註冊的網站做過濾，並避免四處註冊而留下自己的信箱，讓自己的 e-mail 成為他人利用的目標。

（3）將信箱作區隔 ：例如將私人常用信箱以及免費用來註冊用信箱作區隔，也可有效達到減少垃圾信件的產生。

（4）收到垃圾信件時刻意的忽略它：許多電子郵件內容會註冊如不想再收到該信，請按回覆，您將不會再收到該信。此舉只是一種用來確認信箱是否有人使用的技倆。

（5）向 ISP 檢舉：對所使用的網路服務業者提供發垃圾信的來源或帳號，也是對垃圾信件的管制措施。

＊濫發電郵 可罰 2000 萬 匿名最高判 5 年

NCC 籌備處擬草案 商業電郵須加註「廣告」濫發每封罰 500 元到 2000 元 求償無需舉證

國家通訊傳播委員會（ＮＣＣ）籌備處和電信總局研擬完成「濫發商業電子郵件管理條例」草案，違法發送垃圾郵件，每封最高賠償收信人兩千元，若匿名寄發，最高可處五年以下有期徒刑、併科一百萬元罰金，全案最快九月送立法院審議。

ＮＣＣ籌備處昨天表示，考量垃圾郵件被害人不易舉證，損害金額也很難估算，民眾或電子郵件服務提供者請求民事賠償時，不需提供損害證明，而由法院依據每封新台幣五百元以上、兩千元以下，合計不超過兩千萬元標準，裁定賠償金額。ＮＣＣ強調，兩千萬元上限僅適用同一封垃圾郵件，若信件內容不同，則補償必須分開計算。對部分垃圾郵件來自大陸、美國、韓國等地，追查不易，ＮＣＣ說，過去其他國家也曾反映，有些垃圾郵件以台灣的 HiNet 為跳板，但受限於無法可管，無法提供實質協助；待「濫發商業電子郵件管理條例草案」通過，將可本於互惠原則，與相關國家合作，共同追查不法電子郵件來源。

ＮＣＣ籌備處參考美、日、歐盟等國制度，研擬「濫發商業電子郵件管理條例」草案，明訂未來寄發商業電子郵件，必須提供收信人選擇不再接收相同信件的機制，並在郵件主旨欄加註「商業」、「廣告」或「ＡＤＶ」的標示，以及提供正確的信首資訊和發信人的身分資訊及郵遞地址。草案也賦予電子郵件服務提供者在可能危及設備機能的情況下，拒絕提供傳送或接收垃圾郵件的權利。對於部分來源不明、或為躲避查緝，以國外為跳板的垃圾郵件，ＮＣＣ籌備處特別加重處罰，明訂以隱匿或標示不實的身分和信首資訊，發送垃圾郵件，處兩年以下有期徒刑、拘役或新台幣廿萬元以下罰金，若以此為常業者，處六個月以上、五年以下有期徒刑，並得併科廿萬元以上一百萬元以下罰金。

ＮＣＣ籌備處透露，待整個商業電子郵件管理上軌道後，不排除比照美國，協調相關團體建置全國性拒絕商業電子郵件位址的資料庫，供民眾自行註冊，業者在寄發電子郵件前必須到資料庫確認，收信人名單是否有已經註冊拒收商業電子郵件的人，並提前剔除。

3.個人資料外洩 民眾不堪其擾

台東縣政府消費者服務中心昨天接獲部分民眾投訴，抱怨個人資料外洩，之前也有生意人上網購買個人資料，結果收到錯誤資料；消保官張英美也是受害者，曾接獲勒贖電話，她說情況真的很嚴重，中央應正視。

縣政府消費者服務中心昨天接獲三通消費者投訴電話，抱怨個人資料外洩，每天有接不完的電話。一名家庭主婦說，她的手機號碼很少告訴別人，但一天要接獲十幾通電話，詢問她要不要申辦銀行貸款，讓她不勝其擾。一名生意人表示，電信業者聲稱，若消費者懷疑個人資料外洩，願意免費受理更換門號，「我做生意十幾年了，生意做那麼大，主要靠這個門號，如果更換門號我怎麼去一一通知人家，不可能嘛。」這名生意人邊說邊罵。

消保官張英美說，針對消費者資料外洩，行政院消保會昨天開會討論，初步有兩個方向，一是索求補償金，若個人資料在洩漏名單之列，免月租費一至三個月；另一是賠償金，依個人實際受損情形賠償；但至目前還未最後定案。張英美表示，消費者資料外洩情形確實非常嚴重，她之前也接獲許多手機簡訊，多數是詐騙資料；甚至曾接獲勒贖電話，對方聲稱她的女兒在他手中，向她勒贖十萬元。張英美認為，消費者經常接獲許多奇奇怪怪的電話，主要是有集團或個人販賣個人資料，行政院消保會應重視網站販售個人資料的嚴重性，並應禁止公司利用他部門資料介紹其他產品，干擾消費者。

4.慎選求職網站 慎防資料被賣

隨著求職管道激增，新鮮人求職大多透過報紙分類廣告、人力網站或是親友人脈找工作，由於網路時代來臨，約有八成新鮮人選擇上網找工作，人力業者建議，新鮮人必須慎選求職網站，以免個人資料外洩，惹禍上身。

隨著各家人力銀行成立，網路儼然成為新鮮人最常利用的求職工具，但網路求職陷阱多，而且履歷資料包括身份證字號、出生年月日、家庭背景、學經歷等個人機密資料，如果落入不肖集團手中，後果將不堪設想。

udnjob.com 人事線上總經理沈瑋表示，警方曾經破獲一個利用偽造身份證申請信用卡盜刷牟利的犯罪集團。警方發現，犯罪集團竟然利用年輕學子在人力網站登錄的個人資料，藉機偽造身份證件申請信用卡。沈瑋分析，如果求職者沒有選擇公信力強、聲譽卓著的人力網站登錄履歷，將會輕易地將完整的個人資料在網路空間曝光，每曝光一次，就多一次個人資料被被不肖業者濫用的可能性。

國內的人力資源網站達數十家，但僅有少數的人力網站，完全依據就業服務法登記為合法的私立就業服務機構。如何篩選合格、正派經營的人力網站，求職者得花點心思注意。沈瑋建議，新鮮人可以打聽網站業者的品牌口碑，以及業者是否嚴格篩選徵才廠商；此外，網站是否確實嚴密保全資料庫。

沈瑋建議，求職者刊登履歷資料前，可先主動聯繫人力網站的客服人員，了解網站篩選求才企業的標準為何？網站如何妥善管理資料庫？求職者也可進一步以公司名稱或統一編號到經濟部商業司（www.moea.gov.tw）查詢，勞委會職訓局網站（www.evta.gov.tw）也會定期公布違反就業服務法的業者。求職者必須眼觀四面、耳聽八方，多聽多問，注意求職網站的可信度，就可避免個人資料被不肖業者盜賣，淪為受害羔羊。

【2004-06-24/經濟日報/38 版/職場天地】

（六）保護網路上的個人隱私

1.使用者本身在隱私概念的認知

例如思考個人資訊公開的程度，對個人資料那些可以公開或不公開，都可以再加以考量，此外對他人的隱私也要予以尊重。

2.增加使用者電腦的技巧

如確認網路上的安全機制、拒絕不必要的網路餅乾、清除電腦上的暫存記憶體等，這些與使用者對電腦軟體使用技巧的閑熟度有關，透過一般教科書或資訊課程的教學，便可以習得相關技巧。

線上資源：

兒童網路隱私保護法

http://www.jcic.org.tw/000502.htm

網路隱私權

http://infotrip.ncl.edu.tw/law/privacy.html

Kids' Privacy on the Net

http://lrs.ed.uiuc.edu/wp/privacy-2002/kidsprivacy.html

CDTs Guide to online privacy

http://www.cdt.org/privacy/guide/start/

GetNetWise

http://www.getnetwise.org/

網路隱私學習單

一、個人資料的外洩

（1）在網路上，註冊成為會員會不會使自己的資料外洩？

（2）除此之外，還有什麼方式會不小心就讓資料外洩？

二、請問你是否曾到網路上註冊成會員？使用哪些服務？就你所知還有沒有其他類似的網站提供類似的服務？

（1）□有□無

（2）

網站名稱	服務內容
	□資訊（例如新聞、天氣、健康、時尚、電子報等） □社群（交友、聊天、家族、即時通訊等） □商務（旅遊、拍賣、購物等） □個人服務（如個人網頁、相簿、通訊錄、行事曆等） □娛樂（電影、音樂、遊戲、算命）

附錄五 「網路安全ｅ起來」教學媒體

小明日記 Part Ⅰ	小明日記 Part Ⅱ