Computer security: Investigating the impact that security specific education has on users’ behaviour

Samuel David Jones
*Edith Cowan University*

Follow this and additional works at: [https://ro.ecu.edu.au/theses_hons](https://ro.ecu.edu.au/theses_hons)

Part of the Information Security Commons

**Recommended Citation**

This Thesis is posted at Research Online. [https://ro.ecu.edu.au/theses_hons/1018](https://ro.ecu.edu.au/theses_hons/1018)
Edith Cowan University
Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author’s moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
COMPUTER SECURITY: INVESTIGATING THE IMPACT THAT SECURITY SPECIFIC EDUCATION HAS ON USERS' BEHAVIOUR.

Samuel David Jones
Bachelor of Science (Computer Science)

This thesis is presented in fulfilment of the requirements for the degree of Bachelor of Computer Technology (Computer Science) Honours

Faculty of Regional Professional Studies
Edith Cowan University

November 2005
USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.
ABSTRACT

A lack in end-user awareness in computer security issues provides the rationale for this investigation. The research considers whether or not the provision of an educational package addressing computer security issues will improve awareness and transform behaviour of end-users in assessing and enacting appropriate responses in computer security situations.

A group of twenty participants was studied in detail using a mixed methods research approach. The participants were drawn from a cross section of computer end-users, from elementary to advanced levels of computer literacy.

Outcomes include a positive response to the provision of material, however human factors were found to be equally important in affecting the way the end-users assess and react in computer security environments. Package interactivity, empowerment for end-users to prioritise and make their own assessments was found to be critical factors.
DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education.

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Signature: .........

Date: 2-8-2006
ACKNOWLEDGEMENTS

First and foremost, I would like to acknowledge my parents, Peter and Cate.

To my sister Rowie, who has put up with me for 19 years and counting.

Lindsay Offer; for supervising and guiding me in my academic endeavours.

To Angelo Zampogna and Nancy Akl, two of my closest friends. For giving me four years of unconditional friendship, I only hope I gave as much in return.

To all my lecturers: Viv Campbell, Rainer Winkler, Lindsay Offer, Steve Eaton, Terry Haines and Kerry Rodgers. Without your support, guidance and patience I would not have made it this far.
# TABLE OF CONTENTS

**USE OF THESIS**

**ABSTRACT**

**DECLARATION**

**ACKNOWLEDGEMENTS**

**1.0 INTRODUCTION**

1.1 Rationale ............................................................................................................ 6
1.2 Research Question .............................................................................................. 7
1.3 Investigation Design ........................................................................................... 7
1.4 Scope .................................................................................................................. 8
1.5 Overview of Document ...................................................................................... 8

**2.0 BACKGROUND**

**3.0 LITERATURE REVIEW**

3.1 Computer Users ................................................................................................ l2
3.2 Computer Crime ............................................................................................... 13
3.3 Computer Security ............................................................................................ 21
3.4 Education .......................................................................................................... 26
3.5 Significance ...................................................................................................... 28

**4.0 METHODOLOGY**

4.1 Comparing Quantitative and Qualitative Data ................................................. 29
4.2 Outline of Available Research Designs ........................................................... 30
4.3 Research Data ................................................................................................... 34

**5.0 DESIGN AND IMPLEMENTATION**

5.1 Developing the Educational Package ............................................................... 35
5.2 Gathering Participants ...................................................................................... 39
5.3 Pre-Package Questionnaire .............................................................................. 39
5.4 Presenting the Package .................................................................................... 40
5.5 Initial Post-Presentation Questionnaire ............................................................ 41
5.6 Quantitative Two Week Post-Presentation Questionnaire ............................... 41
5.7 Qualitative Post-Presentation Questionnaire .................................................... 42

**6.0 RESULTS**

6.1 Quantitative Results ......................................................................................... 44
7.2 Qualitative Results ........................................................................................... 48

**7.0 ANALYSIS**

7.1 User Awareness ................................................................................................ 50
7.2 User Behaviour ................................................................................................. 51

**8.0 CONCLUSIONS AND FUTURE RECOMMENDATIONS**

8.1 Research Question ............................................................................................ 54
8.2 Limitations ....................................................................................................... 54
8.3 Future Recommendations ................................................................................ 54

**9.0 REFERENCES**

56

**10.0 APPENDICES**

10.1 Appendix A – Presentation ............................................................................ 61
10.3 Appendix C – Initial Post-Presentation Questionnaire ................................. 69
10.4 Appendix D – Two Week Post-Package Questionnaire ................................. 70
10.5 Appendix E – Final Qualitative Questionnaire .............................................. 72
10.6 Appendix F – Population Demographics ....................................................... 74
10.7 Appendix G – Population Behaviour ............................................................. 75
10.8 Appendix H - Population Willingness to Change Behaviour ....................... 77
1.0 INTRODUCTION

Since the Internet's creation, there has been a dramatic change in the way people live and work. Computers and the Internet are used for financial transactions, banking, storing highly sensitive information and a range of other activities. These activities, in a non-computing context, would require a high level of security. The environments from which many users operate from home and work contain many possible security flaws and exploits introduced by users. An attacker, if willing, may employ a wide array of techniques to take advantage of this extensive range of exploits.

This investigation's aim is to discover whether improving end-users' knowledge of relevant exploits and how they are taken advantage of will produce safer behaviour and implementation of computer security countermeasures. It is argued that if computer users can be empowered with this knowledge they will change their behaviour, providing a safer operating environment. Greer (1977, p. 9) states that "the task of education is to change behaviour", this investigation will assess whether or not the provision of an educational package addressing computer security issues, could be shown to change end-users behaviour.

1.1 Rationale

Humans are frequently referred to as computer security's 'weak link' (AusCERT, 2004; Wade, 2004; Pfleeger and Pfleeger, 2003). Wade (2004) states, "all too often it is the people aspect that breaks down" (p. 1). Figures from AusCERT (2004) show that annual losses for computer crime or computer misuse or abuse, increased by 20% compared to 2003 (p.3). For all organisations surveyed the most common problem in reaching an effective information security solution was changing end-user's knowledge and attitudes.

"With the rapid and widespread propagation of today's worms and viruses, technology solutions are, by themselves, inadequate. Organisations need to asses the vulnerability of their system software, features and configurations, and increase user awareness and education." (AusCERT, 2004, p. 18)

AusCERT (2004), states that "since the last Australian Computer Crime and Security Survey, AusCERT¹ has seen a steady increase in the number, and sophistication of scamming techniques directed against users of online banking and electronic banking

¹AusCERT – Australian Computer Emergency Response Team
sites” (p. 24). This provides justification for an investigation concerning to what extent (if any), end-users can be empowered with knowledge on possible attacks and exploits (and how to prevent them), and whether or not this will provide a safer operating environment.

1.2 Research Question

The research question driving the investigation is:

“Would the provision of an educational package addressing computer security issues change end-users’ behaviour and use and implementation of computer security systems?”

Addressing this question provides an insight into the behavioural effect of increasing users’ knowledge.

1.3 Investigation Design

The investigation was conducted using an explanatory approach to mixed method research as defined by Cresswell (2003). An educational package, in the form of an easily understood presentation aimed at the end-user who has a minimum amount of computer literacy, will be developed. The presentation explains, in basic terms, how intruders may gain access to computer systems, malicious software and techniques that may be employed to make computing safer. Participants complete an initial questionnaire outlining demographic information along with their perceived understanding of computer security issues. After presenting the package to twenty participants, data concerning the end-user’s willingness to use more secure systems are collected and analysed. Three questionnaires are presented to participants following the package presentation; one initially and two after a two week period. The first two questionnaires gather quantitative data concerning participants’ perceived change in awareness and behaviour. This is followed by a qualitatively based questionnaire outlining their perceptions of the package. It is proposed that this qualitative data will provide insight into details such as how understandable package was, how comfortable the subject felt and how they felt the presentation could have been improved.
1.4 Scope
The sample population for the investigation contains twenty participants from the Bunbury area. The population demographics include any person, of any age, who use computers either for personal computing or work related tasks. Data on the participants' responses who are not actively involved in computing is not relevant to this investigation. This investigation will not include wireless networks or wireless security issues. The research will explore the various definitions of hackers and crackers, from these definitions a standard definition for this paper will be identified and used.

1.5 Overview of Document
The following section provides a view of the investigation's background. The literature review examines existing knowledge in the fields of human involvement in computing, computer crime, computer security and education. The explanatory approach to mixed method research, as the adopted methodology, is then discussed in chapter four accompanied by a justification for its selection. The investigation design and implementation is presented in chapter five providing a view of how the investigation was performed. A summary of results, adapted from the investigation feedback is presented in chapter six. Chapter seven analyses these results providing a discussion on the effectiveness of the study. Chapter eight draws conclusions from the study and summarises the investigation, also, an outline of recommended future work is provided.
2.0 BACKGROUND

Computers are used in hospitals, businesses, banks and households. They are often used to store important and sensitive data. A lack in computer security in any of the above areas has the potential to disclose information such as patient records, trading policies and client data for businesses, credit card information and account details in banking and personal information in home computing. This list, adapted from Capron and Johnson (2003, p. 7), outlines the relevant principal areas where computers are currently used.

- Law Enforcement – Computers in law enforcement are used to store national fingerprint files, nation wide files describing the mode of serial killers, computer modelling of DNA and DNA databases which can be used to match hair, blood and other evidence, offender records, sex offender records, court proceedings, witness locations and other highly sensitive information.
- Money – Computers are widely employed in banking as well as online banking. The use of computers in this field speeds up record keeping, allowing banks to offer same day services. “Computers have helped to fuel the cashless economy, enabling the widespread use of credit cards and instantaneous credit checks by banks and retailers” (Capron and Johnson, 2003, p. 7).
- Government – Taxes, social security issues, immigration databases are among the uses of computers in government.
- Home – Computers in peoples homes are used for Internet banking, purchasing products online, keeping records, preparing budgets and range of other social, economic and recreational activities.
- Health and Medicine – “Computers help to monitor the seriously ill in intensive care units and provide cross-sectional views of the body” (Capron and Johnson, 2003, p. 7). In addition to this computers are used to store patient records, diagnosis information, prescription details

As shown, computers used in these areas, come into contact with and contain highly sensitive data. For example, criminal records and court proceedings in law enforcement, financial details in money, patient information in health and medicine and personal details in home computers. Computers containing such information are typically secured using network equipment. However, Ernst and Young (2004) state the
following: “No amount of technology can reduce the human dimension” (p. 3). Humans however, when using these services introduce a range of security vulnerabilities and threats.

Outside of computing, the physical security surrounding banks is extremely high. Cameras monitor the bank, money is stored in a vault, and clients must provide sufficient identification before making transactions. Regarding Internet banking, the connection from a home computer to the bank, may appear to be highly secure. However, if the home computer is compromised, then all information entered into the computer (credit card details, passwords and personal identification numbers) is available to an attacker. Computers may become comprised by an end-user failing to take simple precautions, such as using a secure password, checking the authenticity of emails and not installing erroneous software.

The identification of poor user awareness and poor security culture has been identified, however, this has not spurred changes to educate users and improve security culture (AusCERT, 2005):

Inadequate staff training in computer security management (47%) and poor security culture within organisation (40%) were among the top vulnerabilities reported. This compares to 61% of respondents who identified changing users’ (staff) attitudes and behaviour towards computer security practices a challenge for them. (p. 4)

This extract demonstrates the contrast between organisations acknowledging user awareness and security culture is a problem and their willingness to deal with it. In addition only 61% of respondents identified changing these attitudes as a challenge. The survey found that 79% of respondents stated their organisation should “…do more to ensure an appropriate level of IT security qualification” (AusCERT, 2005, p. 12).

Threats to computer users are constantly changing and evolving. Evidence of evolution is apparent in the establishment of a new Internet based scam. Phising targets computer users directly through a socially engineered form requesting personal information. This information usually allows the attacker access to some form of online service such as banking. Riley and Spencer (2005) state “the perpetrators of the phising scams set up a simple con, usually in the form of an email, to lure the victim into surrendering private information”. The information may be credit card numbers, personal identification
numbers, account numbers, passwords to systems or an entire range of personal details. Riley & Spencer (2005) assert “Trend said the phising scams were usually easy to spot, but succeeded because people failed to take the necessary precautions”. This quote highlights, once more, the important of user awareness and education.

A justifiable need exists for organisations to increase computer security awareness among employees. The CSI/FBI underlines that, “for some time, it has been widely recognized that computer security is as much a management problem as it is a technology problem” (p. 4). Despite this however, the following was reported in a 2005 study directed by AusCERT: “only 7% of respondent organisations reported they were managing all computer security issues reasonably well (compared to 5% in 2004 and 11% in 2003 and 2002)” (p. 1). With computer security companies estimating two thousand malicious threats are emerging every month (McAfee, 2005, p. 5), computer users and businesses are faced with an increasing need to do improve computer security. User awareness and behaviour has been clearly established as the main barrier in achieving effective computer security. Greer (1977) states, “the task of education is to change behaviour” (p. 9). It is therefore a natural conclusion that an appropriate step towards an effective computer security solution is the development of an educational package designed to educate and inform end-users.
3.0 LITERATURE REVIEW

This literature review examines and discusses the role and impact of humans in computing, computer crime, computer security and effective adult education. Each section is of critical importance to the investigation. This literature review explores how the human factor impacts on computing, what current threats exist, how these threats may be mitigated or prevented and how the end-users should be educated.

3.1 Computer Users

Dix, Finlay, Abowd and Beale (1998) note humans’ importance in computing, “the human, the user, is, after all, the one whom computer systems are designed to assist” (p. 12). Bishop (2003), states that “the heart of any security system is people” (p. 21). However, Pfleeger and Pfleeger (2003) elaborate that “people are the weak link in any security system…” (p. 596). This emphasises that while people are at the core of any security system, they also represent the weakest link in that system. Pfleeger and Pfleeger (2003) present the following reasons behind the introduction of weaknesses by people in security, “whether through carelessness, poor understanding, pressure, or simple human error, insiders unintentionally expose private data” (p. 596). Wade (2004) supports this notion, he states that:

All too often it is the people aspect that breaks down. Whether it is naiveté, ignorance or simply a lack of training, more and more employees are unwittingly opening a gateway in their company networks to any number of unauthorized users. (p. 1)

This view is endorsed by Ernst & Young (2004) who surveyed 1, 233 organisations from 51 countries and duly discovered that a “lack of employee awareness” was listed as the top obstacle in providing an effective computer security solution. Out of the 1,233 organisations surveyed, “less than half the respondents provided their employees with ongoing training in security and controls” (Ernst & Young, 2004, p. ii). This survey shows that despite the obvious importance of the human factor in computing security, companies are not paying enough attention to user training and awareness programs. AusCERT (2004) supports this stating that the most common difficulty for organisation was “changing user attitudes and behaviour (reported by 65 percent of respondents)” (p. 3). AusCERT further reveals that the total losses for only 57% of the respondent organisations were 16 million dollars, with an average loss of 116, 212 dollars per organisation.
AusCERT (2005, p. 30) provides a graphical representation of which vulnerabilities contributed to an attack on surveyed organisations over a twelve month period. Respondents were asked: “In terms of your organisation’s potential vulnerabilities, what factor may have contributed to those attacks which harmed the confidentiality, integrity or availability of your network data or systems in the past twelve months?” (AusCERT, 2005, p. 30). AusCERT (2005) reveals that “inadequate levels of security on home and other computers used by clients, customers and staff” (p. 30) was listed by 26% of respondents in 2005 as contributing to attacks. AusCERT (2005, p. 30) found that “inadequate staff training and education in security practices and procedures” was listed by 47% of respondents as contributing to these attacks. In addition to this “poor security culture in organisation” (AusCERT, 2005, p. 30) was considered by 40% of organisations as contributing to attacks. For 2005, these factors represent three of the top four vulnerabilities listed by organisations.

Ware (2003) states, “in terms of security policy, companies are doing the ‘blocking and tackling’ technique and covering user behaviour, employee awareness and network and system administration issues” (p. 1). However CSI/FBI (2004) show that “on average, respondents from all sectors—except the high-tech sector and the federal government—do not believe that their organization invests enough in security awareness” (p. 4). This highlights the difference in views between organisations. Peltier (2004) reiterate the need for employee awareness in stating “employees must be educated, or made aware, that they will be expected to protect information” (p. 345).

The above establishes the notion that user awareness is a critical factor in computer security and that educating end-users on computer security issues will improve security. The need for strong computer security established the growing threats to computer systems and end-users.

3.2 Computer Crime

This section focuses on the main threats posed to computer users. These threats are: cracking, fraud, social engineering, denial of service attacks, malicious software and password crackers. Each threat falls under the heading of ‘computer crime’ which is defined by Pfleeger and Pfleeger (2003) as “any crime involving a computer or aided by the use of one” (p. 20). Accurately quantifying the total financial loss due to computer
crime remains a very difficult task. However according to McAfee (2005, p.2), the Federal Bureau of Investigation estimates the overall financial loss is close to 400 billion dollars.

3.2.1 Hackers and Crackers

It is important that an initial distinction is made between hackers and crackers. It is beyond the investigation's scope to argue either way; however, a clear distinction will be made. Jewkes (2002) argues that "the 'true hacker' would claim that pointless vandalism within computing is the work of crackers (usually defined as criminally motivated cyber-trespassers) not hackers" (p. 131). This view is supported by Schwartau (2000), who states that "crackers are criminal Hackers. Since so much hacking is truly useful to the information industry as a whole, it's difficult to label hackers as 'bad'" (p. 41). Schwartau (2000) continues to explain that "hacking does cross into blatantly illegal behaviour, which the US (and other countries) has strictly defined" (p. 41). The following are two important American laws outlined by Schwartau (2000) that constitute criminal behaviour in computing, thus distinguishing a hacker from a cracker.

1. If you possess passwords to a computer network that you do not have permission to use, you have broken a US federal law and perhaps many others.

2. If you actually enter a computer system without permission, even if there are no security controls or password blocking mechanisms, you have also committed a felony (p. 41).

This suggests that simply gaining unauthorised access to a computer system is illegal, and therefore the work of a cracker. Anonymous (2003) defines a hacker as "a person intensely interested in the arcane and recondite workings of any computer operating system" (p. 47). Anonymous (2003) continues to explain that hackers would never intentionally damage data, continuously seek knowledge and always share freely their knowledge. The author contrasts this definition with that of a computer cracker, he states, "a cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent" (p. 47). Unauthorised access, destroying vital data and otherwise causing problems are all distinguishing features of a cracker.
This section establishes the difference concerning hackers and crackers as malicious intent and/or actions (cracker), as opposed to the quest for knowledge and technical enlightenment (hacker). For the purposes of this document reference to individuals who gain unauthorised entry into any computer system will be achieved using the term ‘attacker’.

3.2.2 Hacking

In this section the concept of hacking is addressed, for the purposes of this section the concept will be examined in relation to gaining unauthorised access to a computer system from a remote location. It is beyond the scope of this section to make a distinction between hackers and crackers as this has been addressed in a previous section (section 3.2.1). For the purposes of this section hacking refers to gaining entry to a computer system from a geographically remote location, whether or not it is condoned as illegal activity or not is irrelevant, this section will explore the basic mechanisms used to do so, and the information required.

Anonymous (2003) provides a basic description of hacking and the methods employed by hackers. One aim of this investigation is to present basic information to a group of computer users with little computer literacy, therefore, content from this source will serve as a guide to what information should be presented to participants. Anonymous (2003, p. 97) presents an introduction to hacking. He begins with an introduction to TCP/IP and an explanation of how it works. Following this, network and application level protocols are described including a view of ports. This description is adapted for the purposes of this literature review in order to focus on information relevant to the investigation.

Anonymous (2003) describes the Internet Protocol address (hereafter IP address) as “...a unique identifier for a system on the network” (p. 106). The author continues to describe IP addresses as being 32 bits long, containing 4 numbers, each a byte, separated by decimal points: for example 32.96.111.130. The workings of TCP/IP are outside the scope of this investigation as it is deemed too advanced for users with little computer literacy (whom the investigation is aimed at) Anonymous (2003) describes that connections to computers are “made using a system of ports” (p. 111).
3.2.3 Fraud

According to Lekakis (2005) Internet fraud is costing the National Australia Bank one million dollars per month. He continues to explain that this could blow out to thirty million dollars by the end of the year (article published in July) and the overall cost of Internet fraud to Australian banks could be as high as seventy million dollars per year. Jewkes (2002) presents many scams and exploits that occur on the Internet. These exploits are often aimed at users who are not educated about the risks of computing. Jewkes (2002) covers issues such as identity theft, cyber-stalking, cyber-society, and various other activities.

"The Internet provides unparalleled opportunities for those seeking a new identity to access the necessary information... Detailed information regarding individuals may be available on personal or workspace websites as well as via professional organisations of which the individual is a member." (Jewkes, 2002, p. 94)

Jewkes (2002) explains "businesses have responded to the growth of the Internet by offering online services that provide impostors with the opportunity to engage in fraudulent conduct 'at arms length'" (p. 95). Jewkes (2002, p. 95) provides further insight into this increase in crime by explaining that online businesses provide a sense of anonymity that increases the chance of individuals engaging in fraudulent activities when they would otherwise not risk it in person. Poci (2005), states that in the past five years, Internet fraud has cost consumers five billion dollars.

3.2.4 Social Engineering

Bishop (2003) presents the concept that computer security deals predominately with security controls that can be bypassed by human intervention (p. 21). Social engineering exploits the human factor in computer security in order to trick users into disclosing information, usually authentication details such as usernames and passwords. An example of a social engineering attack is an attacker making a phone call to a highly situated person in a company (such as a vice president), claiming to be an employee of the company who needs his/her username and password for a highly important situation (Bishop, 2003, p. 21). Once the person, who believes the request, discloses their username and password the attacker has access to the system without having to bypass any technical counter measures such as firewalls. Schwartau (2000) avows that you should "never give out personal information on the phone to people you don't know. Telephone solicitation is a great criminal scam. Be especially cautious about cellular
phones” (p. 100). Schwartau (2000) covers hackers, phreakers, identity theft, and Internet terrorists. The publication presents a large number of social engineering techniques and real life instances where they have been used. Many of these instances are unconfirmed and unofficial, however they present a possible reality and are therefore are important to consider in terms of possible attacks.

While socially engineered telephone calls present a threat to computer security, socially engineered emails are responsible for countless security breaches. These emails also represent a growth sector in online threats. Socially engineered emails are being used to coerce users into disclosing personal details regarding financial services via phising. McAfee (2005) defines phising as using spoof e-mails or directing people to fake Web sites to fool them into divulging personal financial details so criminals can access their accounts (p.19). Lepofsky (2004) supports this definition in stating that “phishing scams involve fooling consumers into giving their personal data to thieves masquerading as legitimate banks, credit card companies and other e-commerce operations” (p. 1). According to Symantec (2005) the number of phising threats has grown from an average of 3 million per day to around 5.7 million in the six months prior to September 2005. McAfee (2005) assert phising email complaints now make up more than half of the 15,000 complaints filed monthly to the FBI’s Internet crime center (p. 14). This underlines the financial implications of socially engineered threats and the extent to which they exist.

### 3.2.5 Denial of Service Attacks

A Denial of Service (hereafter DoS) attack is an attack that intentionally disrupts or denies a service or function to legitimate computer users, computer networks or computer systems (Anonymous, 2003; McClure, Scambray & Kurtz, 2001). McClure, Scambray and Kurtz (2001) describe a DoS attack as a threat causing system downtime, lost revenue, and labour increases for tasks such as identifying and recovering from the attack. The following list, adapted from Anonymous (2003, p. 298) explains three ways in which DoS attacks work.

1. Bandwidth Consumption – An attack against network resources. Aimed at making the network slow or stop this attack causes the inability of users to access web sites, email and any files stored on the network.
2. Resource Saturation – Every computer system has a finite set of resources, these include memory, storage, and processor capabilities. This attack involves using up one or all of these resources and is aimed at making the system unusable.

3. System and Application Crash – These attacks exploit a pre-existing program flaw that, when triggered, cause a system or application crash.

This underlines the mechanisms behind DoS attacks. When combined with malicious motives DoS attacks present a serious threat to end-users and organisations. Another threat to end-users is malicious software. With the exception of insider abuse of system resources and laptop theft, malicious software represents the most common form of attack and is responsible for the greatest financial loss for organisations (AusCERT, 2005, p. 17).

3.2.6 Malicious Software

Allen (2001) and Noakes-Fry (2004) identify three types of malicious software: Trojan horses, viruses and worms. Definitions and characteristics of Trojan horses, viruses and worms are identified as follows.

Schwartau (2000) defines a Trojan horse as follows: “In simple English, a Trojan Horse is a software program that is inserted into a computer without you knowing it” (p. 201). Trojan horses provide attackers with a range of information contained inside the infected computer. They may also create a ‘back door’ in to the infected system. Anonymous (2003) provides a more succinct definition of a Trojan horse:

A Trojan is a program that claims to perform some desirable or necessary function, and might even do so, but performs some function or functions that the individual who runs the program would not expect and would not want (p. 352).

As established, a Trojan horse infects a computer without the user’s knowledge, it then performs some undesired function.

Cohen (1985) cited in Anonymous (2003) describes a computer virus as “a program that replicates by ‘infecting’ other programs, so that they contain a (possibly evolved) copy of the virus” (p. 321). Anonymous (2003) argues that computer viruses have no
destructive properties; however they often have malicious intent. This is supported by Serif and Gilliam (2003) who state that “a virus is a set of instructions, often malicious, that can spread from computer to computer by attaching itself to otherwise legitimate programs” (p. 1). The defining characteristic of a virus is therefore its ability to replicate, however, to do so it needs a host. Like a virus, the defining characteristic of a worm is its ability to replicate. However, worms differ from viruses in that they are able to do so by themselves, this defining characteristic of self replication distinguishes worms from viruses. Table 1 provides a summarised cross section of the defining characteristics of Trojan horses, viruses and worms.

<table>
<thead>
<tr>
<th>Table 1 Defining characteristics of malicious software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destructive</strong></td>
</tr>
<tr>
<td><strong>Malicious</strong></td>
</tr>
<tr>
<td><strong>Replicates</strong></td>
</tr>
<tr>
<td><strong>Self replicates</strong></td>
</tr>
</tbody>
</table>

Klander (1997) argues that Trojan horses are a sub type of computer viruses, however, given the Trojan horses inability (by definition) to replicate itself, this differs from the above definitions. It is not within the scope of this document to argue definitions; instead, a plausible single definition is used, that which is stated above.

### 3.2.7 Password Crackers

Password crackers are a tools employed by attackers which discovers passwords using a variety of attacks, including brute force or dictionary attacks (Irakleous, Furnell, Dowland, & Papadaki, 2002; Gollmann, 1999; Klander, 1997). Gollmann (1999) elucidates that in a dictionary attack the attacker matches all words in the dictionary to the user’s password. As the password is encrypted the attacker must first encrypt all words in the dictionary using the same type of encryption as the password. Once the words are encrypted they may be matched directly to the password, once a match is found the password is known. It should be noted that this technique does not require the password file to be decrypted, as each word, once encrypted is unique; the attacker need only match the encrypted states.
The second attack discussed in this section is the brute force attack. Brute force attacks attempt to discover the password by trying combinations of letters in sequential order. Klander (1997) states that "the brute force attack program will try passwords such as aa, ab, ac and so on until it has tried every legal character combination. The hacker will eventually get the password" (p. 430). An attacker using this technique will eventually discover the password, how long this takes depends on the length of the password. Adapted from Wakefield (2004), the following table represents the time necessary to crack a password.

Table 2 Time taken to discover a password

<table>
<thead>
<tr>
<th>NUMBER OF CHARACTERS</th>
<th>POSSIBLE COMBINATIONS</th>
<th>TIME NEEDED FOR A PERSON TO TRY ALL</th>
<th>TIME NEEDED FOR A COMPUTER TO TRY ALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>36</td>
<td>6 minutes</td>
<td>0.000036 seconds</td>
</tr>
<tr>
<td>2</td>
<td>1,300</td>
<td>4 hours</td>
<td>0.00130 seconds</td>
</tr>
<tr>
<td>3</td>
<td>47,000</td>
<td>6 days</td>
<td>0.04 seconds</td>
</tr>
<tr>
<td>4</td>
<td>1,700,000</td>
<td>6 months</td>
<td>2 seconds</td>
</tr>
<tr>
<td>5</td>
<td>60,000,000</td>
<td>20 years</td>
<td>60 seconds</td>
</tr>
<tr>
<td>10</td>
<td>3,700,000,000,000,000</td>
<td>&gt; 999 million years</td>
<td>118 years</td>
</tr>
</tbody>
</table>

- Characters include the letters A to Z and number 0 to 9
- Human discovery assumes one try every ten seconds
- Computer discovery assumes one million tries per second.

Table 2 shows that the longer a password is the harder it is to crack, if a long password is chosen and changed regularly then in the time it takes the attacker to discover the password it has been changed. While this section covers some main threats to computer security, the following section explores the mechanisms and processes that may be employed to mitigate or prevent such threats.
3.3 Computer Security

There is no definitive definition of computer security. Gollmann (1999) defines computer security as follows: “Computer security deals with the techniques used to maintain security within a computer system” (p. 3). Pfleeger and Pfleeger (2003) support this; they assert "the purpose of computer security is to devise ways to prevent the weaknesses [of computers] from being exploited" (p. 9). Technical and end-user based computer security measures are discussed. The first section presents technical countermeasures, including, firewalls, antivirus scanners, spyware scanners and passwords. Following this computer security policies outlining acceptable practice for computer users are presented.

3.3.1 Technical Countermeasures

The following is an account of some predominant technical countermeasures which may be employed by users to create a more secure system. These are: firewalls, antivirus software, anti-spyware and passwords. These countermeasures represent the most common and most appropriate tools for the purposes of this investigation, which is aimed at the computer user with a minimum amount of computer literacy.

3.3.1.1 Firewalls

Firewalls fall under several different headings; this section focuses on the general definition and workings of firewalls. Bishop (2003) defines a firewall as “a host that mediates access to a network, allowing and disallowing certain types of access on the basis of a configured security policy” (p. 780). A firewall controls access between two networks (Klander, 1997), some firewalls accept or reject information based on Internet protocol address and port and others assess the contents of the message and act accordingly. If the necessary properties of the package do not meet the security requirements of the firewall then it is not allowed past (blocked from the network), if the conditions are met, the package is allowed through. Peltier (2004) describes firewalls are the first line of defence in computer security (p. 177). A table provided by Szor (2005, p. 589) highlights a large number of infamous worms that can be denied access by the use of a firewall. This provides justification for the inclusion of firewalls as a technical countermeasure.
3.3.1.2 Antivirus and Antispyware Software

Anonymous (2003) describes antivirus software as the immune system of computer (p. 1). Anonymous (2003) states that “because no anti-viral package (or combination of packages) is a panacea for computer viruses, the key to escaping harm is prevention” (p. 1). The author continues to explain that in order to ensure prevention anti-virus software should be updated frequently, these updates provide protection from recently created viruses. According to Swartz (2003) there was a 519% increase in computer virus infected emails over a six month period in 2003 (p. 1). The threat posed by viruses, worms and Trojan horses can be mitigated or prevented by employing an up-to-date virus and antispyware scanner.

3.3.1.3 Passwords

Today, passwords are the most common form of user authentication to computer systems (Gollman, 1999; Landwehr, 2001; Irakleous, Furnell, Dowland, & Papadaki, 2002). Irakleous, Furnell, Dowland, & Papadaki (2002) explain that “despite their popularity, however, these methods are typically characterised as providing weak authentication, due mainly to vulnerabilities introduced by end users” (p. 1). Klein (1990) and Kessler (1996), cited in Irakleous, Furnell, Dowland, & Papadaki (2002) list these vulnerabilities as follows: badly selected (and therefore easily guessed or cracked), forgotten, written down, shared with colleagues, infrequently changed and kept the same across multiple systems” (p. 100). The following elaborates on these vulnerabilities.

Badly selected passwords which may be easily guessed or cracked (Section 3.2.7) are passwords that are either short (less than six characters) or are common English phrases. As previously discussed attackers may use password crackers to easily discover these passwords. In addition, if a password is a common English phrase it may be easily guessed, for example ‘cat’. As explained in section 3.2.7 the longer a password is, the harder it is to crack. However, by the same token, the longer a password the harder it is to remember. Wakefield (2004) elucidates that the fact passwords must be remembered and frequently changed means that quite often they are written down (p. 1). Sharing passwords with colleagues is a direct contradiction to the purpose of a password, which is to authenticate a person, proving they are who they say they are.
Wakefield (2004) provides a list explaining the properties of strong passwords, she states that “strong passwords integrate all of the following features:

- At least eight characters in length
- A combination of letters of mixed case, and numbers
- Easily typed
- Something known only to the user (i.e., not present in any database)
- Not found in an English or foreign language dictionary
- Never shared
- Never written down” (p. 1).

Wakefield’s (2003) list provides guidelines to ensure passwords are as secure as possible. However, Gollmann (1999) explains that passwords do not provide definitive authentication for a person, authentication (using passwords) only implies that the user knows the password (p. 28). Gollmann (1999) states, “there is no way of telling the difference between the legitimate user and as intruder who has obtained that user’s password” (p. 28). This point, combined with the fact that passwords are currently the most common form of authentication (Irakleous, Furnell, Dowland, & Papadaki, 2002, p. 101), means that all measures should be taken to ensure passwords are as strong as possible.

The above presents the relevant technical countermeasures that should be employed to achieve effective computer security. However, of upmost importance is the manner in which user behave and make use of these tools.

### 3.3.2 Acceptable Practice

Acceptable practice refers to the computer security practices that are acceptable for users in a particular context, for example, at work or at home. Cyber-Ark (2005), cited in the Computer Crime Research Center (2005), states that in a successful information security program, all three pillars—people, process, and technology must be strong. The previous section deals with technology, this section covers the people and process pillars. Anonymous (2003) defines acceptable use as “…a general set of guidelines for administrators and users that emphasizes best practices and security awareness in daily work” (p. 637). This section will outline what should be practiced by users in order to take maximum advantage of the technical mechanisms described above and to
successfully mitigate the threats that are not controllable by the technical countermeasures. It is important in this section to establish a clear line on what users should be taught and what can be expected of them. AusCERT (2004) explains “Users of Internet banking and ecommerce services should ensure that the machine, through which they access the web, can be trusted and is well secured” (p. 25). In addition to employing each of the technical countermeasures discussed above, users should consider the following.

As described in section 3.2.2.3 social engineering attacks are aimed at users who are not aware of such scams, these emails trick people into revealing personal information because they think it is the right thing to do. Spencer (2005) states “Internet users should ignore emails asking for personal or financial information and take note of pop-up warnings”. Users should be aware that banks and other financial institutions will not request login information via email or phone call.

Erbschloe (2005) describes in detail what users should and shouldn’t do in relation to being responsible for computer security. This list (adapted from Erbschloe, 2005), defines important aspects in acceptable practice for end-users:

Things not to do:

- Disable or interfere with antivirus software on your computer,
- Open emails from unknown sources,
- Open email attachments unless you know whom they are from,
- Share access to your computer with strangers,
- Let web sites you visit install software on your computer.

Things to do:

- Use hard to guess password,
- Change passwords often, and,
- Be cautious when downloading files from the Internet (p. 149).

Hanna (2005) emphasises that users should adopt secure passwords, he maintains that “bad and poorly guarded passwords are the bane of most systems” (p. 1). In addition to not letting web sites install software on the computer, users should also be aware of the
Employees should be well versed in the risks of spyware and downloading unauthorised applications from the Internet and opening attachments; and they should be on guard for social-engineering techniques designed to pilfer usernames and passwords from unsuspecting users (p. 1).

This demonstrates that users should be aware of the risks involved in downloading unauthorised applications and email attachments. They should also look for social engineering techniques. In order to identify for something its features must first be known, thus highlighting once more, the need for end-user education.

Acceptable practice and what a user should and shouldn’t do are of core importance to this investigation. The above establishes what countermeasures end-users should use and how they should behave. To sufficiently convey this information to the end-user, effective teaching techniques must be employed. The following section discusses learning theories and teaching theories, identifying how adults learn and how they should be taught.
3.4 Education

This investigation aims to provide educational material to adults on topics concerning computer security. Therefore, the educational value of the package is critical to the substance of the investigation.

3.4.1 Constructivism and Behaviour Modelling

Today, the learning theories that hold the most sway are those based on constructivist principals (Oliver & Herrington, 2003, p. 12). Lebow (1993) and Jonassen and Reeves (1996), cited in Oliver and Herrington (2003), state, in relation to constructivist learning, “learning is based as the construction of meaning rather than as the memorisation of facts” (p. 12). Cunningham, Duffy and Knuth (1993), cited in Oliver and Herrington (2003) present seven pedagogical goals that characterise a constructivist learning environment, they suggest that constructivist learning settings are those which concurrently:

- provide experience in the knowledge construction process;
- provide experience in and appreciation for, multiple perspectives;
- embed learning in realistic and relevant contexts;
- encourage ownership and voice in the learning process;
- embed learning in social experience;
- encourage the use of multiple modes of representation; and
- encourage self-awareness in the knowledge construction process. (p. 12)

This indicates that a successful constructivist learning environment is one that establishes a need or desire within the learner to seek knowledge on the topic. Once this has been achieved the teacher simply facilitates the acquisition of knowledge, providing the learner with the necessary skills to acquire it. Simon (2000) conducted a study involving four hundred and fifty members of the U.S Navy and three training methods: instruction, exploration and behaviour modelling. The study aimed to assess “the relationship of learning style and training method to End-User computer satisfaction and computer use” (p.1). The study found that “behaviour modelling trainees were not influenced by learning style and these trainees had the highest level of satisfaction and computer use” (p.1).

In addition to behaviourism and constructivism, Malcolm Knowles' theory of adult learning provides a framework for the content and development of the package (Knowles, 1984).
3.4.2 Adult education

Knowles’ Theory of Andragogy (as opposed to the Theory of Pedagogy) explains the mechanisms and motives in adult learning. Knowles (1984) presents a section concerning how adults learn in computing; this is especially relevant in the context of the investigation and is expanded upon. Knowles (1984, p. 174) identifies four key points in relation to adult learning and the computer industry. These are summarised as follows:

1. “Adults have a deep need to know why they need to know something before they invest time and energy in learning it.”
2. “Adults are task oriented in their learning. We learn those things best which we learn in the context of using them to do what we want to do.”
3. “Give us choices that will enable us to tie into the use of the computer from different experiential basis.”
4. “Adults have a deep psychological need to be self directing…”

The first point indicates that the effectiveness of any educational content is directly related to whether or not the individual has a pre-existing desire to learn the content. This point indicates that forcing an adult to engage in an education situation and assessing their conformity to the information provided will yield poor results. Lindeman (cited in Knowles, 1984) supports this conclusion, he states “Facts and information from the different spheres are used, not for the purpose of accumulation but because of a need in solving problems...Adults are motivated to learn as they experience needs and interests that learning will satisfy...” (p. 30). Combined with the discussion on constructivist leaning in section 3.4.1, this translates into the fact that the package will have a greater effect on individuals with an existing desire to learn about computer security. The need for computer security must, therefore, be established early in the package.

The second point presented by Knowles (1984) suggests adults learn best when the information presented, is done so in the context of where it would normally be used. For example, teaching an adult how to browse the Internet is best done from in front a computer with an Internet browser running. This allows the individual to place in context immediately the information presented. Lindeman, cited in Knowles (1984),
maintains "adults' orientation to learning is life-centred; therefore, the appropriate units for organising adults learning are life situations, not subjects" (p. 31). Adults learn best in real life situations and situations that directly affect the life of the individual. Placed in the context of this investigation, this means the individual should be actively using computers and the Internet.

The third point states that adults should be presented with the ability to relate what they are learning to other experiences. Lindeman, cited in Knowles (1984), illustrates that "experience is the richest resource for adults' learning; therefore, the core methodology of adults' education is the analysis of experience" (p. 31). Analogies allow people to relate topics and information to real life experiences. Giving people the ability to relate new information to what they already understand makes it easier for them assimilate it, thus, increasing the effectiveness of the learning process.

Finally, Knowles (1984) states that adults need to be self directing in life. Knowles (1984) explains that, as adults "we resent being talked down to, having decisions imposed on us, controlled, directed, and otherwise treated like children" (p. 175). Expanding on this point, Knowles (1990) states "therefore, the role of a teacher is to engage in a process of mutual enquiry with them rather than to transmit his or her knowledge to them and evaluate their conformity to it" (p. 31). The fact that adults like to be self directing must be taken into careful consideration in reference to teaching and developing an effective learning package. The structure of the session should be flexible, allowing the learner to control, to some extent, its direction. Lindeman (cited in Knowles, 1984, p. 31) explains how differences between people increase with age, therefore, to successfully teach adults style, time, place and pace of learning should be taken into careful consideration.

3.5 Significance
This literature review establishes users as the weak link in computer security. In addition it presents a justifiable need for an educational package designed to inform users of the risks of unsafe computing and ways in which computing can be made safer. Discussed in section 3.4 were the education theories of constructivism, behaviour modelling and Andragogy. Providing a basis for the structure and content of the educational package, these theories are employed to ensure the package is as effective as possible.
4.0 METHODOLOGY

Punch (1998) and Leedy and Ormrod (2005) present research methodologies under two headings, quantitative and qualitative. The differences between quantitative and qualitative data and their applicability to this investigation are explored. Following an outline of considered approaches, the section concludes with a detailed description of the explanatory approach to mixed methods research as defined by Cresswell (2005), and why it was selected for this investigation.

4.1 Comparing Quantitative and Qualitative Data

Thomas (2003) distinguishes between quantitative and qualitative research, he states:

"...qualitative methods involve a researcher describing kinds of characteristics of people and events without comparing events in terms of measurements or amounts. Quantitative methods, on the other hand, focus attention on measurements and amounts (more and less, larger and smaller, often and seldom, similar and different) of the characteristics displayed by the people and events that the researcher studies" (p. 1).

Leedy and Ormrod (2005) expand on this explanation in presenting the following general uses for each approach: “Quantitative research is used to answer questions about relationships among measured variables with the purpose of explaining, explaining, predicting, and controlling the phenomena (p. 94). The authors explain that quantitative research is also known as traditional, experimental, positivist approaches (p. 94). They continue to explain that, “in contrast, qualitative research is typically used to answer questions about the complex nature of phenomena, often with the purpose of describing and understanding the phenomena from the participants’ point of view” (Leedy and Ormrod, 2005, p. 94). This approach is also referred to as interpretive, constructivist, or postpositivist approaches (Leedy and Ormrod, 2005, p. 94).

Quantitative research deals with measurable factors which can be interpreted into numbers and statistics. The purpose of quantitative research is to explain and predict, confirm and validate, and test theory (Leedy and Ormrod, 2005, p. 94). This approach deals with numeric data, collected in large samples that are quantified in some way. Punch (1998) supports this in stating, “quantitative research involves measurements, usually or a number of variables, and usually across a sample” (p. 113). To determine the meaning of the data statistical analysis and deductive reasoning are applied with a stress on objectivity. An example of a quantitative study may be determining the
percentage of people who smoke and who also have cancer, this would involve a large population, and purely statistical data. In this investigation quantitative data are used to represent population demographics, perceived awareness and participant behaviour.

Leedy and Ormrod (2005, p. 133) explain that qualitative research deals with factors such as people’s views or opinions and that the approach is used to gain a better understanding of complex situations. Punch (1998) supports this, he states, “qualitative research concentrates on the study of social life in natural settings” (p. 199). Qualitative studies aim to describe and explain, explore and interpret, and build theories that may be used as grounding for future studies. Leedy and Ormrod (2005) emphasise that it is important to recognise that the analysis is potentially biased and subjective (p. 96). Data from qualitative studies are communicated by words, narratives and person voice. In the context of this investigation, determining traits in qualitative data provides the opportunity to gain an insight into the reasons why people may not engage in safe computing, their opinions of the package and their willingness to change behaviour.

From this examination it is concluded that this investigation could benefit from both quantitative and qualitative data. Quantitative data will be used to determine population demographics, user awareness and if behaviour change occurs. Qualitative data will provide insight into the motives behind quantitative results.

4.2 Outline of Available Research Designs
This section provides a discussion on the mixed methods research designs considered for this investigation. Their suitability and the reasons for their exclusion or inclusion are provided. Creswell (2005) asserts, “you use mixed methods when you want to incorporate a qualitative component into an otherwise quantitative study” (p. 510). As presented in section 4.1 the investigation houses aspects that provide justifiable use for both quantitative and qualitative data. Thomas (2003) avows “the best answer frequently results from using a combination of qualitative and quantitative methods” (p. 7). Creswell (2003, 2005) advocates three approaches to mixed methods research, these are: triangulation, exploratory and explanatory. The following section describes each design regarding their advantages and disadvantages and their applicability to the investigation.
4.2.1 Triangulation Design

Triangulation in mixed methods research, as defined by Creswell (2005), “consists of simultaneously collecting both quantitative and qualitative data, merging the data, and using the results to best understand a research problem” (p. 600). Consider the following diagram:

![Diagram](image)

Figure 1 Triangulation mixed methods design (adapted from Creswell. 2005. n. 514)

As Figure 1 demonstrates, equal priority is given to both types of data, and the data is collected simultaneously. After data has been collected, “the mixed methods researcher compares the results from quantitative and qualitative analyses to determine if the two databases yield similar or dissimilar results” (Creswell, 2005, p. 514). Creswell (2005) explains the strength of this design is that it combines the advantages of both quantitative and qualitative data (p. 515). The author maintains quantitative data provides generalisability and qualitative data provides information on setting and context (p. 515). Creswell (2003) highlights that collecting data concurrently means a shorter collection time, however, he also presents a number of weaknesses (p. 217). Creswell (2003, 2005) explicates that comparing data of two different forms can be a difficult task; resolving discrepancies can also be difficult and may involve further data collection (p. 217, 515). Strauss and Corbin, cited in Thomas (2003), argue that both qualitative and quantitative methods can be used effectively in the same investigation. However, most projects and researchers place their emphasis on one form over the other. This is partly out of conviction, but also because of training and the nature of the problem studied (p. 7). This investigation aims to assess behaviour and knowledge change with quantitative data, using qualitative data to show possible reasons behind the quantitative results. It is therefore postulated that more priority should be place on quantitative data.
4.2.2 Exploratory Design

Exploratory mixed methods research aims to explore a phenomenon using qualitative data, then, using quantitative data, explain the relationships found in the qualitative data (Creswell, 2005, p. 516). The following diagram presents an overview of the structure of exploratory mixed methods research.

![Exploratory mixed methods design diagram](attachment:image.png)

Figure 2 Exploratory mixed methods design (adapted from Creswell, 2005, p. 514)

As Figure 2 outlines that emphasis is given to qualitative data, which is collected before quantitative data in a sequential fashion. Creswell (2005) describes the purpose of the quantitative data to build upon, or explain the initial qualitative findings (p. 516). The above design represents a possible framework for this investigation. However, it was concluded that, due to the nature of the study, emphasis should be given to participants’ behaviour, and responses from participants can be used to explain results. Therefore, emphasis should be placed on quantitative (behavioural) data, which is collected initially, followed by qualitative (responses) data to explain the initial results. Section 4.2.3 explains the explanatory approach to mixed method research (as defined by Creswell, 2005) which aligns to the above requirements.
4.2.3 Adopted Approach - Explanatory Design

Research was conducted using an explanatory approach to mixed methods research as defined by Creswell (2005). Consider the Figure 3 as an overview of the explanatory approach to mixed methods research.

As Figure 3 shows, results from the qualitative data will be used to strengthen the initial quantitative data. Figure 3 also demonstrates that more emphasis will be placed on quantitative data. As Creswell (2005) asserts, “the purpose of the sequential explanatory design typically is to use qualitative results to assist in explaining and interpreting the findings of a primarily quantitative study” (p. 215). Morse (1991) cited in Creswell (2005) states that “it can be especially useful when unexpected results rise from a quantitative study” (p. 215). If unexpected results arise, the qualitative data gathered will be used to give insight into why the unexpected results have arisen. In the explanatory approach more emphasis is given to quantitative data, and, as the name suggests, the qualitative data may be used to explain the quantitative data, thus giving more detail to the investigation. Qualitative data are examined for common traits, once identified these traits will be recorded along with their frequency.

At the centre of this investigation is people’s behaviour; therefore, more emphasis must be placed on quantitative data. One aim of this is investigation is to provide grounding for future study into the education of end users (see section 8.0). Creswell (2005) asserts that mixed method research may be conducted when building from one phase of research to the other. Given the multiple phase topology of the investigation this represents clear justification of adopting the explanatory approach choice.
4.3 Research Data

This design was selected as it provides the opportunity to use both quantitative and qualitative data; accordingly, this investigation collects both types. The participants’ behaviour, awareness and demographical information are represented as quantitative data. This may be used to explore relationships such as perceived computer security awareness before and after the presentation (data that are easily quantifiable). Qualitative data will provide insight into quantitative results, where applicable. In addition, qualitative data will be used to represent the perceived effectiveness of the package by supplying data such as what parts the participants liked and what parts they felt could have been improved. Priority is placed on quantitative data in alignment with the explanatory approach to mixed methods research, as defined by Creswell (2005). This means that more emphasis will be placed on quantitative results in the analysis and investigation conclusions. Data concerning participant’s demographics and behaviour will be collected using quantitatively based questionnaires prior to obtaining their qualitative responses from open ended questions in a final questionnaire.

<table>
<thead>
<tr>
<th>QUANTITATIVE DATA</th>
<th>QUALITATIVE DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method of data collection</td>
<td>Data type</td>
</tr>
<tr>
<td>Questionnaires; Closed-ended questions</td>
<td>Numeric scores</td>
</tr>
</tbody>
</table>

Table 3 shows quantitative and qualitative methods of data collection and types of data that are collected in this investigation. As defined by Creswell (2005), quantitative data will be analysed and the results will be explained in more depth in the qualitative phase of the investigation (p. 521). The research data is presented and results are analysed in the following sections: user awareness and user behaviour. Quantitative data will be analysed under these sections establishing a discussion. Qualitative data will be analysed, and traits will be identified in each question. These traits will be presented under each relevant question in the results section. The traits identified in each question will be employed to explain possible reasons or motives for the results shown in the quantitative data.
5.0 DESIGN AND IMPLEMENTATION

The design and implementation of this investigation is described under six sequential headings: the educational package, gathering the participant population, the pre-package questionnaire, delivery of the package, the initial post package questionnaire, the two week post-presentation questionnaire and the final qualitative questionnaire. Aligning with the project methodology, data for the investigation is gathered using four questionnaires: three with a quantitative focus and the final questionnaire that addresses qualitative issues.

5.1 Developing the Educational Package

This section describes the processes taken in developing the package, the justification for its structure and reasons for inclusion/exclusion of information. The educational package was structured as a Microsoft PowerPoint presentation; however, it also includes interactive features. A primary concern in developing and delivering the presentation was that participants viewed it more as a discussion; therefore it is referred to as an educational package.

As discussed in the literature review, cracking, identity theft, fraud, social engineering, denial of service attacks, malicious software and password crackers are responsible for countless computer crimes, stolen identities and the loss of billions of dollars. These topics represent the main threats that may be mitigated by educating users, that is, they are events that the computer user has some control over. The discussion of such threats is irrelevant if users are not presented with the knowledge required to mitigate or prevent them. The presentation is structured using analogies wherever deemed necessary. As discussed in section 3.4.2 of the literature review, analogies help people tie unfamiliar concepts into a familiar context, thus making it easier to understand. The following headings represent sections in the presentation (see Appendix A); under each heading is a description of what it contains and how it was explained to the participants. For the purposes of readability sections within the presentation are referred to as ‘parts’.

5.1.1 Package Introduction and Background

The final product (see appendix A), is organised into a logical progression of topics, explaining each relevant threat followed by how to prevent or mitigate it. Initially the background of the educational package is discussed (parts 1 and 2 of the presentation). Numerous threats to computer security mean that any sensitive information stored on an
unsafe computer which is connected to the Internet is accessible to attackers. This section in the presentation provides the participant(s) with justification for learning the content of the package. As discussed in section 3.4 of the literature review adults have a need to know, why they need to know something before they invest time and energy in learning it. This initial justification for learning aligns with this and it is proposed that starting the presentation with this background creates desire to learn about computer security. This initial section is designed also, to explain to the participants the difference between the package and other sources of information. "This presentation is different because it will empower you with knowledge of computer security issues"; rather than simply stating what should and shouldn’t be done, participants are shown why this is so.

5.1.2 Cracking, Internet Protocol Addresses and Ports

Part 3 of the presentation explains Internet Protocol addresses, ports and cracking. Participants are educated on the fact that attackers use IP addresses and ports to gain access to computers. This is explained as follows:

If an attacker wanted to break into your house he or she would first have to know the address of your house, the attacker would then look for open windows or doors. The same may be applied to computers, if an attacker wants to break into a computer their must first discover they IP address of the computer, they would then look for open ports to gain entry through. This means that your IP address can be thought of as the address of your house and ports can be thought of as doors and windows; open ports are like open windows and doors, closed ports are like locked windows and doors.

5.1.3 Firewalls

As discussed in the literature review (Section 3.3.1.1), firewalls mediate and control access between computer systems. Part 4 of the presentation, as a follow up to the previous section describes firewalls. What firewalls are, how they work and how to use them effectively is presented to participants. Slide number six (Section 4.1) provides a simple diagram demonstrating that a firewall is situated between the computer and the Internet. Presented in slides eight, nine and ten is an explanation of the workings of a firewall and a screen shot of Kerio Personal Firewall 4\(^2\) running. The connections and symbols shown in the screenshot are described to the participant(s). Firewalls are described using the previous analogy of a person’s house: Running a firewall is like having a bouncer at the doors and windows of your house, when an unknown person
requests entry to the house the bouncer checks what they look like and their intentions. In addition, when person leaves the house the bouncer makes sure they have not taken anything with them. The same applies for a firewall, information entering and leaving the computer system is checked against a specific set of rules; if all requirements are met, the information is allowed through.

5.1.4 Malicious Software

As developed in the literature review, (Section 3.2.2.5), the presentation divides malicious software into three sub categories: viruses, worms and Trojan horses. Part 5 of the presentation explains the difference between the three types of malicious software to the participant, highlighting the defining characteristics of each. Viruses, in accordance with the biological definition, need a host in order to survive. They attach to other programs without knowledge or consent and are commonly downloaded from email attachments or applications on the Internet. The defining characteristic of viruses is replication, although, they need a host to do so. Worms, like viruses, have the defining characteristic of replication, the difference however, is that worms are self propagating. This means that they are able to travel across networks, including the Internet, by themselves. They are responsible for using bandwidth and denying services to users. The term Trojan horse refers to a program inserted into your computer without you knowing it. Once inside the Trojan horse performs some undesired function such as logging key strokes. Following the explanation of a Trojan horse an interactive Trojan horse demonstration is conducted. Desktop Scout 4.02 and two laptops are utilised to perform the functionality of a Trojan horse. One laptop is infected with the Trojan horse (the victim’s computer) and one with the Trojan horse control software (the attacker’s computer). The participant is given the opportunity to perform functions such as remote desktop control, directory browsing and file transfer. As part of the interactive session one participant creates a text file on the infected computer with a secret message in it. Another participant is shown, from the attacker’s computer, how to transfer the secret file from the victim’s computer and read the message. This interactive demonstration concludes the malicious software section of the package; the following section provides participants with the necessary knowledge to mitigate or prevent the threat of malicious software.

5.1.5 Antivirus Software and Spyware Scanners

2 Kerio Personal Firewall 4.0 – Available www.kerio.com
3 Desktop Scout 4.0 – Available www.globalpatrol.net
In order to keep a computer clean of the malicious software described above antivirus and spyware scanners should be employed. Part 6 of the presentation provides a brief overview of some available antivirus software and spyware scanners; it also explains that scans should be completed once per week at least. As discussed in the literature review (Section 3.3.1.2) keeping antivirus software and spyware scanners up-to-date is of upmost importance, these tools can only stop malicious software they know about; new viruses, worms and Trojan horses are being created every day.

5.1.6 Passwords and Password Crackers
The literature review (Section 3.3.1.3) establishes that passwords are the main form of authentication used today. It is assumed that every participant has at least one password they use frequently. Part 7 of the presentation explains that passwords should not be written down or told to other people, in addition to this, strong passwords should be chosen. The characteristics of a strong password is that it is eight characters or more in length, contains alpha-numeric (numbers and letters) characters and has no distinct meaning in the English language. This part of the presentation presents examples of strong and weak passwords and highlights that there is an obvious trade off between how easy the password is to remember and how strong it is. The justification for having a strong password is now explained to participants. Password crackers (Part 8.0) are tools used by attackers to discover passwords; they use two main techniques, brute force attacks and word lists. Brute force attacks try all combinations of letters and numbers in order until the password is discovered, the longer the password the time it takes to discover increases exponentially (see Table 2). Word lists match phrases and words to the password until it is discovered, if a password has no logical meaning, or contains numbers then this attack will not work.

5.1.7 Social Engineering and Miscellaneous Knowledge
The design and implementation of Parts 8 through to 11 is explained in this section. If users do not log off computers when they are not using them in a situation where others have physical access to the computer then all possible countermeasures are made redundant. If a computer is left unattended and logged on, anyone, within reason, may use that computer for whatever purposes. Information may be stolen or data may be deleted or modified. All events will be logged under the name of the person who was logged in and left the computer unattended. The presentation also explains that it is
important to disconnect from the Internet when not using it. If the computer is not connected to any network then it is safe from electronic threats such as cracking or malicious software. Social engineering, as described in the literature review (Section 3.2.2.3), aims to trick users into disclosing information, most commonly account details. Two of the most common forms of social engineering are fake emails and phone calls. This section explains that banks and other institutions will not send emails requesting account details, such emails are fraudulent. The term for this attack is Phising. Users, in this section, are also instructed to frequently clear cookies and offline content and shown how to do so.

This concludes the discourse related to the presentation. In what follows, section 5.2 discusses the procedure of gathering a sample population. Following this, the design and implementation of initial questionnaire is presented. Sections 5.5, 5.6 and 5.7 provide the design and implantation of the three post-package questionnaires.

5.2 Gathering Participants
Participants were gathered from a variety of different backgrounds, representing a broad range of estimated computer literacy. A total of twenty participants took part in the investigation, subjects were selected based on their age, estimated computer literacy and use of computers. By selecting participants with varying demographics a clearer indication is given, of what effect, in terms of knowledge, awareness and behaviour, the package has on users.

5.3 Pre-Package Questionnaire
The pre-package questionnaire is designed to collect initial quantitative information describing the sample population's demographics, current computer security awareness and current behaviour (see appendix B). The questionnaire begins with a generic letter describing the purpose of the investigation, the participant's role and how data will be handled. The cover letter informs the participant that all data is de-identified and destroyed upon completion of the thesis. Any reference to individuals is through an alpha numeric code. Page two contains a table outlining a list of available times for presenting the package on various days from the 3rd of October to the 9th; in addition a section is allocated for other times. This timetable allows participants to select a number of times that best suit them, from these possible times participants can be grouped into sessions with others of similar computer literacy (this is estimated from the participant's
reported computer security awareness). The purpose of this is to make participants feel as comfortable as possible. Also any questions asked may be applicable to others in the group. Following the timetable participants are required to fill out contact details: name, contact number, email.

Demographic information was then collected: age and estimated computer use (hours per week). Following the demographical sections, sections outlining behavioural data are presented: What the computer is used for, the number of hours per day the computer is connected to the Internet, what activities are performed on the Internet, what computer security countermeasures are running and up-to-date, and the participant’s estimated understanding of computer security issues.

The information collected from this questionnaire is quantitative, thus, aligning with mixed methods explanatory research. The demographical and behavioural data provides a foundation to cross-reference with further quantitative and qualitative data.

5.4 Presenting the Package
This section explains the manner in which the package was presented to participants. The package was presented to small groups of between two and five participants, structuring the presentation this way gives participants increased opportunity to ask questions and discuss topics. As discussed in Section 3.4 of the literature review adults “have a deep psychological need to be self directing” (Knowles, 1990, p. 31). Knowles (1990) continues to explain that this means the role of the teacher is to engage in a process of mutual enquiry with the learner, rather than convey his/her knowledge with them and assess their conformity to it (p. 31). While bearing this in mind a line must be drawn between allowing the participant to be self directing and presenting the knowledge that is most important in a succinct and logical fashion. The sessions were structured to be interactive, allowing participants to ask as many questions as possible. At the commencement of the presentation all participants were informed that they should view the presentation as an open discussion, and that the structure of the presentation is simply to aid their questions and present information in a logical order. The advantage of this design is that participants feel free to ask questions and discuss topics, if a question is raised that is covered in a later section then it can be covered later, or if deemed important to the current context, discussed at present.
Prior to the commencement of the package users were informed of the following. The package is aimed at people with a minimum level of computer literacy; this means they are not expected to know any of the content of the package. Participants are not expected to understand everything the first time. Participants should feel free to ask questions at any stage in the presentation. Participants should view the package as a discussion between two adults, rather than a presentation.

After each topic was covered questions relating to the content were asked, this allowed continuous assessment of the participants progress. It is proposed that this achieves two goals. Firstly, this will give them a better understanding of the topic by putting it into their own words, and secondly, it will ensure the presentation is not moving at a pace too fast for the participant.

5.5 Initial Post-Presentation Questionnaire
Following the presentation of the package, participants filled out an initial questionnaire (see Appendix C). This questionnaire collects quantitative data on two variables. The first is the participant’s perceived change in their computer security awareness. The second covers the participant’s willingness to adopt a safer approach to computing. Individuals are asked to list their estimated level of computer security awareness before and after the presentation, this serves two purposes. Firstly this feedback was used to assess whether or not the individual now views themselves as more aware of computer security issues. Secondly their estimated level of computer security before the package can be compared to that which they stated before viewing the package.

5.6 Quantitative Two Week Post-Presentation Questionnaire
This post-presentation questionnaire (see Appendix D) was given to the participants two weeks after they received the package, it has two main purposes. Collecting quantitative data, the questionnaire aims to assess how much knowledge the participants retained. Further questions involve whether or not the inclined behaviour change stated in the initial post-presentation questionnaire actually materialised. The questionnaire is split into two sections, the first section contains multiple choice questions designed to assess how much of the package content the participants remembered. The second section assesses change in the use of computer security countermeasures. This is the most important questionnaire as the quantitative data collected is used to determine whether or not behaviour change actually occurred within the population.
5.7 Qualitative Post-Presentation Questionnaire

The questionnaire represents the qualitative phase of data collection. The questionnaire is designed to gather data that provides an insight into the quantitative data previously gathered. As described in the investigation methodology (Section 4.0) the purpose of qualitative data is to explain and explore possible explanations for the quantitative results. The questionnaire contains the following open-ended questions:

1. Explain your view of computer security before the package and, if you listed your estimated computer security awareness as below 5 before the package please describe:
   a) Whether or not you sought information on computer security to become more aware
   b) If you didn’t please explain you reasons for not doing so.
   c) If you did please describe how easy it was to find and understand.

2. Explain, in your own words, your view of the package.

3. Explain if, and how the package changed your view of computer security.

4. How do you think this presentation could have been improved?

The aim of the first question is to gain an insight into what the participant’s views were regarding the availability of existing computer security packages, and how easy they are to understand.

The second question is structured to gain a qualitative insight in the effectiveness of the package as viewed by the participant. The qualitative data gathered from this question is aimed at providing an indication of participants’ views of the package. It is postulated that responses to this question will provide insight into the package’s effectiveness and applicability to computer security.

Question 3 aims to collect qualitative data based on how the package changed the participant’s view of computer security. Should quantitative data collected in the previous questionnaires show change in participant’s behaviour, this data will attempt to provide exact motives for the change.
The final question provides feedback by participants into if and how the questionnaire may be improved. Not only does this provide an insight into the weaknesses of the package, it is especially helpful in restructuring the package for any future investigations.

The final questionnaire represents the qualitative data collection phase of the investigation, thus aligning to the explanatory approach to mixed method research. The results are now presented in Section 6.
6.0 RESULTS

This section structures and presents the data gathered from the investigation as results under the headings of quantitative and qualitative. Creswell (2005) defines mixed methods research as “a procedure for collecting, analysing, and mixing both quantitative and qualitative data in a single study to understand a research problem” (p. 510). As discussed in the methodology section more emphasis is placed on quantitative data which is presented first. It is the purpose of this section to present the results gathered in uninterrupted form, results are interpreted, analysed and discussed in the following section.

6.1 Quantitative Results

The following is a summary of the quantitative results gathered in the investigation. The section commences with a broad indication of population demographics before progressing into user awareness and behaviour change.

The demographics of participants (see Appendix F) are varied. Most respondents are aged either between twenty and twenty five years or thirty five and fifty years old, these age brackets make up twelve out of twenty participants. Another five participants were below the age of nineteen. Sample population computer use covers all hourly brackets evenly, apart from zero to two hours which was not recorded by participants. In terms of participants’ willingness to adopt a safer approach to computing, a dramatic response was record. As shown in Figure 12 (see Appendix H) twenty participants in all areas but two, indicated that they were more willing to change their behaviour after viewing the presentation. In the behavioural traits ‘using a more secure password’ and ‘using up-to-date antivirus software’, all but four participants indicated they were willing to change their behaviour.

Also shown in the quantitative results was that all participants used computers at home and all had an Internet connection. Twelve out of twenty participants used Internet banking and eight purchased products online. The most common Internet connection time was zero to five hours per day. All participants recorded 100% in the knowledge retention test.
6.1.1 Change in Estimated Awareness

Figure 4 represents the participants' estimated computer security awareness on a scale of one to ten, where one is basic and ten is excellent. The initial line represents the participants' estimated computer security awareness prior to viewing the package. The second line represents their view on the same variable, after viewing the package. The third line shows the participants' estimated computer security awareness after viewing the package.

Seventeen out of twenty participants reported an increase in awareness. On average, participants' perceived computer security awareness increased by 3.65 points. The maximum was an increase of nine, reported in one case. The minimum was no increase at all reported in three cases. Participants with estimated computer security awareness' of eight and above before viewing the package did not register a change in awareness. In five cases the participants pre-package awareness decreased by one after viewing the package, in one case it decreased by two, respondent fourteen indicated a decrease of four.
6.1.2 Change in Behaviour

Figure 5 is a representation of the behaviour change that occurred in participants after viewing the package. The initial, lighter bar represents the number of participants that responded ‘True’ to engaging in unsafe computing prior to the package. The second, darker bar shows the number of participants, in total, that changed their behaviour in this area after viewing the package. For example, the first sector refers to the use of weak passwords. Fourteen participants responded ‘True’ initially, meaning they used an insecure password prior to the package. After viewing the package nine participants were recorded as making their password more secure.

Graph showing behaviour change in participants

1. Prior to viewing the package I was using an insecure password.
2. Prior to viewing the package I was opening emails from suspicious senders and unknown senders.
3. Prior to viewing the package I logged others onto my account.
4. Prior to viewing the package I did not disconnect or turn my computer off when not using the internet.
5. Prior to viewing the package I visited erroneous websites.

The above graph shows that a behaviour change was recorded in all sectors. The largest change in terms of total respondents was recorded in sector four, disconnecting or turning off the computer when not using the Internet. From an initial eighteen respondents answering ‘True’ to not turning off or disconnecting the computer when not using the Internet, nine claimed to have changed their behaviour. The largest change in
terms of percentage was witnessed in sector five, where nine out of eleven respondents stopped visiting erroneous web sites. Sectors two and three, opening emails from suspicious and unknown senders and logging others onto their account, reported the least change, with two participants in each sector changing their behaviour.

Figure 6 represents the change registered in participants’ use of technical computer security countermeasures after viewing the package. The initial bar indicates a positive response (Yes) by participants when asked if they were making use of the technical countermeasure in question prior to viewing the package. The second bar indicates the number of participants who gave positive responses to the same question after viewing the package.

![Graph showing the change in use of technical countermeasures](image)

As demonstrated in Figure 6, the use of Firewalls increased by three participants after viewing the package. The use of antivirus software by participants increased by two participants, raising it to nineteen and antisyware use increased by four participants, raising it from eleven, to fifteen people out of a possible twenty.
7.2 Qualitative Results
The following traits were identified in the qualitative data gathered from the final questionnaire (see Appendix E). The traits are described in relation to the question they were identified in.

6.2.1 Question 1
The most common trait discovered in the responses to Question 1 was the admission of laziness by respondents; this trait was recorded in seven responses to this question. The second most common trait identified was the respondent indicating that they did not know where to look for the information coupled with the fear of not being able to understand it; reported in five responses. A third equally common trait was that of the participant having another family member who was deemed responsible for keeping the computer secure. Thus, the respondent indicated there was no need to learn about computer security; this was identified in five responses. A fourth, less frequent trait, was identified four times, the respondent did not realise how little they knew, and how important computer security is.

6.2.2 Question 2
The most common traits discovered in reply to Question 2 are as follows: The package was very informative, the information was presented at a basic level which was very easy to understand and the use of analogies made topics a lot easier to understand. These traits were all recorded in fourteen responses. Recorded in ten responses to this question was a trait highlighting that the package made the respondent realise how little they actually knew about computer security. The third most common trait, identified in six respondents, was that the explanation of the differences between viruses, Trojan horses and worms was very interesting. Equalling this trait, with six responses, was that respondents found the information on how passwords are cracked and why it is important to use a strong password very interesting. Identified in five responses to the question was a trait identifying that the presenter was very well informed and very willing to answer questions.

6.2.3 Question 3
Identified in sixteen responses to this question, was a trait identifying that participants were not aware how important computer security was, and the effect it had on their place of work. Nine responses indicated that the participant was not aware how
important it is to use a secure password. Nine respondents also indicated that they would be more aware when browsing the Internet and opening emails.

6.2.4 Question 4

The most common response to this question was "nothing", recorded in thirteen responses. The second most common response to this question was the inclusion of more interactive sections and more analogies, recorded in ten responses. The third most common response was that more diagrams should be included; this was recorded in seven responses. Recorded in four responses to this question was that the writing should be bigger and a hand out should have been given at the end of the presentation.

This concludes the presentation of the relevant results. The following section analyses and discusses the quantitative results gathered, and uses the qualitative traits identified to investigate further possible motives.
7.0 ANALYSIS

This section analyses the data presented in the results section (Section 6) and forms a critical appraisal. As an overall aim of this investigation is to transform behaviour in end-users by educating them, this section will explore the extent to which behaviour changed as a result of the educational material provided. This analysis is presented under the following sections: user awareness and user behaviour.

7.1 User Awareness

The data collected regarding participants’ estimated computer security awareness are represented in Figure 6. As discussed in section 3.1 of the literature review user lack of user awareness is a current threat to computer security in many contexts. Ernst & Young (2004) found “lack of employee awareness” as the top obstacle in achieving an effective computer security solution. Wade (2004) states “All too often it is the people aspect that breaks down” (p. 1). Ernst & Young (2004) who surveyed 1,233 organisations from 51 countries and duly discovered that a “lack of employee awareness” was listed as the top obstacle in providing an effective computer security solution. Quantitative results gathered in the investigation align with these findings of low levels of computer security awareness among users. Fourteen out of a total of twenty participants, recorded an estimated level of computer security awareness of five or below prior to viewing the package.

Also identified in the literature review was that the most common difficulty for organisations was reported as “changing user attitudes and behaviour (reported by 65 percent of respondents)” (AusCERT, 2004, p. 3). On average, an increase in estimated awareness of three points (on a scale of one to ten) was recorded by participants. This demonstrates that within the sample population of twenty participants, the average perceived security awareness increased. Seventeen out of twenty people reported an increase in awareness, the three participants who did not register a change each had perceived computer security awareness’ of eight or above prior to viewing the package. It is speculated that the reason for this lack of change is that the content covered by the package was already understood by these participants. As the package is aimed at users with a low level of computer literacy it does not contain advanced topics that may benefit these participants.
As shown in the investigation results (Section 6.1.1), five participants recorded a one point decrease in pre-package awareness after viewing the package. One respondent reported a decrease of two, another reported a decrease of three and one respondent reported a decrease of four. These decreases indicate that, within the population of twenty participants, seven people reported a decrease in how aware they viewed themselves as being before the package. As the scale on which participants rated themselves is a perceived estimation, this change underlines that before the package they were actually less aware than they thought they were. The qualitative traits identified in section 7.1.1 show this, with four respondents indicating that they did not realise how little they knew about computer security and how important it was. Section 7.1.2 also saw the trait highlighting that users didn’t realise how little they knew about computer security appear in ten responses. These qualitative results provide an insight into this finding of levels of awareness within the population. These end-users either didn’t realise how little they knew, or did not view the topic as important enough to warrant increasing their own knowledge.

In conclusion, it was discovered that within the sample population, the majority of participants had an admitted low level of computer security awareness. These findings are supported by the literature review which established a current lack in overall security awareness by users. It was speculated that one reason for this was that users did not realise how unaware they were, and therefore, did not seek to increase their awareness. After viewing the presentation seventeen respondents indicated that they felt more aware, this awareness is of trivial importance if it does not materialise in behaviour; the following section analyses whether or not this occurred.

7.2 User Behaviour
This section analyses the change in the behaviour recorded within the population. Results for this section are displayed in Figure 5. As the main aim of the package was to change users’ behaviour, the results identified in this section will provide an insight into the effectiveness of the package within the population. As stated in the document background (Section 2), “the aim of education is to change behaviour” (Greer, 1997, p. 9). Section 3.4 in the literature review establishes a successful learning environment as one that establishes a need or desire within the learner to seek knowledge on the topic. It is speculated that the package achieved this goal by presenting the dangers of unsafe computing and some possible scenarios that, in real life, would have a great effect of the
participant. It is then stated, that once this has been achieved, the teacher facilitates the acquisition of knowledge, providing the learner with the necessary skills to acquire knowledge. The package does this by explaining the fundamentals of certain core aspects of computer security. It also achieves this by allowing the participant to control, to a certain extent, the direction of the package as it was being presented.

Demonstrated in Figure 5 is the claimed behaviour change for each individual in the population. The following is a simplified representation of how many participants claimed to have changed their behaviour.

<table>
<thead>
<tr>
<th>SECTOR 1</th>
<th>SECTOR 2</th>
<th>SECTOR 3</th>
<th>SECTOR 4</th>
<th>SECTOR 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed their passwords</td>
<td>No longer opened suspicious or unknown emails</td>
<td>No longer logged onto their computer</td>
<td>Turned off or disconnected their computer when not using the Internet</td>
<td>No longer visited erroneous web sites</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

From Table 4, it can be seen that in every aspect of unsafe computing covered by the investigation, a claimed behaviour change occurred. When compared with the initial willingness of participants to change behaviour as stated in Section 6, Table 4 indicates a large difference in participants’ willingness and whether or not they actually changed behaviour. In all of the above sectors, except sector one, all participants recorded that they were more willing to change behaviour. Sector five reported the highest behaviour change with half of the respondents who indicated they were willing, actually changing their behaviour.

Changes in each section differed, out of fourteen respondents who stated they previously used unsafe passwords, five claimed to have changed their behaviour and employed a safer password. Section 7.2.3 provides one possible explanation for this behaviour change, identifying a trait in qualitative responses indicating participants were not aware how important having a secure password is. The following discusses the change in use of computer security countermeasures.
AusCERT (2005) found that “inadequate levels of security on home and other computers used by clients, customers and staff” (p. 30) was listed by 26% of respondents. The findings of this investigation were that more than half of the twenty participants employed what was defined as acceptable tools in section 3.3 of the literature review. The figures indicate the number of participants relevant to each section. As shown in the following table, a claimed increase in use of computer security tools occurred within the population.

<table>
<thead>
<tr>
<th>FIREWALLS</th>
<th>ANTIVIRUS SOFTWARE</th>
<th>ANTI-SPYWARE SOFTWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>After</td>
<td>13</td>
<td>19</td>
</tr>
</tbody>
</table>

These findings tend to align with two notions identified in the literature review. The first is that user education will change the behaviour of end-users, thus establishing a safer operating environment. The second notion supported, is that a constructivist approach to teaching is an effective way to educate users. By establishing a need or desire for behaviour change the inclination of the individual to seek knowledge is increased.

In conclusion, the results obtained from the investigation seem to support the notion, identified in the literature review, that the construction of a desire to learn is an effective means by which to educate. Within the population, an increase in computer security awareness was identified coupled with a claimed change in behaviour and implementation of countermeasures.
8.0 CONCLUSIONS AND FUTURE RECOMMENDATIONS

The learning theories of constructivism, behavioural approaches and Andragogy were taken into account in designing the educational package addressing computer security issues. The package was presented to twenty participants, who were required to complete questionnaires to determine their responses to the package. The investigation adopted an explanatory mixed methods research approach, as defined by Creswell (2005).

8.1 Research Question

The literature supported the notion that educating end-users results in a more secure operating environment. The research question, “would the provision of an educational package addressing computer security issues change end-users’ behaviour and use and implementation of computer security systems?” is explained as follows. By empowering participants to accept greater responsibility in addition to seeking knowledge, the package was successful in changing end-user’s behaviour within the group studied. Use of computer security tools within the population was shown to increase as a result of the package. A high percentage of participants adopted safer behaviour as a result of the package. User education is not the only solution to increasing computer security, however, if users are aware of the various threats to computer security and the ways in which they can prevent, or mitigate, these threats, a more secure operating environment will result.

8.2 Limitations

Although the research successfully addressed the research question, the following limitations are recognised. Population size was limited to twenty participants who lived in the Bunbury area. This limits the investigation, as the sample population represents a small fraction of computer end-users, and prevents the application of statistical algorithms to quantitative data thereby reducing generalisability.

8.3 Future Recommendations

The following recommendations are suggested as a result of this investigation. An increased population size would provide increased integrity to the investigation and greater representation of computer end-users. As suggested by respondents, the addition of more interactivity within the package is recommended. This also aligns with Knowles’ Theory of Andragogy and the Theory of constructivism. A wireless
demonstration allowing interactive control of computer from a remote locating is suggested, as this will show participants that a physical connection is not required for a computer to be vulnerable. In addition, the provision of a longitudinal survey will allow a single group of users to be followed and behavioural changes tracked.
9.0 REFERENCES


10.0 APPENDICES

10.1 Appendix A – Presentation

Contents

1 Introduction

2 Background

3 Attackers, Internet Protocol
  IP addresses, Port numbers

4 IP and Ports

5 Firewalls

6 How a firewall works

Computer Security Presentation

Sam Jones
2005

Introduction

This presentation will cover the fundamentals of computer security topics.
Understand that this presentation is to give you an understanding of how security is breached and
methods of preventing breaches.
You are not expected to understand everything,
please feel free to ask questions at any time.

2 Background

Why is information important?
What is the difference between this presentation and other sources of
information?
This presentation is different because it
will empower you with knowledge of
computer security issues.

3 Attackers, Internet Protocol

IP addresses, Port numbers

IP address is the most important piece of information to an attacker.
IP address is your location on the
internet.
Every time you connect the internet your IP
address changes.
An example of an IP address is:
192.168.0.1
Ports are used to transfer information in and out
of your computer.

4 IP and Ports

An example of a port is:
TCP/123
TCP/IP address is the equivalent of your home
door and windows are the equivalent of your
doors and windows to your house
Open doors and windows to your house
A connection to your computer would look like
192.168.0.2:1151

5 Firewalls

Firewalls block programs and attackers
from accessing your computer.
Firewalls monitor your IP address (and the IP
address of the person attempting to
contact you) and your Ports.
A firewall is like having a bouncer at your
front doors and windows.

6 How a firewall works

A firewall is situated between the information on your computer and the Internet. All
traffic coming in and out of your computer will pass through the firewall.
4.2 Firewalls explained

A firewall is a device between the information on your computer and the Internet. All traffic coming in and out of your computer will pass through the firewall. Traffic reaching the firewall (whether it is entering or leaving your computer) is analysed using security tests. If the traffic passes the test then it is allowed through, if not, it is blocked.

4.3 Firewalls explained 2

A firewall will greatly improve the security of your computer.

However, attackers may disguise attacks as genuine information to gain access to your computer.

Downloading erroneous information and opening erroneous email can allow attackers to bypass your firewall.

5. Malicious software - Malware

5.1 Viruses

• Viruses are human interaction to start.
• Viruses are a program or double clicking on a file.
• Viruses downloaded from email attachments.

5.2 Worms

• Worms are self-propagating programs.
• The defining characteristic is replication.
• Once they are released they travel across networks and across the internet by themselves.
• They are responsible for using resources and bandwidth.

5.3 Trojan Horses

• Trojan Horses are invisible to a program.
• They are not evil in your computer.
• The program may be downloaded via an email.
• Trojan Horses may either send information out of your computer (for example keystrokes) or create a back door into your computer.
• This "back door" may be used by attackers to gain easy access to your computer.

5.0 Anti-virus software

• Use anti-virus software to keep your computer clean.
• Use up-to-date anti-virus software.
• Use new anti-virus software once per week.
7.1 Passwords 1 - 3

- Passwords are the main form of identification
- They are used in most computers and computer programs
- Write your password down
- Change your password regularly
- Strong passwords should be chosen

7.2 Passwords 3 - 4 Importance

- It is important to have a strong password

9.0 Password crackers

- There are many methods to crack passwords
- One method is to use a dictionary
- The attacker tries combinations of letters and words until they find a match
- The longer the password the longer it will take to crack
- In the case of an 8 character password it is approximately 118 hours
- The attacker can also try words that match commonly used phrases and words against the passwords. If your password is a common word or contains numbers the attack can be very effective.

9.01 Logging On and Off

- It is important to log on to your computer when you have finished using it.
- It matters how much security is put in place if you leave your computer logged on other people have access to all your files.
- People may also use your computer for malicious activity and all events will be recorded under your name.

10.0 Social Engineering

- Employees may use social engineering in order to make you disclose information.

13.0 Other

- Turn off your computer/modem when you are not using it. If your computer is turned off it is impossible to hack into.
- Frequently clear your Cookies and offline content.
References

1. Windows XP
2. DesktopScout
3. www.microsoft.com

DesktopScout version 4.0 available:
www.labcastrol.net/desktopscout/
10.2 Appendix B – Pre-Package Questionnaire

Dear Sir/Madam,

I would like to invite you to take part in the enclosed survey and subsequent study. I am enrolled as a full time honours student at Edith Cowan University in Bunbury. This semester I am completing a thesis based on educating users in computer security issues. Should you choose to take part in this study a one and a half hour session will be conducted. The session will consist of between two and five other individuals and will outline security elements of computing. You will be taught how to make better use of computer security countermeasures.

I appreciate that you are busy and your time is valuable, however, I hope that you are able to find time to support me in my endeavours. I am happy to answer any questions you may have, please feel free to contact me via phone or email.

All personal information gathered will be de-identified immediately and destroyed upon the completion of research. Reference to individuals in any subsequent papers will be achieved through a non-identifiable alpha-numeric code.

Yours sincerely

Sam Jones
COMPUTER SECURITY INFORMATION PRESENTATION

PLEASE FILL OUT THE FORM BELOW DETAILING DEMOGRAPHIC AND AVAILABILITY INFORMATION.

EDITH COWAN UNIVERSITY – HONOURS RESEARCH

INFORMATION GATHERED FROM THIS PRESENTATION WILL BE USED TO INVESTIGATE THE IMPACT OF EDUCATING COMPUTER USERS ON COMPUTER SECURITY ISSUES AND COUNTERMEASURES.

CONTACT DETAILS
Sam Jones
Mobile: 0427479496
Home: 97959782
Email: sdjones@student.ecu.edu.au

Please select which time(s) most appropriately suit(s) you:

<table>
<thead>
<tr>
<th>Monday 3rd Oct</th>
<th>Tuesday 4th Oct</th>
<th>Wednesday 5th Oct</th>
<th>Thursday 6th Oct</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:00 – 08:30</td>
<td>9:00 – 10:30</td>
<td>07:00 – 08:30</td>
<td>07:00 – 8:30</td>
</tr>
<tr>
<td>15:00 – 16:30</td>
<td>11:00 – 12:30</td>
<td>15:00 – 16:30</td>
<td>09:00 – 10:30</td>
</tr>
<tr>
<td>17:00 – 18:30</td>
<td>13:00 – 14:30</td>
<td>17:00 – 18:30</td>
<td>11:00 – 12:30</td>
</tr>
<tr>
<td>19:00 – 20:30</td>
<td>15:00 – 16:30</td>
<td>19:00 – 20:30</td>
<td>13:00 – 14:30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Friday 7th Oct</th>
<th>Sunday 9th Oct</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:00 – 8:30</td>
<td>07:00 – 8:30</td>
<td>Other</td>
</tr>
<tr>
<td>09:00 – 10:30</td>
<td>09:00 – 10:30</td>
<td></td>
</tr>
<tr>
<td>11:00 – 12:30</td>
<td>11:00 – 12:30</td>
<td></td>
</tr>
<tr>
<td>13:00 – 14:30</td>
<td>13:00 – 14:30</td>
<td></td>
</tr>
<tr>
<td>15:00 – 16:30</td>
<td>15:00 – 16:30</td>
<td></td>
</tr>
<tr>
<td>17:00 – 18:30</td>
<td>17:00 – 18:30</td>
<td></td>
</tr>
</tbody>
</table>

QUESTIONNAIRE

NAME:

CONTACT NUMBER:

EMAIL:
AGE:
0 – 20 □
20 – 25 □
26 – 35 □
36 – 50 □
50 – 100 □

ESTIMATED COMPUTER USE (HOURS PER WEEK)?
0 – 2 □
2 – 10 □
10 – 20 □
20 – 40 □
Over 40 □

FOR WHAT DO YOU USE YOUR COMPUTER?
Home □
Work □
Gaming □
Study □
Internet □
Other □ - Please state

DO YOU USE THE INTERNET FOR?
Internet banking □
Email □
Research □
Purchasing products □
**WHICH OF THE FOLLOWING ARE CURRENTLY INSTALLED, UP-TO-DATE AND RUNNING ON YOUR HOME COMPUTER?**

<table>
<thead>
<tr>
<th>firewall</th>
<th>Yes</th>
<th>No</th>
<th>Unsure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus software</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Antispyware software</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

**Estimated understanding of computer security issues:**

1 □ - Basic  
2 □  
3 □  
4 □  
5 □  
6 □  
7 □  
8 □  
9 □  
10 □ - Excellent

**Thankyou for expressing interest and participating in this project. Please contact me and I will arrange for collection of the questionnaire.**
10.3 Appendix C – Initial Post-Presentation Questionnaire

NAME:

POST PRESENTATION QUESTIONNAIRE

PLEASE SELECT YOUR ESTIMATED UNDERSTANDING OF COMPUTER SECURITY ISSUES BEFORE AND AFTER THE PRESENTATION.

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

WILL YOU NOW BE MORE INCLINED TO (PLEASE ANSWER YES OR NO)?

Use a more secure password?
Not open emails from suspicious senders?
Not visit erroneous websites?
Keep antivirus software up-to-date and scan regularly?
Use a firewall?
Not log other people into your account?
Turn your computer off or disconnect when you are not using the Internet?

Thankyou for your participation.
Sam Jones
10.4 Appendix D – Two Week Post-Package Questionnaire

NAME:

PLEASE COMPLETE THE FOLLOWING SECTIONS TO THE BEST OF YOUR ABILITY.

In the context of computer security your IP address is:

a) Your Intellectual Property address.
b) Your Internet Protocol address.
c) Your International Pass-code address.
d) Your Internet Ping address.

Your IP address above is best described as:

a) The logical address of your computer on the Internet.
b) An Internet based authentication method.
c) The power of your computer.
d) The length of time you have been connected to the Internet.

In the context of computer security a firewall is:

a) A mechanism to control access to a computer system and block unwanted and malicious data.
b) A covering blanket for your computer, it keeps your computer cool and protects it from dust.
c) A physical wall around your computer that prevents it from being stolen.
d) The logical address of your computer on the Internet.

Please select the “strongest” password from the list below.

a) qi92mw252fe
b) cat
c) filament
d) hello34

Why is it important to have a strong password?

a) Because strong passwords are easier to remember.
b) Because strong passwords can be typed quickly.
c) Because you can tell people what it is.
d) Because strong passwords are harder to crack.
Your bank or any other financial institution will send you emails asking to confirm your login details?

a) Yes  
b) No

PLEASE state True OR False to each of the following questions.

Prior to viewing the package I was using an insecure password.  
If True. I have now changed it to be more secure.

Prior to viewing the package I was opening emails from suspicious senders and unknown senders.  
If True. I no longer open emails if I am wary of the sender.

Prior to viewing the package I logged others onto my account.  
If True. I no longer log others onto my account

Prior to viewing the package I did not disconnect or turn my computer off when not using the Internet.  
If True. I now disconnect or turn my computer off when using the Internet.

Prior to viewing the package I visited erroneous websites.  
If True. I no longer visiting erroneous web sites.

I now use a firewall.

I now use up-to-date antivirus software and scan regularly.

I now use up-to-date antispyware software and scan regularly.

Thankyou for your participation.
Sam Jones
Appendix E – Final Qualitative Questionnaire

NAME:

PLEASE COMPLETE THE FOLLOWING SECTIONS TO THE BEST OF YOUR ABILITY.

Explain your view of computer security before the package and, if you listed your estimated computer security awareness as below 5 before the package please describe:

d) Whether or not you sought information on computer security to become more aware

e) If you didn’t please explain you reasons for not doing so.

f) If you did please describe how easy it was to find and understand.

________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________

Explain, in your own words, your view of the package.

________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________

Explain if and how the package changed your view of computer security.

________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
How do you think this presentation could have been improved?

Thank you for your participation.

Sam Jones
10.6 Appendix F – Population Demographics

Figure 7 Graph showing the sample population age

Figure 7 represents the ages of the sample population.

Figure 8 Graph showing computer use (hours per week) within the sample population

Figure 8 illustrates the amount of time participants spent using computers per week.
10.7 Appendix G – Population Behaviour

Figure 9 Graph showing computer use (activities) within the sample population

Figure 9 shows the relevant activities that participants within the population used computers for.

Figure 10 Graph showing Internet use (hours per day)

Figure 9 shows the amount of time that participants’ computers spent connected to the internet per day.
Figure 11 Graph showing activities performed on the Internet

Figure 11 shows activities which participants performed on the internet.
Figure 12 Graph showing the populations willingness to change behaviour after viewing the package.

Figure 12 shows how willing participants were to change their behaviour in each area immediately after viewing the package.