Educating users about information security by means of game play

by

Thomas Philippus Monk

Dissertation

submitted in fulfillment of the requirements for the degree Magister Technologiae in Information Technology in the Faculty of Engineering, The Built Environment and Information Technology of the Nelson Mandela Metropolitan University

Supervisor: Johannes F. van Niekerk
Co-Supervisor: Prof. Rossouw von Solms
Abstract

Information is necessary for any business to function. However, if one does not manage one’s information assets properly then one’s business is likely to be at risk. By implementing Information Security controls, procedures, and/or safeguards one can secure information assets against risks. The risks of an organisation can be mitigated if employees implement safety measures. However, employees are often unable to work securely due to a lack of knowledge.

This dissertation evaluates the premise that a computer game could be used to educate employees about Information Security. A game was developed with the aim of educating employees in this regard. If people were motivated to play the game, without external motivation from an organisation, then people would also, indirectly, be motivated to learn about Information Security. Therefore, a secondary aim of this game was to be self-motivating. An experiment was conducted in order to test whether or not these aims were met.

The experiment was conducted on a play test group and a control group. The play test group played the game before completing a questionnaire that tested the information security knowledge of participants, while the control group simply completed the questionnaire. The two groups’ answers were compared in order to obtain results. This dissertation discusses the research design of the experiment and also provides an analysis of the results. The game design will be discussed which provides guidelines for future game designers to follow.

The experiment indicated that the game is motivational, but perhaps not educational enough. However, the results suggest that a computer game can still be used to teach users about Information Security. Factors that involved consequence and repetition contributed towards the educational value of the game, whilst competitiveness and rewards contributed to the motivational aspect of the game.

Keywords: Information security, Information security education, Educational game design
Acknowledgements

I would like to thank the almighty heavenly Father who makes everything possible.

My family and friends for all their support.

My supervisor, Johan van Niekerk, for all his guidance and my co-supervisor, Professor von Solms, for the motivation he gave me.

Finally, I would like to thank NMMU and NRF for their financial support.

Thank you!
Table of Contents

Chapter 1: Introduction ............................................................................................................. 1
  1.1 Introduction .................................................................................................................... 1
  1.2 Problem Relevance ......................................................................................................... 3
  1.3 Problem statement ......................................................................................................... 5
  1.4 Thesis Statement ........................................................................................................... 5
  1.5 Research Objectives ..................................................................................................... 6
    1.5.1 Primary Research Objective ................................................................................. 6
    1.5.2 Secondary Research Objectives ......................................................................... 6
  1.6 Research process .......................................................................................................... 6
  1.7 List of chapters ............................................................................................................. 7

Chapter 2: Information Security ............................................................................................... 8
  2.1 Introduction ................................................................................................................... 8
  2.2 Information security in general ................................................................................... 9
    2.2.1 Asset ...................................................................................................................... 9
    2.2.2 Vulnerability ......................................................................................................... 10
    2.2.3 Threat .................................................................................................................. 10
    2.2.4 Risk ..................................................................................................................... 10
    2.2.5 Controls ............................................................................................................... 11
  2.3 Information as an asset ............................................................................................... 13
    2.3.1 Confidentiality .................................................................................................... 14
    2.3.2 Integrity ............................................................................................................... 14
    2.3.3 Availability ......................................................................................................... 15
  2.4 Five dimensions of information security awareness ..................................................... 15
    2.4.1 The organisational dimension ............................................................................ 16
    2.4.2 The general public dimension ............................................................................ 16
3.4 Awareness, training and education ................................................. 39
  3.4.1 Awareness .................................................................................. 40
  3.4.2 Training ..................................................................................... 40
  3.4.3 Education .................................................................................. 41
3.5 Education to reach unconscious competence .................................... 42
  3.5.1 Unconscious incompetence ....................................................... 42
  3.5.2 Conscious incompetence ........................................................... 43
  3.5.3 Conscious competence ............................................................... 43
  3.5.4 Unconscious competence .......................................................... 43
3.6 Problems of current education methods ........................................ 44
  3.6.1 Motivation .................................................................................. 44
  3.6.2 Time and money ........................................................................ 44
  3.6.3 Facilitates one form of learning .................................................. 45
  3.6.4 General public education ............................................................ 45
3.7 Identifying target audience ............................................................. 46
3.8 Education in the business and larger social context ....................... 47
  3.8.1 Target audience should be able to understand the content .......... 47
  3.8.2 Learning repetitively .................................................................. 47
  3.8.3 Practical teaching ....................................................................... 48
  3.8.4 Provides feedback ..................................................................... 48
  3.8.5 Learners responsible for their own learning .............................. 49
  3.8.6 Accessible from home and work ............................................... 50
3.9 Conclusion ...................................................................................... 50

Chapter 4: Educational Games .............................................................. 52
  4.1 Introduction ................................................................................... 52
  4.2 Educational games as a solution to information security problems ... 52
    4.2.1 Self-motivation ........................................................................ 53
    4.2.2 Can reach general public ....................................................... 53
4.2.3 Use multiple teaching methods ................................................................. 54
4.2.4 Supports feedback ...................................................................................... 54
4.2.5 Games as part of information security culture ............................................. 54
4.3 Problems related to educational games used for information security education ................................................................................................................... 55
4.4 What is an educational game? ........................................................................ 56
4.5 Individual analysis of educational games ....................................................... 58
  4.5.1 Puzzles .......................................................................................................... 59
  4.5.2 Simulations .................................................................................................... 60
  4.5.3 Reading/Dialog ............................................................................................. 63
  4.5.4 Unconscious learning .................................................................................. 64
  4.5.5 Collaborative learning .................................................................................. 65
  4.5.6 Games that use multiple teaching methods ................................................. 65
  4.5.7 Games relating to information security ....................................................... 69
  4.5.8 Discussion of content .................................................................................. 71
4.6 Design factors for an educational game on information security .................. 73
  4.6.1 Force players to learn .................................................................................. 73
  4.6.2 Creating an understandable game ............................................................... 74
  4.6.3 Prevent negativity surrounding educational games ...................................... 74
  4.6.4 Include motivational techniques ............................................................... 75
  4.6.5 Implement a grading system ...................................................................... 75
4.7 Conclusion ........................................................................................................ 76
Chapter 5: Experimental Design ........................................................................ 78
  5.1 Introduction ..................................................................................................... 78
  5.2 Research process .............................................................................................. 78
  5.3 Strengths and weaknesses of methods ............................................................ 79
  5.4 Implementation of Hevner's design-science .................................................. 82
    5.4.1 Design as an Artefact ................................................................................. 82
5.4.2 Problem Relevance ......................................................................................... 82
5.4.3 Design Evaluation ......................................................................................... 83
5.4.4 Research Contributions ............................................................................... 83
5.4.5 Research Rigor ............................................................................................... 83
5.4.6 Design as a Search Process .......................................................................... 84
5.4.7 Communication of Research ......................................................................... 84
5.5 Design of the research process ......................................................................... 84
5.5.1 The prototype ................................................................................................ 85
5.5.2 The questionnaire .......................................................................................... 88
5.5.3 The experiment ............................................................................................... 89
5.6 Limitations ......................................................................................................... 91
5.7 Ethical considerations ....................................................................................... 93
5.8 Conclusion ......................................................................................................... 93
Chapter 6: Implementation ..................................................................................... 95
6.1 Introduction ....................................................................................................... 95
6.2 Selecting the educational content ...................................................................... 95
6.2.1 Email attacks (i.e. Spam) .............................................................................. 96
6.2.2 Phishing/Pharming ....................................................................................... 97
6.2.3 Viruses/Worms outbreaks ............................................................................ 98
6.2.4 Spyware ......................................................................................................... 99
6.2.5 Employee misconduct .................................................................................. 99
6.2.6 External financial fraud involving information systems ......................... 101
6.2.7 Social engineering ...................................................................................... 101
6.2.8 Physical threats ............................................................................................ 102
6.3 Transforming educational content into game content ..................................... 103
6.3.1 Refining the list of security threats .............................................................. 103
6.3.2 Creating game scenarios ............................................................................ 105
6.4 Implementation of the game ............................................................................. 106
6.4.1 Overview .............................................................. 106
6.4.2 How the game is played ........................................ 108
6.4.3 How the game conveys educational content .............. 109
6.4.4 Teaching methods .................................................. 115
6.4.5 Motivational aspects ............................................... 117
6.5 Preliminary evaluations .............................................. 118
6.6 Conclusion ................................................................ 119

Chapter 7: Results and Discussions .................................... 120
7.1 Introduction ................................................................ 120
7.2 Results of the preliminary evaluations ......................... 120
7.3 Results of the experiment ........................................... 121
7.4 Results of the questionnaire ....................................... 123
7.5 Discussion of results ................................................... 126
7.5.1 Educational content ............................................... 126
7.5.2 Motivational factors .............................................. 127
7.5.3 Hidden content ..................................................... 128
7.5.4 Graphics ............................................................. 129
7.5.5 Competitive scores ............................................... 130
7.5.6 Repeated play ...................................................... 130
7.5.7 Force players to learn ............................................ 131
7.5.8 Simulation, knowledge acquisition/testing, reading/dialog (multiple teaching methods) ...................................................... 131
7.6 Conclusion ................................................................ 133

Chapter 8: Conclusion ....................................................... 135
8.1 Introduction ................................................................ 135
8.2 Summary ................................................................... 135
8.3 Possible Further Enhancements .................................... 138
8.3 Conclusion ................................................................ 138
References .......................................................................................................................... 139
Appendices ..................................................................................................................... 148
Appendix A ...................................................................................................................... 149
Appendix B ...................................................................................................................... 158
Appendix C ...................................................................................................................... 168
Appendix D ...................................................................................................................... 173
List of Figures

Figure 2.1: Components constituting a Risk - Adapted from von Solms & von Solms (2008, p101) ........................................................................................................................................... 11

Figure 2.2: Threats, Vulnerabilities, Safeguards, and Assets - Adapted from NIST (1995, p. 62) ........................................................................................................................................... 13

Figure 2.3: Information Security Risk Management Process as Described by Goguen et al (2002) ........................................................................................................................................... 19

Figure 3.1: The location of the learning models along the philosophical continuum ........................................................................................................................................... 31

Figure 3.2: The Dimensions of the Learning Theories Adapted from Leidner & Jarvenpaa (1995) ........................................................................................................................................... 37

Figure 5.1: The Information Systems Development Approaches - Adapted from Alavi (1984) ........................................................................................................................................... 86

Figure 6.1: Main window of Cash City ........................................................................................................................................... 107

Figure 6.2: Desktop simulated in Cash City ........................................................................................................................................... 110

Figure 6.3: The email program with an example message ........................................................................................................................................... 111

Figure 6.4: The anti-spyware program within the game ........................................................................................................................................... 112

Figure 6.5: The "congratulations" message ........................................................................................................................................... 112

Figure 6.6: The "you are fired" message ........................................................................................................................................... 113

Figure 6.7: The "Create New Password" window ........................................................................................................................................... 114

Figure 7.1: Comparison of games scores to the amount of security mistakes made by players ........................................................................................................................................... 122
List of Tables

Table 2.1: Summary of examples of risks.................................................................12

Table 4.1: Summary of puzzle educational games ..............................................60

Table 4.2: Summary of simulation educational games .......................................62

Table 4.3: Summary of reading/dialog educational games .................................64

Table 4.4: Summary of educational games that uses unconscious learning .........64

Table 4.5: Summary of educational games that uses collaborative learning ........65

Table 4.6: Summary of educational games that uses multiple teaching methods .................................................................68

Table 4.7: Summary of educational games on information security .................70

Table 6.1: Top 8 repeated external breaches experienced - Adapted from Deloitte (2009, p. 31) .................................................................96
Chapter 1: Introduction

1.1 Introduction

When businesses started using computers to store information it seemed that all the problems related to controlling information would be solved. Unfortunately, these solutions introduced other problems. One of these problems is security (Sharma & Sefchek, 2007).

Computer security is crucial to modern companies, because, although widespread access to business information may be necessary, misuse of that information must be prevented. People who want to gain access to business information include hackers, scammers and people who want to commit other criminal activities. When cyber criminals, such as described above, obtain information illegally the consequences may include: a loss of assets, ruined company reputations and businesses closing down. Computer viruses can have similar consequences although viruses are generally not written to infect a specific institution.

Protecting electronic information is also known as Information Security. Information Security is a multi-faceted discipline that depends on hardware, software and people. Hardware, such as firewalls, helps a great deal towards securing information. Programming standards ensure that software supports an adequate level of security, when the developers follow those specific standards. The users of the system are the main source of information security breaches (Ernst & Young, 2008; Deloitte, 2009) and remain to be the weakest link in the security chain. Cyber criminals prefer to target the users of the system to gain entry to information, because that is the most vulnerable facet of the security system.

Companies try to teach their employees how to protect information by making use of information security education, training and awareness. Information security awareness makes employees aware of security threats and controls; this is usually achieved by using posters or other physical reminders. Information security training teaches the
employees how to protect themselves against security threats; this is usually achieved through lectures and workshops. Information security education provides the employees with a deeper understanding of why they must secure information (von Solms & von Solms, 2008).

The problem with information security education, training and awareness is that many people are generally not motivated to learn on their own. Information security awareness may make employees aware of a security issue, but does not ensure that the employees understand how that message should be practiced.

Many home users may also benefit from learning how to protect their information. Home users often lack the education that business employees would have obtained. This makes them easy targets for cyber criminals who use viruses to gain access to their personal information such as credit card numbers. Increased general knowledge about information security would also alleviate costs associated with education when members of the general public become computer-oriented employees.

One way in which people can be motivated to learn about information security is to make it an enjoyable experience. A computer game might be a good solution to some of the identified problems related to information security, because:

- Computer games are often self motivational;
- Computer games can be used to verify whether knowledge has been obtained;
- Computer games can be distributed to home users to increase their general knowledge about information security.

In general, computer games have been very successful in the last couple of years. Good games generate enough fun and enjoyment for the player to remain occupied for long periods of time. Educational games are games that have an added goal in mind, in addition to the enjoyment factor: they also attempt to teach the player about a certain topic. Although relatively few educational games have done well commercially, they are
used to teach interesting subject content such as biology (Kelly et al., 2006) and history (McMichael, 2007; Underberg, 2008; Jenkins, Klopfer, Squire & Tan, 2003).

This research project proposes the use of a computer game that educates players on the subjects of information security awareness. This game will be targeted towards employees of companies who deal with information and lay Internet users.

The computer game needs to demonstrate the essential processes for securing one's information. The game must also reveal, to the player, what the biggest threats associated with information security are and what the consequences are of weak security.

1.2 Problem Relevance

Handling information security has been, and continues to be, a huge problem for companies. Some researchers, such as Furnell, Jusoh & Katsabas (2006), inspect how software should be developed to enhance information security. However, Deloitte’s survey (2009) indicates that human error is the greatest cause (86%) of information security failure, while technology is the second greatest cause (63%). Therefore, this project will focus on the human aspect of information security.

Users are often ignorant of the impact of their actions when they are using information systems. Information security programs attempt (Albrechtsen, 2007; Puhakainen, 2006) to solve this problem by educating the users about information security. However, for various reasons these programs often fail. One reason for the failure of security programs is that the role of motivation is often not taken seriously enough (Siponen, 2000).

Another reason can be identified through learning science, which reveals that people have diverse learning preferences (NIST, 2009). As people become older they develop their own preference of how to learn new things. For some people reading related material is a good way to learn something new, while other people prefer a “hands on” approach to grasp new ideas. Thus, some people may learn enough from traditional
information security programs while others need to be educated through another medium.

Increasing the general knowledge of information security would also make information security programs more successful. Siponen (2001) identifies a *general public dimension* as one of his five dimensions of information security. The general public is often oblivious of security threats such as phishing and spam (Furnell, Bryant & Phippen, 2007), while novice internet users often lack the knowledge to protect themselves against those kind of threats (Furnell, Tsaganidi & Phippen, 2008).

Video games can serve as a motivational tool and also facilitate learning (Prenski, 2001). Educational games have been suggested to be used for school curriculums (Bottino & Ott, 2006) and have been used for tertiary education (Underberg, 2008; McMichael, 2007; Kelly et al., 2007). Educational games have taught students a host of different subject content, such as: biology (Kelly et al., 2006), history (McMichael, 2007; Underberg, 2008), physics and environmental science (Jenkins et al., 2003).

Research has been conducted by making use of a scenario-based program to educate users about information security (Furnell, Gennatou & Dowland, 2000). Further research has been conducted by making use of computer games to educate players about security issues (Cone, Irvine, Thompson & Nguyen, 2007; Sheng et al., 2007). However, no research project has been found that targets all users of electronic information.

Various studies have been conducted to determine which game genre is more popular (Amory, Naicker, Vincent & Adams, 1999) and also which game genre is better suited to be used for educational purposes (de Castell & Jenson, 2003). Game genres determine how the game is played, viewed and often how one will learn by playing the game. For example Dickey (2007) proposes an educational game that will follow the MMORPG (Massively Multiplayer Online Role Playing Game) game genre. By making use of this genre one would expect to learn from the game’s dialog, physical experience and perhaps learning through collaboration with other online players.

Unfortunately, merely identifying a game genre in order to develop a game is not where the design phase ends. Various educational games need certain game elements to work
correctly in order to make the game a success, regardless of its genre. These game elements fit the nature of those named by Squire et al. (2003).

The game elements need to ensure that all the employees of a company can learn security concepts as specified by international standards (ISO 27002, 2005). Information users outside company boundaries can also benefit from the game to increase general knowledge about information security (Siponen, 2001), while diverse learning strategies are being used to convey the subject matter.

In summary, information security risks are a growing concern, which is a big threat to private information. Educating the people who use information about these risks should significantly reduce the number of victims to the companies who are at risk. Therefore, fewer information assets will be stolen and, as a result, fewer risks should occur in the future. However, many information security programs fail to educate their learners satisfactorily. This project will test an information security program in the form of a computer game, because games are motivational and they can use diverse learning strategies. They can also reach the general public, who are targeted by security threats and, therefore, they need to be educated regarding it.

1.3 Problem statement

All users of electronic information need to be educated about information security, but traditional information security awareness programs do not cater satisfactorily for diverse learning preferences.

1.4 Thesis Statement

Computer games can be used to effectively educate users about information security.
1.5 Research Objectives

1.5.1 Primary Research Objective

The primary research objective of this dissertation will be to indicate how computer games can be used to effectively educate users about information security.

1.5.2 Secondary Research Objectives

In order to attain this primary objective several secondary research objectives have been defined. These secondary objectives include:

- To develop a computer game to educate users about information security related concepts;

- To determine whether the game is “popular” enough for users to play it without external coercion;

- To determine whether the game successfully conveys information security concepts.

1.6 Research process

An extensive literature review has been conducted in order to find out what the academic community knows about the information security and educational gaming research fields. First, a broad literature review was conducted to provide general background regarding the subject matter. This was followed by more specific literature reviews that examined specific aspects of the research fields.

An experiment by means of a prototype took place to determine how people perceived the game. There were two groups of participants: the first group played the game and completed the questionnaire while the second group only completed the questionnaire. The questionnaire contained the same information security questions for both groups.
Questionnaires were used to determine what the participants knew about information security. The results of the questionnaire for the group that played the game were compared with the results of the group that did not play the game. This gave an indication of whether or not the game had educational value. The participants had the opportunity to play the game again if they wished to do so; this gave an indication of whether or not the game motivated people to play it. Qualitative methods were used to analyse these results.

1.7 List of chapters

This dissertation has been laid out in accordance to the general guidelines provided in Hofstee, 2006, p. 35-43. The following provides a brief overview of the chapters of the dissertation:

1. Introduction. This chapter explains how this project fits into the research field and introduces the aims of the project.

2. Information Security. This chapter describes why information security is important and discusses the current problems it poses.

3. Information Security Education. This chapter describes information security education approaches and discusses why they fail.

4. Educational games. This chapter gives an overview of games that have been used to educate people.

5. Experimental Design. This chapter explains how the various elements of the experiment which tested the game were designed.

6. Implementation. This chapter describes how the elements of the experiment were implemented.

7. Results and discussions. This chapter discusses the research results and findings.

8. Conclusion. This chapter further discusses the research findings and concludes the project.
Chapter 2: Information Security

2.1 Introduction

People, in modern society, should consistently protect sensitive information against untrustworthy parties. Untrustworthy parties can use the sensitive information of other users (such as identity numbers or credit card numbers) to conduct criminal activities (such as fraud or theft). To protect information, people need to identify which of their information is sensitive; only thereafter, can they take necessary safety precautions. Therefore, people need to know what information is sensitive as well as how to protect it.

The classification of sensitive information has changed somewhat since the Internet became widely used. This is because the Internet connects people with untrustworthy parties very easily (Furnell & Ward, 2008). Furnell & Ward (2008) state that the Internet is similar to a jungle in this respect. A jungle contains predators that feed on other animals, which become their prey. Similarly, the Internet contains “legitimate” users (potential prey) with users who wish to exploit the information of other users (predators). Furthermore, it is difficult to regulate the Internet, because when governments start initiatives to review Internet content the private sector is likely to complain that these initiatives threaten their privacy (Endeshaw, 1998). Therefore, it is difficult to monitor the behaviour of Internet users and Internet predators. However, predators can only gain access to information, on computers, that are connected to the Internet. Therefore, users should identify what information, stored on their computer, can be used by someone else in a manner that would be harmful to its owner. By doing this they should determine which of their information is sensitive.

After users have become aware of what information requires protection, they need to implement some security measures. Information security is the process that people would use to protect their information and the systems that use it (van Niekerk & von Solms, 2010; Whitman & Mattord, 2003, p. 9). Users may choose to refrain from sharing
information over the Internet, which could be seen as a security control. However, these
users will not be able to reap many of the benefits that the Internet offers, as discussed
later in this chapter. The alternative is for users to learn proper practices which would
enable them to use and share their information in a secure manner. This dissertation
focuses on this alternative.

The remainder of this chapter examines information security as well as the people who
are affected by it. The importance of information will be discussed along with the
different types of controls, which can be implemented to protect it.

2.2 Information security in general

To understand Information security one should be familiar with the basic concepts of
security in general. In essence security can be described as the protection of assets
against threats through the introduction of controls to reduce the risks introduced by
vulnerabilities. The following sub-sections define these security concepts.

2.2.1 Asset

An asset is anything which adds value to the business (ISO 27002, 2005, p. 1). Therefore,
assets include physical items such as machinery, but also intangible possessions such as
information. Information is a very important asset to any business and it is often more
valuable than physical assets.

For example, if a file cabinet of a company is stolen containing records of clients, the most
important asset that has been lost, in this case, is the information on those records. The
cabinet and the paper therein can be replaced by buying new ones. However, if a backup
of the records does not exist, then each client needs to be contacted in order to recover
the information. Furthermore, if clients learn about the theft then they will lose trust in
the company, which is very difficult to regain. If the company does have a backup of the
records then an asset has still been lost because confidentiality, integrity or availability
(CIA) has been compromised. CIA is further examined in Section 2.6.
Information is not only an asset to businesses but also to home users. Home users may not be responsible for the protection of information of other people, but their own information should still be very valuable to them.

2.2.2 Vulnerability

A vulnerability is a weakness in security that can be exploited intentionally or by accident (Goguen et al., 2002, p. 15). If company machinery were at risk of being damaged, then 'not having a lock on the door' would be considered a vulnerability. If proper security is installed on the door, i.e. security lock, biometric scanners, etc, then that vulnerability would be removed.

A vulnerability may be exploited intentionally or by accident. Sometimes intruders from outside the company wish to cause harm to the company intentionally. However, if a company employee were to cause harm to the company, by accident, the effects may be just as devastating.

2.2.3 Threat

A threat is the intent, situation or method that causes a vulnerability to be triggered (Goguen et al., 2002, p. 12). Threats can include natural disasters, such as fire, flood or a lighting storm. It may include human error, such as improper use of machinery or vandalism. Threats can also be associated with computer systems when hackers, viruses and improper computer usage are involved.

2.2.4 Risk

A risk involves an asset to be potentially compromised by a threat through a vulnerability (von Solms & von Solms, 2008, p. 101). When these three factors come together, a risk can be identified.
Some risks have more potential to be harmful than others. Furthermore, no matter how much security is implemented, a certain degree of risk will always remain. Therefore, some form of assessment should take place for businesses to decide what risks to address, as discussed in Section 2.3.1. It is unrealistic to address each and every risk. Companies need to budget and assess what level of security is viable for them. Risks are addressed through controls.

![Diagram of components constituting a risk](image)

**Figure 2.1:** Components constituting a Risk - Adapted from von Solms & von Solms (2008, p101)

### 2.2.5 Controls

Risks can be mitigated by implementing *controls*. Controls, countermeasures or safeguards are the same concept that refers to policies, procedures, guidelines, practices or organisational structures to reduce the effects of risks (von Solms & von Solms, 2008, p. 101). For the purposes of this dissertation ‘controls’ will be used to refer to this concept. Controls are discussed further in Section 2.7.

The concepts discussed from Section 2.2.1 to Section 2.2.5 provide a basic description of security in general, as depicted by Figure 2.2. This dissertation focuses on information security and, therefore, these concepts should be viewed from an information security perspective.
Information security deals with information assets. Information assets are tangible or intangible forms of information which has value. Below are three examples, of risks, that highlight different ways in which information assets can be threatened.

Example 1: Workstations can be stolen from a company. The assets that would be compromised, in this case, would include the physical computer and the information it contains. However, the company could be more concerned about the information on the workstation, which is probably worth more to them than the computer. Therefore, the identified asset of this risk is the information on the workstation. The threat of this risk would be theft and the vulnerability would be a window without burglar proofing. Controls against this risk could be to burglar proof the window or to hire a security guard. Both these controls can eliminate the vulnerability of the risk and thereby preventing the risk from occurring.

Example 2: Emails can be intercepted by hackers. The asset that would be compromised would be communication in the form of emails. The threat of this risk would be that hackers can obtain communication. The vulnerability can be an insecure wireless section of the network. A control against this risk could be to encrypt emails before they are sent.

Example 3: Employee actions can compromise passwords. The asset that would be compromised would be employee passwords. The threat of this risk would be employee actions such as writing down their passwords on a piece of paper, or sharing their passwords with other individuals. The vulnerability, in this case, could be untrained employees. A suitable control for this risk would be to inform employees to keep their passwords secret.

<table>
<thead>
<tr>
<th>Example</th>
<th>Asset</th>
<th>Threat(s)</th>
<th>Vulnerability</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Workstations</td>
<td>Theft</td>
<td>Window</td>
<td>Burglar proofing</td>
</tr>
<tr>
<td>2</td>
<td>Emails</td>
<td>Interception</td>
<td>Wireless network</td>
<td>Encryption</td>
</tr>
<tr>
<td>3</td>
<td>Passwords</td>
<td>Writing down</td>
<td>Untrained staff</td>
<td>Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sharing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2.1: Summary of examples of risks
The above mentioned examples emphasise the fact that information security is applicable in many different situations, but they are essentially about protecting information. However, one can only protect information if one knows how to maintain information as an asset.

### 2.3 Information as an asset

Information can take many forms. One can think of information. One can write information down on a piece of paper. Or one can store information on digital media with a computer.
If information is important then it is also an asset, regardless of the format it is currently in. However, the value of information is lost when confidentiality, integrity or availability (CIA) are lost (Pfleeger & Pfleeger, 2003; Whitman & Mattord, 2003, p. 10; ISO 27002, 2005, p. 17; Tudor, 2006). The following sub-sections will discuss these factors individually.

### 2.3.1 Confidentiality

Confidentiality ensures that private information is **not** accessible to anyone who is not authorised to access it and that it is accessible to users who **are** authorised to access it (Whitman & Mattord, 2003, p. 11). People should not be able to view information that does not concern them. *Employees who discover that they are being underpaid, by viewing the payroll* is an old example of why confidentiality should be kept.

It could be even more important to ensure that persons outside the organisation do not view company information. Company secrets, for instance, should be kept a secret to maintain their competitive edge for that organisation.

### 2.3.2 Integrity

Integrity ensures that the information is, and remains, accurate. Therefore, humans need to store information on a computer correctly and that information should remain to be true. If any event causes accurate information to change into inaccurate information then that information has lost its integrity. Threats to the integrity of information can occur when the information is stored or transmitted (Whitman & Mattord, 2003, p. 13).

Inaccurate information is usually caused by human interference. It is humans who enter incorrect data into computer systems.
2.3.3 Availability

Availability ensures that the information is accessible to the people who need it, when they need it. It is completely useless to gather information if no-one can view it. Furthermore, information should be received fairly quickly after someone has been authorised to access it, without interference or obstruction (Whitman & Mattord, 2003, p. 10).

If confidentiality, integrity or availability is compromised then information has become less useful which means that an asset has decreased in value. Therefore, information assets need to be maintained by ensuring that confidentiality, integrity and availability are not compromised. This needs to be safeguarded by people depending on their situation. It is, therefore, necessary for these people to be aware of information security and how it relates to them.

2.4 Five dimensions of information security awareness

Many people are affected by information security and, therefore, need to be aware of it. Previous research has been done to determine who these people are and what they need to know. This study will not focus on all these types of people. However, it is necessary to examine many different perspectives in order to gain a broad understanding of information security.

Siponen (2001) has identified five different groups of people who should be aware of information security. Each of these groups is associated with an aspect of information security. Siponen (2001) identified these dimensions (as he names it) to indicate (among other things) that although information security is important for organisations it is becoming more of an issue for other people as well. These dimensions are:

- organisational;
- general public;
The following sections will briefly examine each of these dimensions in more depth.

### 2.4.1 The organisational dimension

It is generally acknowledged, over the last few years, that security awareness should be incorporated within the security strategies of organizations (Thompson & von Solms, 1998; Furnell & Gennatou & Dowland, 2000; Drevin & Kruger & Steyn, 2007; Kritzinger & Smith, 2008). The organisational dimension includes different categories of employees, such as: top management, IT management and end-users (Thompson & von Solms, 1998; Siponen, 2001). These different categories of employees may be made aware of different aspects of information security depending on what information they work with. For example, IT management should be aware that they are responsible for the creation of information security policies, while end-users should be aware of what information security policies they need to be concerned with.

### 2.4.2 The general public dimension

Information security problems affect organisations as well as individuals (Furnell & Ward, 2008). Furthermore, the security of an organisation is connected to the level of awareness of home users (Furnell & Bryant & Phippen, 2007). The general public dimension includes IT computer/IS professionals and other end-users (Siponen, 2001). These users need to be aware of risks that threaten their personal information. These may include threats of a non-technical nature, such as stolen identity document or credit card, or threats associated with the Internet, as discussed in Section 2.4.
2.4.3 The socio-political dimension

The socio-political dimension includes lawyers, public relations people, politicians and the government (Siponen, 2001). These people are responsible for the effects of information security on society. Therefore, they need to know how electronic services, legislation, ethical concerns and general public awareness of information security should be implemented (Siponen, 2001).

2.4.4 The computer ethical dimension

The Generally Accepted Information Security Principles (GAISP) document states that information security should be conducted while maintaining ethical standards (GAISP, 2004, p. 6). Scholars are entrusted with research ethics and information security norms in order to assist the other dimensions (Siponen, 2001). Therefore, they need to be aware of past and current developments in information security to conduct further research.

2.4.5 The institutional education dimension

The institutional education dimension seeks to educate students about information security in order to establish a secure culture among them (Siponen, 2001). All Internet users need education in order to protect themselves (Sukhai, 2004). People who teach computer systems need to know what information security content to convey to their students. They also need to be aware of the dangers associated with information security to be able to explain why the content is important.

This section emphasised the fact that different people need to know different aspects of information security. However, the organisational dimension is, arguably, the most researched dimension, perhaps because their awareness campaigns are not as successful as they should be (Puhakainen, 2006; Albrechtsen, 2007; Ernst & Young, 2009). Puhakainen (2006), Albrechtsen (2007) and Ernst & Young (2009) discuss awareness campaigns that businesses employed with their employees. However, there are several
other factors that businesses need to be aware of when addressing information security. The following section examines these factors.

2.5 Information Security from a business perspective

If a business does not address information security its reputation can be ruined (Ernst & Young, 2008) or it may even face bankruptcy (Monk & van Niekerk & von Solms, 2010). An organization should make their employees aware of information security as security techniques depend on awareness (Siponen, 2001). However, awareness is not always enough to protect assets of businesses to an acceptable level. Von Solms (2000) states that to manage information security properly an organisation should be able to measure its effectiveness while making use of best practices, international information security certifications and cultivating an information security culture. The following sub-sections will examine each of these topics as they should enhance the organisation's level of information security.

2.5.1 Risk management and measurement

Risk management is a continual process whereby businesses address risks (Ernst & Young, 2009). It has been identified as one of the top security aspects which organisations want to improve upon (Ernst & Young, 2009). It can be sub-divided into three processes: Risk assessment, risk mitigation and risk evaluation (Goguen & Stoneburner & Feringa, 2002). Organisations use risk assessment to identify the risks that they should address. Goguen et al. (2002, p. 24) identify three factors which should be taken into consideration when assessing risks:

1.) The likelihood that a threat would attempt to exploit a vulnerability;

2.) The magnitude of the impact should a threat successfully exploit a vulnerability;

3.) The adequacy of security controls aimed at reducing the risk.
Risk assessment should reveal what the most threatening risks are, which will be the risks that need to be addressed more urgently.

The second process, risk mitigation, involves prioritising and implementing security controls to mitigate the risks that were identified. Finally, risk evaluation ensures that as computer systems change, and consequently the risks involved, controls are updated to handle them. Businesses must constantly be on the lookout for new risks. Therefore, the risk management processes should be cycled through continuously as illustrated by Figure 2.4.

![Risk Management Process Diagram](image)

**Figure 2.3:** Information Security Risk Management Process as Described by Goguen et al (2002)

While managing risks, businesses should be aware that weak controls may lead to them being negligent towards the information of their customers, which is a criminal offence. In this instance, the court could rule that the organisation did not protect the information
of their customers correctly, and, therefore was negligent towards it. Other legal and regulatory issues regarding information security have emerged during the last couple of years (von Solms, 2006), such as the Electronic Communications Act of South Africa. Therefore, legal implications should be considered when initiating security controls. Suitable controls can be created with the help of best practice documents, which is the second topic that businesses need to be aware of.

2.5.2 Best practices and international certifications

Two well known best practice guidelines which relates to information security are COBIT (COBIT, 2007) and ISO 27002 (ISO 27002, 2005). ISO 27002 is an international best practice (von Solms & von Solms, 2008, p. 39). It provides detailed information on how information security controls should be implemented. On the other hand, Control Objectives for Information and Related Technology (COBIT) provides guidelines for information technology in general. Therefore, ISO 27002 is more specifically aimed at security than COBIT. However, COBIT and ISO 27002 can be used in conjunction, which will provide more guidance to businesses than using them separately (von Solms & von Solms, 2008, p. 49).

A best practice should have a certification attached to it for businesses to be able to prove to each other that their information is secure and, therefore, security concerns should not be raised when certified businesses work together (von Solms, 2000). ISO 27001 is an internationally recognized standard that organisations can comply with in order to achieve certification. ISO 27001 is the certification attached to the ISO 27002 best practices (von Solms & von Solms, 2008, p. 48). Through best practices management of businesses should become knowledgeable on how their employees are supposed to implement security. However, employees may be against security processes although the business is certified. One method to improve employees’ perceptions on information security is to incorporate an information security culture.
2.5.3 Information security culture

An organisation should seek to implement a security culture among its employees in order to highlight the importance of controls. Corporate culture can be defined as: “the beliefs and values shared by people in an organisation” (Smit et al., 2007). It can be broken down into three levels: Artefact, espoused values and shared tacit assumptions (Schein, 1999). Artefact level constitutes everything that is real or can be sensed (see, hear, smell, touch and taste). Espoused values are “official” beliefs of the company, which is usually documented in some way. It also explains what the roles of the artefacts in a company are. Shared tacit assumptions are beliefs and values of employees (van Niekerk & von Solms, 2010) of the business and have less of an influence as one employee’s view would not affect the other employees. The three levels of corporate culture can be viewed as moving from more real and influential to less provable and secretive.

If the workforce of an organisation adopts a good information security culture then the chances that the employees would correctly use security controls should increase (van Niekerk & von Solms, 2010). A ‘good’ information security culture would mean that education is at a suitable level and a general belief that security is important would exist among employees. Therefore, information security education plays a role in the development of an information security culture (Siponen, 2001).

2.5.4 Employee education

All employees should be educated about information security to be able to understand and implement controls (Siponen 2001, ISO 27002, 2005). It is the business’s responsibility to ensure that its employees are properly educated to perform work related tasks. However, employees are often not educated enough to perform security oriented tasks (Siponen, 2000; van Niekerk & von Solms, 2006; Furnell et al., 2007; Stephanou & Dagada, 2008). Furthermore, even if employees are educated about information security they might not adhere to procedures due to a lack of motivation (Siponen, 2000) or other reasons (Albrechtsen, 2007). Information security education will be dealt with comprehensively in Chapter 3.
Despite having many options available to them organisations find it difficult to make their employees aware of information security. This is not only a problem in organisations but also for the general public dimension, discussed in section 2.2.2, which may be even more difficult to spread awareness to (Furnell & Jusoh & Katsabas, 2006; Funell & Tsaganidi & Phippen, 2008).

### 2.6 Information Security in the larger social context

Home Internet users are in a different situation than employees of businesses because they are not necessarily tied to an organisation which is responsible for their competence. Some home users are unaware of the issues surrounding information security while others choose to ignore these issues (Siponen, 2001). Siponen (2001) states that general knowledge of information security needs to be enhanced, in order to address the dangers that the Internet poses. The Internet can endanger the information, wealth, hardware and software of users.

The Internet is used for different reasons. These reasons can be grouped into different internet services:

- Government;
- Entertainment;
- Social networking;
- Finance;
- Education.

This is not a complete list of services rendered by the Internet. However, they should indicate different types of information transferred over the Internet. The following sub-sections will explain how each of these is used, the information that is required by them
and how these services attempt to educate their users to protect the supplied information.

2.6.1 Government

Online government services, or e-government, may require users to supply some of their information. This information is likely to include data that can be linked to the identity of the user, because the government attempts to verify that the user is who he states he is. Ironically, if another Internet user intercepts his information then that user can use the information to impersonate the legitimate user and commit other acts of fraud. The information that government services require may also include banking. If this information is intercepted then an illegitimate user can gain access to money that does not belong to him. Tax and visas are two examples of services that require users to enter these types of information over the Internet.

The South African Revenue Service (SARS) provides a tax service named ‘eFilling’. SARS encourages taxpayers to use eFilling to submit their tax details online. eFilling requires users to enter identification information, bank account details and financial information. All of this information can be threatened by phishing attacks (explained in Chapter 6). SARS have already identified fifteen phishing attacks (South African Revenue Service, 2010), which attempted to rob users of the above mentioned information. Details about these attacks can be obtained from the SARS website. However, SARS does not educate users about information security before they start using eFilling.

Another example of a government service is providing visas. A visa is the document that enables people to visit other countries. When a person applies for a visa to visit the United Kingdom, for example, he/she needs to apply for it online, which requires a large amount of personal information. These include identification information about themselves and relatives, contact information, such as email address and contact numbers, and credit card numbers if payments are processed online. This website which enables South Africans to apply for a visa for the United Kingdom does not provide any information which would help users to secure their information.
2.6.2 Entertainment

Various forms of entertainment might require users to enter information over the Internet. Many entertainment oriented websites requires users to register, which may require users to submit their email address. If a user supplies his email address to an untrustworthy website he is likely to receive email attacks. Entertainment websites may require payment from the user, in which case, bank details of the user need to be provided. Many of these websites do not protect their users from information security risks sufficiently. The website of Look and listen (www.lookandlisten.co.za), a popular South African media store, is one example of this. To date the website seems to have no visible link to a page that advises the users on security concepts. Furthermore, no information on security is presented before online payment is processed.

Another example of a service that requires information is online games. Online games are increasingly popular activities on the Internet. Some online games do exist that attempt to educate their players on how to secure their information. One example of an online game that does this is Runescape, the popular MMORPG (Massively Multiplayer Online Role Playing Game). The players of Runescape are free to choose whether they want to receive this education. Without choosing to obtain education, players of Runescape will not receive information security training through the game (Runescape, online).

Entertainment websites are associated with harmful programs that may threaten the information of home users. These programs may include viruses, spyware and keyloggers.

2.6.3 Social networking

Social networking can be described as building and maintaining contact with people over the Internet. This activity has been gaining popularity during the last few years. The most popular social networking website, Facebook, has over 500 million registered users (Zuckerberg, 2010), which is approximately a fourteenth of the population of the human
race. Websites such as Facebook provides functionality of sharing information with other users. Any information that a user wishes to share may be placed on Facebook.

Once information is uploaded to Facebook it is potentially accessible to many users. Users who seek to steal information may login to Facebook just as easily as regular users. Facebook provides users with security settings to make their information inaccessible to hackers. However, a large amount of users do not use these settings. Social networking users are often unaware that the information they are sharing may incur risks.

2.6.4 Finance and e-commerce

A large amount of individuals (and businesses) use the Internet for Internet banking, e-commerce and other financial services. Banks provide internationally recognised credit cards (such as Visa and Mastercard) for their customers to buy goods and services online. Credit card numbers may be at risk when users use these services. If a credit card number of a user is compromised then his or her money may be stolen.

It is in the interest of the banks to educate their customers about securing information. Most banks provide educational content about information security on their website. Banks make use of ‘text messages’ and other communication services to warn their customers about potential risks. However, by doing so, the bank may lose a lot of time and money. Some customers fall victim to threats even when banks employ these techniques.

E-commerce websites are known to store user data as cookies. Cookies are small files stored on a PC that records browsing information. Although these files are not stolen by the e-commerce website, the information in the files is in an unsafe format. The use of cookies can be disabled by home users although many of them do not know how to do this.
2.6.5 Education

Internet users may use the information super highway to obtain education in various fields. Many courses make use of the Internet for students to read online educational material and take online courses.

Again, identification details, contact information and financial information may be required to use these services. Students should be careful with their information, but they are often unable to do so because they are not educated by these services.

It becomes difficult for home users to use the Internet, by any means, without supplying some personal information. Programs such as viruses, spyware and keyloggers as well as cookies that threaten information, exist on the Internet. Users remain responsible for their own information and cannot depend on an external organisation to educate them. Therefore, some form of education should be focused on home users, preferably before they provide their sensitive information over the Internet. Siponen (2001) states that information security awareness should form part of the general knowledge or home users.

The last two sections discussed the organisational and general public dimensions identified by Siponen (2001) and argued why people need to be aware of information security. However, awareness alone is not enough (Grant, 2000; Schlieger & Teufel, 2003; Pfleeger & Pfleeger, 2003; van Niekerk & von Solms 2004; Furnell et al., 2007). The people associated with these two dimensions need to be educated about information security. It should be noted that these dimensions deal with the victims of information security threats and that it is difficult to educate them (discussed in the next chapter). It can be argued that the institutional education dimension also deals with potential victims of information security threats. However, the main focus of the institutional education dimension is on the educators. Therefore, the focus of this study will be aimed at the ‘victims’ of information security, which can also be described as those who need education. Education is vital to ensure that information remains as an asset by implementing security controls. A security control is not something that should be implemented once. It needs to be implemented in everyday processes.
2.7 Information security as a process

Security should be maintained though a continual process that includes implementing controls. The use of controls mitigates threats that cause information to lose confidentiality, integrity or availability. Controls can be broken down into physical, technical and operational controls (van Niekerk & von Solms, 2006).

2.7.1 Physical controls

Physical controls protect businesses against threats by using physical security measures. *A lock on the door or movement sensors* would be examples of physical controls. Example 1 discussed in Section 2.2 mentions *hiring a security guard* and *burglar proofing* as two other examples of physical controls.

Information security is often associated with controls that safeguard information from the dangers of the Internet. However, all the information gained by websites is stored on computers. Therefore, if no physical measure exists that inhibits someone from physically stealing those computers then the information would be under a great amount of risk. Electronic information can be stolen physically, only if a thief gains access to the physical medium that stores the information. Therefore, physical controls are essential to information security.

2.7.2 Technical controls

Technical controls resolve vulnerabilities that are technology related. They involve all the tactical and technical issues relating to security and address the selection of suitable technology (Whitman & Mattord, 2003, p. 222). *‘Forcing users to authenticate themselves before accessing something’* is an example of a technical control. Example 2 discussed in Section 2.2 mentions *password encryption* as another example of a technical control.
When information is stored electronically more security is needed because physical **and** technical controls should be implemented. Therefore, businesses should determine whether they can afford to convert their physical information into electronic information before they make the final decision.

Technical controls are usually forced upon users to ensure that they perform their tasks securely. Forcing users to perform technical controls takes away the choice of the users, which eliminates human error. Therefore, technical controls are more likely to be effective than *operational controls* (Goguen et al., 2002, p. 32).

### 2.7.3 Operational controls

Operational controls protect businesses against threats that may occur due to human behaviour, either intentionally or by accident. ‘**Not** downloading and installing software from the Internet’ can be a business rule which would also be an operational control. Example 3 discussed in Section 2.2 mentions *password education* as another example of an operational control.

Operational controls are more difficult to control than physical and technical controls. The users of the system are the main source of information security breaches (Schneier, 2000; Mitnick & Simon, 2002, Whitman & Mattord, 2003, p. 17; Ernst & Young, 2008; Deloitte, 2009) and remain to be the weakest link in the security chain. To a large extent, physical and technical controls rely on the implementation of operational controls (van Niekerk & von Solms, 2006; Stephanou & Dagada, 2008). When a technical control forces users to use a secure password, for example, users are likely to write it down on a piece of paper, which is not secure behaviour. Therefore, companies should manage their operational controls carefully. This dissertation focuses on the dangers that users pose on information security, which in a business environment is about implementing and maintaining operational controls. Therefore, this study supports the notion that the behaviour of users (the victims of information security threats) can be altered to perform controls successfully if they receive the proper education and motivation to do so.
2.8 Conclusion

Information security is about preventing risks. A risk consists of a threat, vulnerability and an asset. Risks can be mitigated by using controls. People need to be educated in order for them to be able to implement these controls. However, information security is a process that needs to be maintained. Therefore, people should also be continually motivated to implement the controls that they have learnt.

Different roles that people have regarding information security in society were identified. The roles most applicable to this study were the organisational and general public dimensions. The organisational dimension has been researched the most. However, there exists no definitive solution to make employees adhere to operational controls. The general public dimension, on the other hand, has not been researched as much. People in the general public dimension are very vulnerable to information security threats.

In conclusion, people need to be educated in order to protect their information assets that are stored on computer systems as awareness, alone, is not enough to alter the behaviour of users. However, educating people about information security as well as motivating them to act securely is a very difficult task. The next chapter will discuss education, in general, and will narrow its focus on information security education.
Chapter 3: Information Security Education

3.1 Introduction

The previous chapter identified the lack of education as a primary factor that causes information security problems. This chapter focuses on the concepts around information security education and what methods are used to convey such knowledge.

The fundamental education models are discussed to determine how different education programs may be implemented to address information security. Each model has its own strengths and weaknesses. Therefore, some analysis is needed to determine which of the models will suit information security education. Within these models steps can be followed that would teach learners about information security more effectively.

Nurturing learners to the point where they are security efficient is a multi-step process. An educator must understand the steps involved with information security education and how each step plays a part in the bigger picture. These steps can be implemented by using various methods.

Therefore, effective implementation methods need to be identified with regard to information security education. These methods may change as learners become more knowledgeable about the field of study. This chapter discusses these methods as design criteria, which can be implemented in an education program to teach learners about information security.

It should be noted that, for the duration of this chapter, 'learners' refers to any person that could benefit from gaining knowledge about information security. This would include employed and unemployed persons, home users, as well as people from all age groups.

The next section examines the fundamental models used to convey information to learners.
3.2 Models of learning

In order to produce an education program it is necessary to examine the most popular learning/teaching paradigms to evaluate which one is the most appropriate for program success. Leidner & Jarvenpaa (1995) discuss objectivism, constructivism, collaborativism, cognitive information processing and socio-culturalism as widely accepted models of learning. Objectivism and constructivism are at opposite ends of the philosophical continuum (Vrasidas, 2000) with socio-culturalism situated somewhere in between (Leidner & Jarvenpaa, 1995). Collaborativism and cognitive information processing are deviations from constructivism. Each of these educational models will be briefly examined in more depth.

![The Philosophical Continuum](image)

Figure 3.1: The location of the learning models along the philosophical continuum

3.2.1 Objectivism

All five of the learning models discussed in these sub-sections are based on how the human mind perceives things. The mind can perceive reality as an absolute truth where
only one reality exists. An object is simply what it is, nothing more, and nothing less. The opinion of objectivists is that truth lies within the world that people live in.

Objectivism (the traditional model of learning) is the most popular model for organised teaching courses. In objectivism teachers are knowledgeable experts, in the field of study, and their goal is to convey their knowledge to their learners who do not have as much knowledge as they have. The learners receive the course material as the teacher expresses it. Therefore, they are subject to one (absolute) point of view (Vrasidas, 2000). If the learner does not understand the study content it is due to ineffective communication. Very little communication is necessary from the learners as the teacher decides how and what content is taught. Therefore, objectivism makes four assumptions (Leidner & Jarvenpaa, 1995):

- There exists a reality that individuals agree upon;
- The reality can be transferred to a learner;
- The mind should act as a mirror of reality instead of an interpreter thereof;
- All learners use the same process in order to understand reality.

By attending an objectivism oriented course a learner receives only one perspective of the study content. Furthermore, the learner is discouraged from interpreting information. Therefore, only the information the teacher expresses is conveyed in the classroom. No new information is created.

*How the teacher expresses content* is crucial to the success of an objectivistic course. Therefore, teachers must communicate accurately, use visual representation and evaluate the learners to make sure that they understand the course material.

Evaluating the learners can be done by continuous assessments created by the teacher. How well the learners complete the assessments will determine whether they have attained the knowledge that the teacher conveyed to them. On the other side of the philosophical continuum lies constructivism.
3.2.2 Constructivism

Unlike objectivism, constructivism views reality from different perspectives with many different truths (Vrasidas, 2000). There does not exist a reality outside of the human mind, the human mind constructs its own representation of reality. Therefore, every person has a unique perspective on reality. According to constructivism theory truth exists within the human mind.

Constructivist courses are learner-centred as the learner decides how and what material needs to be covered. Learners are encouraged to discover new knowledge by themselves, which results in them having their own opinions about it (Leidner & Jarvenpaa, 1995). Furthermore, when a learner discovers knowledge by him/herself he/she gains a sense of pride that would not be attained if the teacher simply told him/her the knowledge. As a result, the knowledge is more memorable. Knowledge of the learners may change regularly as they make new discoveries.

Learners decide what material they want to cover and how quickly they go through it. They determine whether they understand a concept enough in order to proceed to the next topic. As constructivism supports some learners to work more quickly than others, learners in the same class can be ahead of others. Learners may also choose to work on different topics from their class mates.

A good example of a constructivism classroom was presented in the first episode of The Simpsons, which has titled: ‘Bart the genius’. Bart, the well known trouble making boy of the Simpson family, switches his IQ test with the cleverest student in his class. After attaining a very good IQ score Bart is transferred to a school for the gifted. At this school, Bart’s class ‘coordinator’ tells him that at this school the learners can make their own rules. “If you want to take a nap take one”. “If you are bored you can sit and read a book”. He is responsible for learning as much as he wants in whatever field he chooses.

As in The Simpsons the teacher takes a coordinator role in real scenarios. He makes sure that the learners are in an environment where they can make their discoveries forming a type of partnership with the learner. Dissimilar to The Simpsons, it is unlikely for primary school children to receive this type of education mainly because assessment
cannot be taken. School classes may take a constructivism approach by predetermining what knowledge the students should learn. However, this is not a ‘pure’ constructivist implementation (Leidner & Jarvenpaa, 1995). Masters (or doctorate) students writing a dissertation (or thesis) is a better example of a constructivistic education strategy.

One of the shortcomings of constructivism is that it limits a learner from interacting with its peers. Collaborativism is the model that seeks to bridge this gap.

### 3.2.3 Collaborativism

Collaborativism is a deviation from constructivism as many of the same principles apply to both. The difference of collaborativism is that it focuses on learner interaction. As a learner creates his/her own interpretation of knowledge he/she also receives multiple interpretations of the same knowledge from his/her peers. Therefore, the knowledge of the learner may change when new perspectives of the knowledge are introduced to him/her. Furthermore, learners tend to understand concepts more clearly when they explain it to other people. Therefore, a learner benefits from the participation of the other members in the group as well as their own participation.

Leidner & Jarvenpaa (1995) identifies four assumptions of collaborativism:

- **“Knowledge is created as it is shared, and the more it is shared, the more is learned”;**
- **“Learners have prior knowledge they can contribute to the discussion”;**
- **“Participation is critical to learning”;**
- **“Learners will participate if given optimal conditions such as small groups to work with”.**

The learners need some prior knowledge of the discussed topic for collaborativism to be viable. If the learners do not have their own opinion about the information then they will
simply repeat the point of view that the teacher explained. Multiple perspectives need to be communicated for learners to gain a shared understanding of concepts.

To reach a shared understanding of concepts, listening and communication skills of the learner are very important. By sharing information in a group learners should develop their own listening and communication skills more quickly (Hardless & Nulden, 1999). However, some learners do not have the necessary skills to benefit from group activities. Other learners may not be motivated enough to share their perspectives on the course material. The teacher may need to motivate these learners to become more active in their groups. However, if the teacher forces the learner to share his/her thoughts it could frustrate the learner to the point where he/she refrains from any group participation. This scenario would leave the learner as well as the teacher frustrated.

The teachers are responsible for providing optimal conditions for the learners to participate. Their responsibility shifts from a coordinator to a facilitator of shared knowledge. They should ensure that conditions are appropriate for learners to share information. The teacher should provide feedback to the learners, and concurrently learners should provide feedback to the teacher. Finally, the teachers should assess the learners by using a cooperative method, because learners are denied to learn from their peers if they are assessed separately. Collaborativism is not the only example of a learning model which stems from constructivism.

### 3.2.4 Cognitive information processing

Cognitive information processing is another deviation from constructivism. The aim of cognitive information processing is for learners to store knowledge in long-term memory. In order for learners to gain long-term memory the knowledge must move through three stages, namely: sensory, short-term, and long-term (Reiser & Dempsey, 2007).

Learners become aware of external objects or concepts through their five senses (hear, see, smell, touch and taste). After they become aware of a concept it can be stored in their short-term memory. Concepts that are stored in short-term memory can be
retrieved by the learner, but can also be forgotten. Therefore, the learner needs to be constantly reminded of the concept until it is committed to long-term memory. Concepts in long-term memory are less prone to be forgotten by the learner. Cognitive information processing seeks to produce learners who have committed the study content to the extent where they can effectively and reliably retrieve it.

Cognitive information processing assumes that learners have preferred learning styles (Leidner & Jarvenpaa, 1995). This means that learners should be treated and taught as individuals with individual needs. Learners in the same class may take different routes to commit the study content into long-term memory. Therefore, feedback from the teacher is very important as the learners have unique preferences. Furthermore, the learners need to be reminded constantly of what the correct information is. Prior knowledge that the learner has of the study content may affect how effectively they process new information (Leidner & Jarvenpaa, 1995).

Attention is a key concept in cognitive information processing. As learners may have short attention spans they tend to focus their attention selectively. Through selective attention learners are more prone to remember concepts on which the teacher places emphasis. This can be done by making use of graphics and highlighting words in text (Reiser & Dempsey, 2007).

### 3.2.5 Socio-culturalism

Socio-culturalism agrees and disagrees on the concepts of both objectivism and constructivism. In socio-culturalism truth lies with a human’s mind, body, history and surroundings. A person should refrain from following society but instead, a person is motivated to change society through his/her experience.

Learning according to socio-culturalism focuses on the organisational culture of the learner (Soloway et al., 1996). The organisational culture of each learner should be taken in consideration for them to be taught, because study content needs to be in context. If the study content is rooted in the culture of the learner then he/she should be able to grasp it more quickly.
Socio-culturalists argue that constructivism and collaborativism are biased because they reject the understanding derived by the minority cultures (Leidner & Jarvenpaa, 1995). Cultural and social factors of the majority of the learners overshadow the opinions of the minority in the group, which takes away their perspective on society. Similar to constructivism, socio-culturalism assumes that learners should have their own perspective of the truth. However, the truth of one learner should not be moulded into the truth of another learner or teacher.

<table>
<thead>
<tr>
<th>Learning is</th>
<th>Realism of Context</th>
<th></th>
<th>Control of the Learning Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation of Knowledge by Student</td>
<td>Low</td>
<td>High</td>
<td>Learner</td>
</tr>
<tr>
<td>Sharing of Knowledge</td>
<td></td>
<td></td>
<td>Peer Group</td>
</tr>
<tr>
<td>Dissemination of Knowledge by Instructor</td>
<td></td>
<td></td>
<td>Instructor</td>
</tr>
<tr>
<td>Abstraction</td>
<td>Low</td>
<td>High</td>
<td>Personally Experienced</td>
</tr>
<tr>
<td>Knowledge is</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3.2: The Dimensions of the Learning Theories - Adapted from Leidner & Jarvenpaa (1995)

This section described the fundamental teaching models and their strengths and weaknesses. The next section discusses how they should be used for an education program that teaches information security.

37
3.3 How the models of learning affect information security education

The five models of learning discussed in the previous section should be taken in consideration when an educational program for information security is developed. Each of the models of learning poses problems when it is used to formulate an information security course.

- Objectivism may fail to provide the learners with practical understanding and the necessary motivation to learn information security. This is usually in the form of lectures and reading material, which have these weaknesses. People are generally not motivated to attend lectures or read educational material on information security (Monk et al., 2010).

- Constructivism deals with various perceptions which may not relate well with information security. The aim is not to teach learners to be experts on information security to the point where they may create their own opinion on how to solve problems. The aim of the desired program is to provide learners with enough information to handle a security situation in an appropriate manner.

- Collaborativism provides people with an opportunity to communicate about information security. However, new knowledge cannot be attained if people, in general, do not have a sufficient understanding of information security. Similar to the previous point, the program needs to facilitate learners who do not know a lot about information security.

- Cognitive information processing may not succeed to transfer knowledge to long-term memory, because people are generally not motivated to learn about information security (Monk et al., 2010).

- Socio-culturalism may be too difficult to implement as a single course that will fit each and every culture of the students. It can be argued that the organisational culture of learners is more or less the same.
Therefore, instead of selecting one of these models this section will discuss the concepts that the models present which may benefit information security education.

As information security is external from the human mind and there is generally one correct way of implementing controls, it could be argued that information security suits the objectivistic perception of the truth. On the other hand, learners could understand information security concepts better if they discovered them by themselves (constructivism) or if they reached conclusions about it by communicating with someone else (collaborativism). However, information security is not just about understanding concepts; it is also about implementing controls practically. Practical experience is attained from repeated practice and can be developed more easily by making use of the preferred learning style of the learner (both of these are cognitive information processing concepts). It is also very important to motivate a learner of information security (another concept of cognitive information processing). Finally, the organisational culture of the learner could be addressed (socio-culturalism) by the program.

Before discussing what educational model this study will follow, this chapter examines how current education programs for information security are formulated. By analysing how information security programs are formulated, as well as the weaknesses thereof, a set of criteria can be created which should enhance their chances of success.

3.4 Awareness, training and education

The National Institute of Standards and Technology (NIST) released a document that specifies how learners should be educated on information security. This document is NIST 800-16 (1998) and it describes learning as a continuum, whereby learners progress through three levels in order to obtain education. Many education programs that teach information security are designed according with the specifications of NIST 800-16 (Whitman & Mattord, 2003, p. 222). These three levels are: awareness, training and education.

Note that this dissertation uses the term ‘education’ as the entire process that a learner goes through to obtain the information they need to become knowledgeable in the
concepts of information security. ‘Education as part of the continuum' will be expressed as such to avoid any confusion.

The three levels of the continuum teach the learners about different aspects of information security.

### 3.4.1 Awareness

In order to learn more about a certain concept one must be aware of its existence. Once a learner has an understanding of a concept the ideas around it can be learnt more easily. However, if a concept is misunderstood it would be difficult to learn more about it. Awareness is often used to introduce a topic/concept to a group of people who have no previous experience with it.

The goal of awareness programs on information security is to make people pay attention to it (NIST 800-16, 1998, p. 15). These programs often discuss the threats involved to gain the attention of people. These people might not be familiar with the term ‘information security', but they should be informed about threats that could affect them.

Awareness can also be used as a reminder to persons who are educated about information security to follow organisational policies and procedures (ISO 27002, 2005, p. 25). A good example of this is when a company notices an increasing amount of virus problems which they address by sending emails to their employees reminding them to update and use their anti-virus programs. Videos, newsletters and posters are other examples of how to spread awareness (Whitman & Mattord, 2003, p. 223; NIST 800-16, 1998, p. 15).

### 3.4.2 Training

Training requires learners to take an active role when being taught (ISO 27002, 2005, p. 25). When learners have become aware of a topic they can begin to learn how to deal with it practically. A group of people should receive training to know what they can or cannot do with regards to computer systems. Learning about computer systems often
requires some degree of training because computer systems are often operated by people.

When people receive training about information security they should be taught the necessary skills and competency with regards to computer systems (NIST 800-16, 1998, p. 16). However, people use information systems in various ways. Therefore, all learners do not need to be taught about information security to the same degree. Persons who work with computers everyday should most likely be taught more than persons who use computers once every month. However, it is still possible to formulate a baseline of training topics that each learner would benefit from.

### 3.4.3 Education

Once learners are familiar with a concept, and have practical experience with it, it becomes much easier for them to understand the deeper meaning behind their newly acquired skills. However, it is difficult for students to reach a deeper understanding of concepts.

Education sets out to teach learners why they need to implement information security processes. Persons are more motivated to do things when they know the reason behind it. Motivation is an important subject of security, because people, generally, have a negative perspective on it (Monk et al., 2010). Once learners understand the importance of securing information they are more likely to mitigate risks.

NIST 800-16 (1998, p. 17) views education, in the continuum, differently from training because of its exploratory nature. Therefore, they perceive education to be practiced primarily by security experts. The view of this study is that when a learner receives education they understand why they are trained to mitigate threats, which is similar to the view of Whitman & Mattord (2003, p. 223). By following this view, education is required for all learners, not just experts. Another option is to train students to such an extent that they would implement security controls without concentrating on it.
3.5 Education to reach unconscious competence

After learners have been through the continuum it would benefit them greatly to reach *unconscious competency* with regard to information security. ‘Unconscious competent’ is the term used to describe when people start to perform tasks automatically, without the need to think about it.

When one starts driving cars one needs to concentrate on what one is doing all of the time, but after a while it becomes much easier and only a small amount of thought needs to be spent on it. Being unconsciously competent with regard to security tasks is a very good level of practice to achieve. Staying with cars as an example, many people put on their seatbelts while not thinking about it because they are unconsciously competent with regard to car safety. Many educators would like their students to reach unconscious competency to perform tasks. However, in order to reach unconscious competency one must perform a task repetitively until one no longer needs to think about how one performs it.

Unconscious competence is suited for security oriented practices, because people no longer need to focus on security tasks. A person who reaches unconscious competence can also perform complex tasks without really thinking about it.

Howell (1982) identifies three stages that lead up to being unconsciously competent.

3.5.1 Unconscious incompetence

The first stage is when learners do not know about the tasks which need to be performed and, therefore, do not think about how they should perform those tasks. It is called ‘unconscious incompetence’ because they do not think about the tasks (unconscious) and they cannot perform the tasks (incompetence). In the continuum learners will be at this stage before awareness has taken place.
3.5.2 Conscious incompetence

The second stage is when the learner knows that they should perform certain tasks, but they are unable to perform them. This stage is called ‘Conscious incompetence’ and learners should reach this stage after awareness has been taught.

3.5.3 Conscious competence

After learners have received training and education about tasks they are now able to think about the tasks that they are able to perform. ‘Conscious competence’ is a good stage for learners to reach. However, reaching this stage is not ideal for security related tasks.

3.5.4 Unconscious competence

The final stage that learners can advance to is being ‘unconsciously competent’ when performing tasks. Ironically, learners revert to a stage where they no longer need to think about the tasks they are performing. However, this stage is more sought after than conscious competency because less time is wasted and learners tend to perform tasks automatically (Thomson & von Solms, 2006). Therefore, this stage is more ideal for security related tasks.

Furnell & Thomson (2009) introduces eight levels that determine how compliant users are in terms of information security. These eight levels are: disobedience, resistance, apathy, ignorance, awareness, obedience, commitment and culture. There is not a clear link between these levels and the stages of competency. However, these levels provide a way of classifying users by their behaviour, which can then be used to determine at what level they need to be educated.

The stages of competence have been related to information security with the aim to teach employees to behave securely in a more natural manner (Thomson & von Solms, 2006). It can be argued that NIST's continuum solves different problems of information security education than the stages of competency. Therefore, the following section examines
some of the most important problems with information security education that this study focuses on.

3.6 Problems of current education methods

Unconscious competence may be reached after training has occurred. Training is a level of the continuum which many organisations use to educate their staff (Whitman & Mattord, 2003, p. 223). However, information security programs are not always successful. It is, therefore, necessary to examine the problems identified with creating an information security program in order to overcome them.

3.6.1 Motivation

Motivation is a key concept when teaching learners about information security and it is often not taken seriously enough (Siponen, 2000). If the learners identify the benefits of attaining the knowledge they are being taught, then they are happy to learn about it. Conversely, if the learners do not see how the educational content would benefit them, then they will be irritated when education is forced upon them.

Employees are often not motivated to attend information security seminars or view educational online material. Information security is viewed, by many, as a boring topic to study. Therefore, better motivational techniques should be implemented by educational programs on information security.

3.6.2 Time and money

Businesses have the option to pay for their employees to receive education during business hours. However, many businesses do not have the time and money available for this type of education. This is especially true for small businesses (Furnell & Gennatou & Dowland, 2000).
It is necessary that every employee within the organisation should be educated about information security (ISO 27002, 2005, p. 25). Therefore, ample amounts of time and money may be necessary for an organisation to become adequately secure.

3.6.3 Facilitates one form of learning

Many information security programs only provide a single form of learning. The problem with this is that adults are already adapted to their own style of learning (NIST, 1998, p. 20).

For example, someone in the company might come from a very technical background. He has learnt all his skills from people who verbally explained the machinery, or by viewing how people work with the machinery and from personal experience. If this person is given a book to read about information security it would not be expected of him to learn as much as he would from someone showing him how to perform these tasks and explaining them to him.

If an educational program supports different styles of learning, the chance of that program supporting the learning style of every participant increases. Therefore, educational programs aimed at adults must try to implement multiple learning styles.

3.6.4 General public education

General knowledge about information security needs to be increased for the public to become more aware of the dangers it involves (Siponen, 2001). Methods of spreading public awareness of information security do exist, for example, radio programs and television talk shows. However, it is very difficult to create an educational program that will teach the general public about information security.

If the general public knew how to protect their electronic information then businesses would not need to additionally educate their employees. It is not easy to enhance general knowledge on certain topics. However, it is a factor that influences information security and many home Internet users suffer from information security threats.
By following the criteria listed above, an educational program that is highly motivational, facilitates different forms of learning, is fairly cheap and can be spread to the general public should hopefully be a successful one. In order to meet the above criteria the designer of the educational program on information security would have to consider the target audience of the program.

### 3.7 Identifying target audience

It is important for every employee in the organisation, who works on a computer, to be educated about information security (ISO 27002, 2005, p. 25). It would also be beneficial for the general public to gain knowledge about information security (Siponen, 2001). *Home users* are more difficult to educate because employees can be bound, contractually, to learn educational content.

Age groups are an important factor to consider when identifying a target audience. Employees are most likely adults while home users could range from a younger audience to an older one. A big problem with educating adults is that they are already set on a style of learning that they are familiar with (NIST, 1998, p. 20). Younger audiences, on the other hand, should not be educated through material that is too complex. To summarise the target audience should be aimed at:

- Employees of companies;
- The computer using public in general;
- People from most age groups.

An educational program that teaches employees as well as home users from most age groups would be the most ideal for the purposes of this dissertation. Now that a target audience has been established it is possible to determine how an education program on information security should be created.
3.8 Education in the business and larger social context

This chapter has reviewed several factors that should be considered when an educational program, focused on information security, is being designed. This section presents a set of criteria for this type of program that meets the requirements of information security education while solving the problems that have been identified in Section 3.6. Some of the criteria were determined by related research while others were determined by this research project. The criteria are discussed in the following sub-sections.

3.8.1 Target audience should be able to understand the content

By being involved with the program the target audience should be educated enough to be able to understand the educational content. The target audience identified ranges from young to old and employees from throughout company departments. However, it is not enough to present this content to the audience, the entire audience needs to be able to understand the content. Understanding is reached through the education stage of the continuum. Most education courses allow a percentage of learners to fail (van Niekerk & von Solms, 2006). However, this should not be the case for an information security course.

It has been proven that employees are more likely to perform tasks if they understand why they need to perform them (Schlienger & Teufel, 2003). This further emphasises the role that understanding plays with regard to information security.

Learners should be educated after they attend the program, which is a concept derived from objectivism. However, this does not mean that the program should only be attended by the learners once.

3.8.2 Learning repetitively

Unconscious competence can only be reached when the learner performs tasks repeatedly. It would benefit the learners to reach unconscious competence before they are faced with the dangers of the Internet. Therefore, if an information security program
could be used to reach unconscious competence then the learners should handle risks better.

It is difficult to create an educational program about security that incorporates recursion. Again, motivation plays a big role in accomplishing this. Learners will not be motivated to attend the same security workshop ten or twenty times. The educational program should therefore propose a method that would motivate learners to go through it multiple times. Motivation and repetitive learning are concepts from cognitive information processing.

### 3.8.3 Practical teaching

Whitman & Mattord (2003, p. 223) states that training should be received so that understanding may follow, which relates to the first item in this list of criteria. The second item, in this list, focuses on tasks that should be performed repetitively. The suggested curriculum is based on operational controls, which make teaching the content in a practical manner viable.

If the educational program combines textual information with practical exercises then the program would include diverse teaching styles, which is important for education, especially when it concerns adults (NIST, 1998, p. 20). Making use of different learning styles is another concept from cognitive information processing.

### 3.8.4 Provides feedback

Including practical exercises, as mentioned by the previous section, makes it possible for the program to give feedback to the learners. The idea is that the program will make use of some kind of simulation that will evaluate how well the learners carried out their tasks.

In a simulation, making mistakes does not incur any real risks, which makes it possible for learners to make mistakes without any damage being inflicted. Therefore, learners have the freedom to experiment. If learners make mistakes then it should be explained to
them what they did wrong and why it was the incorrect action to perform (Furnell & Gennatou & Dowland, 2000).

Feedback will not only ensure that the learners are aware of how much they are educated about information security, but will also allow managers to assess how their employees’ education is progressing, in a business environment. Therefore, feedback should be beneficial to the entire target audience.

Feedback comes in two forms: formative and summative. Formative feedback involves that the learners gain constant feedback on their learning performance, while summative feedback only provides the learners with feedback at the end of the program. To keep the learners updated on their performance formative feedback should be provided by an educational program on information security. However, feedback should also be provided to people who wish to verify the progress of learners, which could be managers who are concerned with the security skills of their subordinates. This feedback is more suited to summative feedback.

Feedback is important for all the learning models discussed at the beginning of this chapter. However, feedback from other people (collaborativism) in an environment that they are comfortable with (socio-culturalism) should be encouraged.

3.8.5 Learners responsible for their own learning

Van Niekerk & von Solms (2006) state that “users should be responsible for their own learning”. Employees of businesses can be bound contractually to be responsible for their own education in certain fields. By making it the employees’ responsibility to educate themselves, saves the organisation assets, such as time and money. This approach should work better if employees are motivated to learn about information security in their own time. This is the same approach that constructivism assumes.

Home users are responsible for their own education; no organisation is responsible for their education. The next chapter explains how one could motivate home users to learn about information security.
3.8.6 Accessible from home and work

In light of the previous point, the content of the educational program should be accessible to the learners at home, and in some cases, at work. The program should be in digital format which will enable employees to copy it from work and enable home users to download it from the Internet.

To summarise, the list of criteria is:

- Target audience should be able to understand the content;
- Learning repetitively;
- Practical teaching;
- Provides feedback;
- Learners responsible for their own learning;
- Accessible from home and work.

This list of criteria is formulated to solve problems with existing information security education programs. It also seeks to guide the users to a stage of unconscious competence while keeping them motivated.

Motivation could be added to the previous list of criteria, however, every part of the educational program would benefit if learners were enjoying it. The next chapter will explain how the proposed program generates motivation and how it meets the criteria specified in this section.

3.9 Conclusion

This chapter discussed the fundamental models of learning as their concepts and assumptions may contribute to the formulation of any education program. It was determined that no single model is appropriate to an educational program about
information security. However, concepts of multiple models may be used to strengthen such a program.

The levels of education were discussed that learners should go through to be competent at understanding information security concepts. A program that works through these levels to bring learners to a stage of unconscious competence should be strived for. It is unlikely that this project would produce such a program. However, it may contribute to future developments that reach the sought after results.

Problems with current education programs about information security were identified. Motivation was emphasised as a key underlying problem. Learners should be motivated to learn about information security to make general public education viable. The target audience identified for the educational program consists of the general public and employees of organisations, as specified by the previous chapter.

Criteria were formulated that an information security program of this nature should strive to achieve. The specified list of criteria focuses on the educational aspects of these programs. However, this chapter continued to emphasize the importance motivation plays in educational programs about information security. The next chapter will introduce how an information security program can be formulated to meet the criteria specified in the previous section, while motivating the learners to enhance their education.
Chapter 4: Educational Games

4.1 Introduction

It can be argued that people are, typically, not motivated enough to attend information security seminars or work through educational online material. Motivation has been identified in previous chapters as a key component to education in general and, more specifically, to information security education. This chapter discusses the use of an educational game to increase the motivation of learners engaged in information security education.

The remainder of this chapter will discuss educational games in general in order to identify the components of such games that might be applicable to the specific needs of information security education. Previous research done in the field of educational gaming will be examined to attain a broad perspective on educational games. This will be followed by more specific research to determine how an educational game should be created in order to educate its audience. The chapter concludes by examining how educational games may be suited for an information security program.

4.2 Educational games as a solution to information security problems

The use of educational games is the method by which this project seeks to overcome the problems of information security as discussed in Chapter 2 by incorporating the criteria for education programs as highlighted in Chapter 3. Educational games resolve the problems of information security programs through the following factors.
4.2.1 Self-motivation

Educational games can be made to be self-motivational. Motivation has been identified as a key factor in information security education throughout this dissertation. This factor can be exploited even further by employing stealth learning into the game.

A very good scenario would be if the employer gives the game to his employees and tells them to play it. The employees then play the game in their leisure time, learning how they should secure the information of the company. The employees play the game long enough and often enough to be kept reminded of the issues surrounding information security.

This is an optimistic scenario because the game in question needs to be very enjoyable for employees to keep on playing the game. This project is not likely to produce such an enjoyable game after a few iterations. However, the above scenario should still be strived towards in business situations. Motivation is also a factor when educating the general public.

4.2.2 Can reach general public

Educational games can be distributed to the general public. Due to the motivation people have to play games, it is possible to increase the general knowledge of home users if a game is provided to them.

Games can be distributed by using several measures. They can be transferred through portable hard drives and computer networks as people share the games they enjoy with their friends. Organisations may have the interest of increasing the knowledge of their customers on information security. This is particularly true for banks. Banks may upload a game to their website in order for their customers to download it for them to use their online services correctly. Adults form a big part of the general public which means that diverse teaching methods can play a large role in their education.
4.2.3 Use multiple teaching methods

Educational games can make use of diverse teaching methods. This is highlighted in the tables in section 4.2, which lists teaching methods that educational games use. Table 4.7 lists educational games that use more than one teaching method to convey its content. It is necessary to verify whether people are learning from the game after teaching methods have been applied. Some sort of feedback should be provided to implement this.

4.2.4 Supports feedback

Games can be written to verify how well a player plays the game. Educational games can use the same principle to determine how much a player has learnt. This type of feedback is important to employees who wish to monitor their progress and for employers to view how much their employees know about information security. Therefore, formative and summative feedback can be used such as described in Section 3.7.4.

If the fact that the game is an educational one is kept a secret from the players then the way feedback is provided should be done without revealing that the game is an educational one. This would form a part of the culture of the employees if their manager gains knowledge of the scores of their subordinates.

4.2.5 Games as part of information security culture

Games can support an information security culture in various ways. People enjoy sharing their experiences of similar things amongst each other. If all the employees in a department play the same game they will start talking about it.

People also like to compare how well they do things. If the game makes use of a scoring system which reflects how well the players are playing the game then these people will start to compare their game scores. This should motivate the employees to obtain better scores, which means they will play the game more. Companies may also wish to load the game on their staff computers to record every employee’s score. If the employees can view each other’s scores they should be even more motivated to play the game to receive...
the highest score. Companies can further promote the game by giving out prizes, on a 
regular basis, for the employees who receive the highest scores since the last time prizes 
were given out.

These are appropriate reasons to consider educational games as a solution for problems 
related to information security. However, there are some problems associated with using 
this approach.

4.3 Problems related to educational games used for 
information security education

The previous section discussed the reasons why educational games should be used to 
convey content on information security. It introduced scenarios whereby business 
employees and the general public could gain knowledge from educational games. 
However, these scenarios have weaknesses.

Some people do not like computer games. This point relates to the negativity that 
surrounds educational games as well as all the people in the world who dislike computer 
games. Despite the popularity of computer games one will still find people who do not 
want to play them. The older generation is more prone to be against new technology, but 
some young people are against computer games as well.

Critics of educational games often state that they do not like games, but admit that they 
have played Solitaire. Solitaire is the most used program within Windows (Levin, 2008). 
This is, arguably, because Solitaire is on one’s computer already, is very simple to play 
and generates enough motivation for players to play it instead of doing something else. 
One can then argue that if an educational game is already installed on workstations and 
adopters to the above mentioned criteria then it could be as successful as Solitaire.

It has been mentioned, in Section 4.3.1, that a company could install an educational game 
on its computers to promote an educational game. The obvious problem with this 
approach is that the employees might play the game at times that they should be 
working.
A possible solution to this problem is to have the game available only at times where business is slow or at times that the business can afford less productivity from their workforce. A more ideal situation would be to give the game to the employees for them to play it in their leisure time. However, then there is no guarantee that their employees are playing the game. Therefore, the weight of control needs to be considered against employee productivity.

Despite minor weaknesses of educational games it would appear that the benefits discussed in Section 4.2 outweigh the weaknesses addressed in this section. Therefore, an educational game should be created that aims to be used as Section 4.2 describes. The next section will discuss educational games, in general, which should be defined before specific cases of educational games are examined.

4.4 What is an educational game?

The purpose of most games is to provide enjoyment for those who plays it. Computer games have existed since the early days of computing and have since emerged as a multibillion-dollar industry (Harris, 2005).

The popularity of computer games would suggest that they have a very high entertainment value. Computer games can make use of sound, graphics and intriguing storylines to increase their entertainment value. This makes sense when one considers how popular audio CDs, movies and novel books are. There exists no formula to guarantee that a game would become popular. However, factors, such as the ones mentioned, do exist that increases the likelihood of a game becoming popular.

Note should be taken that players play games, not users. This chapter will refer to the persons engaged by the game as ‘players’.

Educational games are games that seek to be enjoyable by its players, but have an additional goal which is to educate its players on educational content (de Castell & Jenson, 2003). They are also known as ‘edutainment’ (Moreno-Ger & Burgos & Martinez-Ortiz & Sierra & Fernandez-Manjon, 2008), ‘serious games’ (Kelly et al., 2007) or even
digital game-based learning’ (Yue & Zin, 2009). Designers of these games attempt to create a product that reduces the need to motivate players to learn.

However, educational games are currently not very successful, or at least not as successful as commercial games (de Castell & Jenson, 2003). One of the reasons for this is because people have a negative perception of them (Bellotti, Berta, Gloria & Primavera, 2009). In the past, some game developers have failed to incorporate the educational value into games to produce an enjoyable product (de Castell & Jenson, 2003). Hence, many people avoid playing educational games because of negative past experiences. Another perception of educational games is that they are mostly targeted towards children (Corbeil, 1999). Therefore, adults may view them as ‘kids stuff’ and this means that they may be reluctant to play them. A third reason why educational games are not successful is that people tend to focus on the educational aspect thereof, which lessens the enjoyment aspect. McMichael (2007) noticed this effect when he gave his students an assignment that involved playing a game. Even though the game was not an educational one some of the students were against playing it purely because it was given to them as part of an assignment.

Despite some negativity that surrounds educational games a lot of research is being conducted about such games. One can deduce from this that in principle educational games is an interesting idea. The next section discusses categories of research that involves games, in general (not educational games), as these categories affect research of educational games.

Much research has been done on gaming. It is necessary to identify areas of research that should be considered when designing an educational game. De Castell and Jenson (2003) identified seven themes of research within games.

- Play and pleasure;
- Studies of gaming genres;
- Game-development, systems, and content point of view;
In addition to these seven areas of research within educational gaming, individual analysis of educational games can be identified as an eighth area. Papers that are included in this area usually describe their proposed educational game and explain how they teach their target audience. As few of these papers refer to what design principles contribute to the educational value of the game, this area is different from the constructionist theory area discussed earlier in this section. The next section lists researched games that form part of the individual analysis area.

### 4.5 Individual analysis of educational games

The previous section discussed research areas that relate to games. This section examines individual cases of educational games. This is done to discover how researchers create educational games and what the modern trends with regards to educational games are. A qualitative content analysis as discussed by Krippendorff (2004) is used to analyse these educational games. This method requires a large amount of individual cases in order to draw conclusions. However, the conclusions will still be argued and/or interpreted. The individual cases were analysed in terms of graphics, target audience, what educational content it conveys and what method it uses to convey its content. The cases are grouped by the method it uses to convey educational content, except for the games that teaches information security content as these games are explained in more detail. The games are grouped as:

- Puzzles;
- Simulations;
4.5.1 Puzzles

Puzzle games are good for teaching as the player needs to continuously think about the goals which will bring him/her closer to solving the game. Information can also be attained as the player notices events which bring him/her closer to their goals. The following are examples, found in research papers, of puzzle games.

Bottino & Ott (2006) describe five two-dimensional games that teach logic to primary school students. The first of these games is named MasterMind. The goal of the game is to determine a sequence of colours randomly selected by the game. MasterMind provides feedback on how close the player’s guess was to the correct sequence after each guess. A large degree of trial and error is required by the player as he needs to interpret the feedback of the program in order to complete it.

The second game is named Teravex (Bottino & Ott, 2006). This game works similar to a traditional puzzle (placing individual pieces together to form a cardboard picture), but instead of edges that fit together the pieces’ numbers need to match. The game ends when all the pieces are placed in such a way that adjacent numbers match together.

The third game introduced by Bottino & Ott (2006) is TreeTrent (Bottino & Ott, 2006). The game works very similar to Microsoft MineSweeper.

The fourth puzzle game is Hexip (Bottino & Ott, 2006). This game works similar to TreeTrent, but instead of four square boxes it uses hexagons.
The final game discussed by Bottino & Ott (2006) is Brickshooter. It is a 2D game that teaches primary school students logic and visual skills. The game involves players to match coloured bricks by shooting (or clicking) other bricks of random colours.

Norte & Lobo (2008) discusses Sudoku Access as a 2D game that teaches school students logic skills. A Sudoku is a Japanese puzzle that requires players to enter missing numbers to correspond with revealed ones. Sudoku Access is a digital Sudoku game that is developed to enable disabled people to solve a Sudoku on the computer.

Treez (Ford & Minsker, 2003) is a game that teaches tree traversal techniques for data structures to university students. Players of Treez are required to move through a multi-node tree and successfully navigate from the first node to the last one. A new combination of nodes is generated when the game starts.

<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterMind</td>
<td>Logic</td>
<td>2D</td>
<td>Primary school students</td>
</tr>
<tr>
<td>Teravex</td>
<td>Logic</td>
<td>2D</td>
<td>Primary school students</td>
</tr>
<tr>
<td>TreeTent</td>
<td>Logic</td>
<td>2D</td>
<td>Primary school students</td>
</tr>
<tr>
<td>Hexip</td>
<td>Logic</td>
<td>2D</td>
<td>Primary school students</td>
</tr>
<tr>
<td>Brickshooter</td>
<td>Logic and visual skills</td>
<td>2D</td>
<td>Primary school students</td>
</tr>
<tr>
<td>Sudoku Access</td>
<td>Logic</td>
<td>2D</td>
<td>School students</td>
</tr>
<tr>
<td>Treez</td>
<td>Tree traversal techniques</td>
<td>-</td>
<td>University students</td>
</tr>
</tbody>
</table>

Table 4.1: Summary of puzzle educational games

### 4.5.2 Simulations

Some games can be described as simulations. These games simulate a scenario wherein players may learn. Learning is generally achieved when a player views his/her results of the decisions he/she makes within the scenario. The game should clearly show players these results in order for them to learn. The following are examples of educational simulation games.
Sabri et al. (2010) describes a serious game for orthopedic surgeons to practice knee replacement surgery. “Total knee arthroplasty serious game” is a very graphical 3D game that seeks to increase the skills of knee surgeons. The game is still under development. Therefore, the study has not reached a conclusion at this point in time.

Second Chance (Pacheco, Motloch & Vann, 2005) is a game that teaches environmental protection, sustainability and awareness aimed at high school students. The game was a product of collaboration between organisations.

Environmental Detectives (Jenkins, Klopfer, Squire & Tan, 2003) is a 2D game which enables high school and university students to learn about environmental disaster recovery. In this game the player assumes the position of an environmental engineer who needs to make the correct decisions to recover from an environmental disaster. The Environmental Detectives game is played on a cell phone.

Cybertronix (Sanderson et al., 1997) is a 3D game which enables players to take control of an electronic manufacturing company. The game is aimed at university students. Cybertronix simulates the designing, ordering components, floor management and marketing aspects of the manufacturing process.

Taran (2007) discusses a 2D game that simulates risk management in a company to give university students some ‘practical’ experience. This game is also a multiplayer board game. Players assume the position of a project manager who plans, verifies requirements, designs, implements and tests products. Taran (2007) refers to the game as “board game” as the author does not give the game a name.

SDSim (Connolly, Stansfield & Hainey, 2007) is a game that simulates the software development process. This game is mostly for adults. Players assume different roles i.e. project manager, systems analyst, systems designer and team leader in order to create successful projects. The game supports the software development lifecycle which consists of design, development and evaluation steps.

SimSE (Navarro & van der Hoek, 2009) is a 2D simulation that teaches the software development process. This game is aimed at university students. SimSE is a single player
game that enables the player to make choices as a project manager. The goal of the game is to give students “practical experience” in this field. Players are able to change various factors which may change the successfulness of a project and several software development processes may be implemented by them.

Wang & Zhu (2009) discuss a 3D game which works on top of Second Life. This game also teaches the software development process and is aimed at university students. Second Life is a 3D online game that simulates human life itself. This game uses the game engine of Second Life to speed up development time. Another advantage of using this approach is that players can play the game online.

<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Total knee arthroplasty serious game”</td>
<td>Performing surgery</td>
<td>3D</td>
<td>Adults</td>
</tr>
<tr>
<td>Second chance</td>
<td>Environmental protection</td>
<td>-</td>
<td>High school students</td>
</tr>
<tr>
<td>Environmental detectives</td>
<td>Environment disasters</td>
<td>2D</td>
<td>High school and university students</td>
</tr>
<tr>
<td>Cybertronics</td>
<td>Manufacturing process</td>
<td>3D</td>
<td>University students</td>
</tr>
<tr>
<td>“Board game”</td>
<td>Risk management</td>
<td>2D</td>
<td>University students</td>
</tr>
<tr>
<td>SDSim</td>
<td>Software development management</td>
<td>-</td>
<td>Adults</td>
</tr>
<tr>
<td>SimSE</td>
<td>Software engineering process</td>
<td>2D</td>
<td>University students</td>
</tr>
<tr>
<td>“Game in second life”</td>
<td>Software engineering process</td>
<td>3D</td>
<td>University students</td>
</tr>
<tr>
<td>hACME</td>
<td>Software security</td>
<td>-</td>
<td>University students</td>
</tr>
<tr>
<td>Flightgear</td>
<td>Aircraft flight</td>
<td>3D</td>
<td>Adults</td>
</tr>
</tbody>
</table>

Table 4.2: Summary of simulation educational games

hACME (Nerbråten & Røstad, 2009) is a simulation aimed at university students that teaches software security. This game consists of levels. Each level is created as a
separate scenario. Players need to overcome a set of challenges to move on to the next level. This makes it easier for the developers to incorporate new levels, possibly teaching players about new scenarios.

FlightGear (Perry & Olson, 2001) is a 3D game that simulates the flight of aircrafts. It can be used to learn how to fly aircrafts. It was become popular to learn how to fly through a game because of the risks involved in real life. Simulations are also used to train air traffic control personnel.

4.5.3 Reading/Dialog

The games examined in this sub-section require their players to read text and/or listen to dialog in order to learn content. This method is similar to learning by reading a book, which many people are familiar with. Players may receive information from different perspectives if the games include different characters that the player can communicate with. A lot of games include textual ‘tips’ that help their players to understand the game. This method may use the same technique to help players understand various concepts.

Revolution (Jenkins et al., 2003) is a 3D game that teaches history. The game is very graphical because it is built upon Neverwinter Nights (an existing commercial game); this is similar to Wang & Zhu’s game reviewed in Section 4.4.2 which is built upon Second Life. In Revolution players assume the role of a townsperson in the time of the American Revolution. Players are educated about history when they communicate with agents in the game.

Tafelkids: The Quest for Arundo Donax (Jenson, de Castell, Taylor & Droumeva, 2008) is an online, 2D game aimed at school students. The game teaches its players about the history, culture and music of the Baroque period. The game developers made use of mini-games in order to teach these different concepts. Mini-games can be described as a collection of small games within the main game.

Winter Dreams (Tsoupikova, 2002) is a 2D game that is targeted towards preschool children. The game teaches language and listening skills. Winter Dreams is similar to a
digital bedtime story as the game narrates a fairy tale. This digital bedtime story includes animations and enables players to change the course of the story.

<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revolution</td>
<td>History</td>
<td>3D</td>
<td>-</td>
</tr>
<tr>
<td>Tafelkids: The Quest for Arundo Donax</td>
<td>History, culture and music</td>
<td>2D</td>
<td>School students</td>
</tr>
<tr>
<td>Winter Dreams</td>
<td>Language and listening skills</td>
<td>2D</td>
<td>Preschool children</td>
</tr>
</tbody>
</table>

Table 4.3: Summary of reading/dialog educational games

### 4.5.4 Unconscious learning

Unconscious learning is also known as *Stealth learning* (Prensky, 2001) which is when players learn concepts without them being aware of the learning process. By employing unconscious learning players may be more motivated to play the game, because it is not presented as an educational game. Games can make use of *hidden content* for a similar effect. However, this may not be as beneficial as unconscious learning. Unconscious learning is difficult to employ in certain games. Therefore, it is rare to find genuine examples of such games. This sub-section reviews one game that implements this technique.

*Alert Hockey* (Ciavarro, Dobson & Goodman, 2008) is a 2D ice hockey game which was tested on school children. This study investigated whether a game could change behaviour of players. Alert Hockey enables players to play ‘dirty’, e.g. shove other players, high sticking and tripping. However, if the players play ‘dirty’ the game raises in difficulty level (unbeknown to its players). The study concluded that the game does alter the behaviour of players as they played less ‘dirty’ every time they replayed the game.

<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Hockey</td>
<td>Disciplined behaviour in sport</td>
<td>2D</td>
<td>School students</td>
</tr>
</tbody>
</table>

Table 4.4: Summary of educational games that use unconscious learning
4.5.5 Collaborative learning

Collaborative learning follows the concepts of Collaborativism as discussed in Section 3.2.3. This means that players learn from each other instead of learning from one central source. This section reviews one example of a game that uses collaborative learning to convey educational content.

*Go Wild Scavenger Hunt* (Monahan, 2002) is a 2D game that teaches Internet browsing to school students. The game requires players to find Internet content over the web. Go Wild uses collaborative learning as students win or lose as part of a team. Players may comment on the content other players submits.

<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go Wild Scavenger Hunt</td>
<td>Internet browsing</td>
<td>2D</td>
<td>School students</td>
</tr>
</tbody>
</table>

Table 4.5: Summary of educational games that use collaborative learning

4.5.6 Games that use multiple teaching methods

Some games make use of more than one method to convey information to its players. This sub-section reviews games that employ multiple teaching methods.

*Elemental* (Chaffin, Doran, Hicks & Barnes, 2009) is a 3D game that was tested on university students. The game teaches computer programming, specifically to code tree traversal techniques. At the start of each level the player is presented with a programming environment where he should write real code. When the player submits his code the game changes to a 3D environment where a visual representation of his code is displayed. In this environment the player can see the tree that his code is traversing. As no physical tree exists it can be stated that this game simulates programming by using a metaphor. When the avatar in the 3D environment reaches a node, textual information is presented to the player. Therefore, this game makes is a simulation that makes use of dialog to convey content.
Wu's Castle (Eagle & Barnes, 2009) is a 2D game that teaches university students computer programming. Players of the game assume the role of a character that lives in medieval times. Similar to the previous example this game is a simulation as part of a metaphor, because programming instructions are visually represented. The game character can communicate with other characters that may give him advice on programming.

Polyglot Cubed (Grace, 2009) is a 3D game that teaches university students languages. This game is another example of a simulation that uses a metaphor, which includes textual instructions to educate players. The game play involves players identifying pictures with words with instructions guiding them.

Tower of Cubes (Tan & Seng, 2010) is a 2D game that teaches university students about data structures. The game represents data structures as cubes. The player needs to match cubes which have an effect on the data structure. Therefore, Tower of Cubes is a simulation with a metaphor attached to it that involves players to solve a puzzle.

Turkey Maiden (Underberg, 2008) is a 3D game that teaches high school students about history. This game is a simulation as the game simulates a historic town. Players can explore this town, make decisions that can influence history and talk to townspeople to receive a greater insight into how people lived during that time.

Murder on Grimm Isle (Dickey, 2006) is a 3D game that teaches its players how to form arguments. The game is aimed at school as well as university students. The game simulates a murder mystery where the player can obtain clues from interviewing people in the game. By matching acquired phrases the player learns how to formulate appropriate arguments.

Storytelling Alice (Kelleher, Pausch & Kiesler, 2007) is 3D game aimed at middle school students that teaches computer programming. Students can learn from the game by reading/hearing dialog from the game. Storytelling Alice simulates programming by enabling players to drag-and-drop code elements that formulate programs within the game. This is done to remove errors encountered by incorrect syntax.
**SMILE** (Adamo-Villani & Wilbur, 2007) is a 3D game that teaches primary school students math and science. The game is very graphical in that it includes cartoon characters in a 3D town. Players may enter several houses in the town, each containing a hands-on math or science activity.

**Twisted Physics** (Samuelson, Halff, Halff & Brown, 2010) is a 3D game that teaches science to high school students. This game is very graphical and it simulates a laboratory. Twisted Physics immerses the player in a story which requires them to explore and experiment to move on in the story.

**Biohazard** (Holland, Jenkins & Squire, 2003) teaches adults about biochemistry. The game simulates a hospital wherein players are required to fulfil several tasks. The game uses information acquisition and testing to teach players how to do tasks correctly.

**Supercharge** (Holland, Jenkins & Squire, 2003) is a 3D game that teaches physics. The game is aimed at school as well as university students. The game simulates an environment with charged particles. By moving these particles in the simulation players learn physics through information acquisition and testing.

**Immune Attack** (Clements, Pesner & Shepherd, 2009) is a 3D game that teaches the workings of the human immune system. The game is aimed at school as well as university students. The game simulates an environment where the player may receive information on the immune state of a person while being able to manipulate it, for example by choosing to kill bacteria. Feedback is given on the choices that the players make.

**Seagame** (Bellotti et al., 2009) is a 3D game that teaches high school students how to be safe at sea. This is a very graphical game as players can walk along a 3D beach or travel on the ocean on a boat. The game does not perceive itself to be an educational game. Therefore, it can be argued that the game hides its educational content. Furthermore, information acquisition and testing is used to instruct players to implement safety procedures.
<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Teaching method</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>EleMental</td>
<td>Computer programming</td>
<td>Reading/Dialog Simulation through metaphor</td>
<td>3D</td>
<td>University students</td>
</tr>
<tr>
<td>Wu’s Castle</td>
<td>Computer programming</td>
<td>Reading/Dialog Simulation through metaphor</td>
<td>2D</td>
<td>University students</td>
</tr>
<tr>
<td>Tower of Cubes</td>
<td>Data structures</td>
<td>Puzzle Simulation through metaphor</td>
<td>2D</td>
<td>University students</td>
</tr>
<tr>
<td>Turkey Maiden</td>
<td>History</td>
<td>Reading/Dialog Simulation</td>
<td>3D</td>
<td>Eighth-grade students</td>
</tr>
<tr>
<td>Murder on Grimm Isle</td>
<td>Argumentation</td>
<td>Reading/Dialog Simulation</td>
<td>3D</td>
<td>High School and university students</td>
</tr>
<tr>
<td>Storytelling Alice</td>
<td>Computer programming</td>
<td>Reading /Dialog Simulation</td>
<td>3D</td>
<td>Middle school students</td>
</tr>
<tr>
<td>SMILE</td>
<td>Math and Science</td>
<td>Reading /Dialog Simulation</td>
<td>3D</td>
<td>Primary school students</td>
</tr>
<tr>
<td>Twisted Physics</td>
<td>Science</td>
<td>Reading /Dialog Simulation</td>
<td>3D</td>
<td>High school students</td>
</tr>
<tr>
<td>Biohazard</td>
<td>Biochemistry</td>
<td>Acquisition/testing Simulation</td>
<td>-</td>
<td>Adults</td>
</tr>
<tr>
<td>Supercharge</td>
<td>Physics</td>
<td>Acquisition/testing Simulation</td>
<td>3D</td>
<td>High school and university students</td>
</tr>
<tr>
<td>Immune Attack</td>
<td>Immune system</td>
<td>Acquisition/testing Simulation</td>
<td>3D</td>
<td>High school students and university first-years</td>
</tr>
<tr>
<td>SeaGame</td>
<td>Safety at sea</td>
<td>Acquisition/testing Hidden content Simulation</td>
<td>3D</td>
<td>High school students</td>
</tr>
<tr>
<td>Polyglot Cubed</td>
<td>Languages</td>
<td>Reading/Dialog Simulation through metaphor</td>
<td>3D</td>
<td>University students</td>
</tr>
<tr>
<td>Eduventer-II</td>
<td>History</td>
<td>Dialog/Reading Hidden content Simulation</td>
<td>3D</td>
<td>-</td>
</tr>
<tr>
<td>DinoQuest Online</td>
<td>Science</td>
<td>Puzzle Acquisition/testing Dialog/Reading Simulation</td>
<td>-</td>
<td>School students</td>
</tr>
</tbody>
</table>

Table 4.6: Summary of educational games that use multiple teaching methods
Eduventure-II (Wechselberger, 2008) is a 3D game that teaches history. This game is similar to Turkey Maiden as it simulates a city in history and educates its players by means of dialog. Eduventure-II hides some of its content to make the game more appealing.

DinoQuest online (Scacchi, Nideffer & Adams, 2008) teaches science to school students. The game includes several mini-games. Each mini-game differs from what teaching methods it uses although each game teaches the player about science. Simulation, reading/dialog, acquisition and testing as well as puzzles are used by these mini-games.

### 4.5.7 Games relating to information security

As this study is about teaching people about information security the papers that have conducted similar studies are covered in more depth. This sub-section reviews games which teach information security related content.

CyberCIEGE (Cone, Irvine, Thompson & Nguyen, 2007) is a very graphical 3D game that aims to teach security concepts to the US military. The game simulates a world with people, computer hardware as well as software. CyberCIEGE switches from a 3D game to a 2D one when the player uses a computer within the game. The game consists of scenarios that players must solve correctly to move forward in the game. These scenarios may include troubleshooting network hardware and changing settings on computers. The game provides tips and feedback to its players via popup indicators. CyberCIEGE can be viewed as a game that teaches information security, because it trains players to follow security policies (Irvine & Thompson, 2004).

Anti-phishing Phil (Sheng et al., 2007) is a 2D game that teaches players to recognise phishing threats. Phishing is a technique whereby fake websites lure people who browse the Internet to enter sensitive information. Phishing is discussed in more dept in Chapter 6. If a person knows how to verify the URL of a website he/she is more likely to browse the correct websites, which reduces the chances of being phished. The Anti-phishing Phil game gives players a time limit to identify whether displayed URLs are correct. If the player identifies the URL incorrectly, or runs out of time, then immediate feedback is
given to him/her explaining to him/her why. The method of teaching can be described as information acquisition and testing. Players receive information and are tested whether they understand it. Anti-phishing Phil is not a simulation game as nothing in the game simulates Internet browsing. The results of this study concluded that the game is more effective to educate people than if they were to read phishing related material.

*E-Tool* (Furnell, Gennatou & Dowland, 2000) is a 2D program that educates adults on information security. This is a training program and not a game. However, this program is included in this list, because it is very similar to an educational game. E-Tool provides users with a score as feedback on their choices and incorporates visual elements. The game contains scenarios for users to work through. Each scenario presents a picture to the user which contains equipment that may be threatened. By clicking on the equipment, users receive descriptions about it. Users need to determine what information security threat resides in the scenario and then select suitable controls to mitigate the threat. The game calculates a score based on the appropriateness of the selected controls and provides feedback to the users if they selected the wrong set of controls. Therefore, information acquisition and testing is the learning method this program uses.

<table>
<thead>
<tr>
<th>Name</th>
<th>What teach</th>
<th>Teaching method</th>
<th>Graphics</th>
<th>Target audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberCIEGE</td>
<td>Network security</td>
<td>Simulation</td>
<td>3D</td>
<td>Adults</td>
</tr>
<tr>
<td>Anti-phishing Phil</td>
<td>Phishing detection</td>
<td>Acquisition/testing</td>
<td>3D</td>
<td>University students</td>
</tr>
<tr>
<td>E-tool</td>
<td>Information security</td>
<td>Acquisition/testing</td>
<td>2D</td>
<td>Adults</td>
</tr>
<tr>
<td>“Board game”</td>
<td>Information security</td>
<td>Acquisition/testing</td>
<td>2D</td>
<td>Mostly adults</td>
</tr>
</tbody>
</table>

Table 4.7: Summary of educational games on information security

Newbould & Furnell (2009) introduces a 2D digital board game that teaches information security concepts. A “board game” was implemented because it helps users to quickly understand how the game works (Newbould & Furnell, 2009). The game starts when the player rolls the dice, which moves their figure around the board. The board consists of
coloured squares. Depending on the colour the figure lands on, it determines what topic the player is questioned on. This is similar to the popular board game *Trivial Pursuit*. However, all the topics in this game are about information security and all the questions are multiple choice. After a question has been answered immediate feedback is given to the player. Therefore, this game uses information acquisition and testing as its education method.

### 4.5.8 Discussion of content

The results of the content analysis done on educational games can be used to deduce some conclusions.

Educational games are about various topics. Physics, history and biochemistry are topics identified as being researched. Therefore, a lot of fields that can benefit from the use of educational games exist.

‘How the game conveys content’ reveals several things. There exist different methods that games use to educate its players and no *golden*, one-size-fits-all method exists. The methods do, however, match with certain topics. The four games about history are made to tell a story to the player through dialogs and/or reading some text. Hence, some teaching methods are better suited for certain game topics. Many of the game developers choose simulations as their teaching method. Researchers debate whether a program that simulates an environment is truly a game (Squire et al., 2003). Regardless, it is very educational for players to enter a digital environment where they can see and learn how things work. This also enables the player to experiment in a danger free environment. If you want to alter the course of history rather do it in a game! Experimentation in games is tied together with consequences to form acquisition/testing within simulations. Fifteen of the games analysed used multiple teaching techniques. Multiple teaching techniques enable learners to receive information in different forms, which may help the education process. If a player sees something in a simulation, for example, and reads an explanation of what happened, the point is more likely to be conveyed than if it was only seen or only read.
Three of the games analysed hide their educational content from the players. This can also be called 'stealth learning' (Prensky, 2001) and it is often used to decrease the negativity surrounding educational games. Players may enjoy a game more when they are unaware that they are learning educational content (McMichael, 2007). Therefore, stealth learning enables educational games to be viewed as normal computer games by its players.

Twenty educational games were identified as using two-dimensional (2D) graphics, but twenty-two educational games were identified as using three-dimensional (3D) graphics. It seems as if there is no clear preference between 2D or 3D graphics when it comes to educational games. However, implementing 3D graphics is more complex than implementing 2D graphics. A lot of educational game designers believe that 3D games will produce a more enjoyable product. This might also be the case when the designers want the educational game to be perceived to look like a commercial game (Bellotti et al., 2009). Researchers might want to implement 3D graphics, but cannot due to their limited development resources.

Researchers can spend less time developing games if they use existing platforms to create the game. Second life, Neverwinter nights and Oblivion have been identified by papers as platforms that educational games can be created with. These three platforms enable 3D graphics.

As mentioned earlier in this chapter, many educational games are targeted towards children and young people (university students). School students at various stages were targeted by twenty-one of the games analysed. University students were targeted by thirteen of the games, while only seven of the games were targeted to adults. Researches may favour university students as they often have easier access to them. However, the figures suggest that educational games (and perhaps games in general) are not usually created for adults.

In summary the analysis indicates that educational games:

- Are studied in various fields;
Include various teaching methods, some better suited to specific content;

Make intensive use of simulations;

May be viewed as a normal game by using ‘stealth learning’;

Are implemented by using 2D as well as 3D graphics;

Can be created by using existing platforms to minimize development time;

Are targeted, mainly, towards children but also to adults.

The research conducted on educational games does reveal some information security related work. However, this is not enough to indicate that it is generally accepted that information security content can be conveyed by an educational game. The next section determines design factors that should be considered when creating an educational game about information security.

4.6 Design factors for an educational game on information security

It is important to establish what factors contribute to the success of an educational game from a design perspective. Some of these factors were compiled though related literature while others are introduced to solve problems that are particular to information security. The following are design factors that this project will implement with the goal to create a successful educational game that teaches information security concepts.

4.6.1 Force players to learn

Players should **not** be able to be successful at playing the game without learning its educational content. Being good at playing the game should also mean that the player knows the educational content of the game well. Fisch (2005) describes this factor as “content needs to be well integrated into educational games”, essentially “forcing players
to learn” is the same factor that Fisch describes. However, the statement: “force players to learn” emphasises the educational aspect of this factor.

This factor might sound a bit obvious. However, many educational games do not adhere to this point. This is mainly due to the struggle to bridge the gap between enjoyment and learning within educational games. “Educational games” do exist that are exactly like commercial games, but the educational content that the game provides can be skipped by the player (Yue & Zin, 2009). These games often make it possible for the player to progress in the game without learning educational content, which is what this project seeks to avoid.

An educational game should ensure that the players have used their knowledge of the content of the game in order to progress in the game. If the players do not have that knowledge then the game should teach them that knowledge. In order to gain knowledge the game should be fairly simple to understand.

4.6.2 Creating an understandable game

Players need to understand an educational game in order for them to learn educational content. The less time players have to familiarise themselves with a game the more important it is to make the game easy to understand. As this study has limited resources available to perform lengthy experiments it must ensure that the game is understandable in order for the study to reach meaningful results. If the players of the game state that they did not understand the game then it will be difficult to argue that the game is educational or it is not educational. If players are aware that the game is educational then, although they may understand the game, they may be against playing it because of negative perceptions towards educational games.

4.6.3 Prevent negativity surrounding educational games

The game should not be viewed in a negative way such as some other educational games. It should be viewed as a “normal” game, with the goal to be entertaining, to its players. This can be achieved by hiding the content of the game from its players (Bellotti et al,
Section 4.2 examines some games that use ‘hidden content’ to create a more enjoyable game.

Creating an information security educational game to fully hide its contents might be impossible. However, the game can still be made to appear as a normal game until the player gets used to the game. Arguably, this approach might not be a ‘genuine’ content hiding implementation. However, it should give the game a better first impression on players. Players often make up their minds about a game fairly quickly. Many players might start to enjoy the game before they realise that it is an educational game. Once people's minds are made up about something it is generally difficult to convince them otherwise. Therefore, creating a good first impression should be sufficient for the purposes of this study. Other motivational techniques also play a role in achieving this.

4.6.4 Include motivational techniques

Additional attention must be given to the motivational aspect of this educational game. Being a game, and hiding the fact that it is an educational one, does not guarantee that enough people will enjoy playing it. However, playing a game should still be more motivational than other, more common, information security education techniques.

Players should be able to see each other’s scores in a business environment to increase competitiveness of the players. When a group of people play the same game, being a computer game or otherwise, they should enjoy determining who the best player is. Even if one person in the group is commonly known to be the best player the other people in the group should be motivated to try to become the next best player. Chapter 6 explains all of the motivational techniques that were used by the game. A player's score will be calculated by a grading system, which is described as the next factor.

4.6.5 Implement a grading system

A grading system will determine how well the player is playing the game. This grade should be shown to the player as a source of feedback, so that they will know how well they are playing the game.
A grading system is usually implemented by issuing points to the player when he does something good and deducting points when he does something poorly. The points are tallied at the end of the game and the final score of the player is presented to him.

In the case of the proposed game, when the players conform to the rules of information security their scores will strongly reflect this by being a high one. On the other hand, if the players do not conform to information security practices then their scores should be fairly low.

By recording previous scores may reveal some interesting information for organisations. This may include keeping track of employee effectiveness to perform security controls, comparing employees to determine the overall level of security compliance and individual scores that may be used to identify the easiest targets to security attacks.

The design factors proposed above can be generalised to work for educational games that teach content other than information security. However, they should be suited for an educational game for information security based on the techniques discussed by Section 4.3. Educational and motivational techniques are emphasised throughout this chapter as an educational game must be designed to maintain both. However, it may be difficult to implement both in a game, since these two aspects are often conflicting.

4.7 Conclusion

This chapter explained educational games. They are difficult to create because they are created with the intent of being educational as well as enjoyable. There exists negativity towards educational games because of previous games that did not successfully implement education and motivation in a single game.

Research in gaming was explored as it may contribute to uncovering how problems regarding information security may be solved. A lot of research has been conducted on games and a lot more is needed for educational games.
A content analysis revealed popular trends for educational games that have been researched. These trends can be used to identify what game factors should result in a good educational game. However, due to negative reactions of educational games the techniques should be tested. How these techniques are implemented will also have an impact on the results of this study.

The strengths and weaknesses of using educational games to convey information security knowledge were discussed. The advantages seem to greatly outweigh the disadvantages. The strengths discussed are aligned with the problems identified with information security programs as discussed in the previous chapter.

Finally, factors were established that would form a key role in the design and success of this type of educational game. These factors build upon the criteria specified for an educational program about information security, which was concluded by the previous chapter. However, these factors focus on an educational game as the program, which includes both educational and motivational factors.

The next chapter discusses the design of the experiment that was implemented to verify the techniques used to create the educational game.
Chapter 5: Experimental Design

5.1 Introduction

Chapter 3, of this dissertation, examined how educational programs convey knowledge about information security and identified some of the problems with these programs. Chapter 4 discussed educational games as a possible solution to these problems when certain criteria are met. This chapter discusses the methods used to evaluate whether a game that uses this criteria will be educational enough and enjoyable enough to solve the problems of educational programs on information security as discussed in Chapter 3.

The rest of this chapter will discuss the design of an experiment in which an educational game was evaluated against the predetermined criteria. The next section provides a brief overview of all the methods used during this experiment.

5.2 Research process

This study used several methods to ensure that the results of the research would be rigorous. Firstly, a prototype educational game was developed according to principles identified by means of a literature study. Secondly, an experiment was used to evaluate the effectiveness of the prototype by means of a questionnaire and observation. This section provides an overview of the process of these research methods.

A computer game was created, as a prototype, to evaluate its educational and motivational design techniques. Papers that described this prototype were presented at two South African conferences (Information Security South Africa (ISSA) 2009 and South African Institute for Computer Scientists and Information Technologists (SAICSIT) 2009) as research in progress to strengthen its proof of concept. Since the output of this part of the research is an artefact, design-science, as described by Hevner, March, Park & Ram (2004), was adhered to ensure that proper research design principles were followed by this study. This method, and its applicability to this study, are discussed in depth in
Section 5.4. The *prototyping* development life cycle was used to implement this prototype. Three iterations of the life cycle were completed.

Secondly, a questionnaire was used to determine whether learners enjoyed the game and whether they learnt the intended lessons contained in the educational content through playing it. The questionnaire included multiple choice questions on information security, multiple choice evaluations on the motivational aspects of the game and one open-ended question where participants could add comments they may have regarding the game.

Before the experiment could be implemented ethical clearance was obtained from the Research Ethics Committee (Human) or REC-H committee at the Nelson Mandela Metropolitan University (NMMU). The entire questionnaire was provided to the ethics committee as well as a detailed explanation on the experiment, what the results were for and a description of the participants that were used. The REC-H committee approved ethical clearance for the experiment.

A final experiment took place where the participants played the game and completed the questionnaire. The second part of the experiment was done on participants who only completed the questionnaire. This group served as the control group. The participants, in both groups, consisted of first year engineering students at the NMMU. Observations were used in the experiment to note responses that would strengthen the outcomes of the study, which could not be recorded by using other measures.

After the results of the experiment were compiled it was presented at the SAICSIT 2010 conference as a full research paper. The next section discusses the strengths and weaknesses of the above mentioned methods to clarify why they were used.

### 5.3 Strengths and weaknesses of methods

Several strengths and weaknesses of using the methods discussed in Section 5.2 are prevalent. The strengths of a prototype are that it serves as a proof of concept and it can be tested by participants that match people that would play the game in practice. A weakness could be that the design techniques that the prototype tests is done in a
specific context, which makes it more difficult to evaluate. If the design techniques were evaluated by an expert review, for instance, then they could be evaluated on their own. However, by using a prototype the techniques are placed within a context of a game with different factors attached to it. One of these factors would be usability, although the final experiment did not measure usability it should have an impact on learner motivation as well as the educational value of the game. However, all the design techniques are supported by research as well as some of the factors that constitute the context of the game, as discussed in Section 4.2. Therefore, a prototype was selected to test the identified design techniques to which an educational game for information security should adhere.

The experiment to verify the effectiveness of the developed prototype was conducted on two groups. The first group of participants played the game, completed the questionnaire, received remuneration for their time and efforts, and was encouraged to replay the game if they wanted to. This group was called the ‘play group’ of participants. The second group was only required to complete the questionnaire. This group served as a control group. The results of the questionnaires were compared between the play group and the control group. The experiment could have been designed with one group of participants if they completed the questionnaire, played the game and then completed the same questionnaire. If the ‘before’ and ‘after’ questionnaires were compared it should indicate whether the game was educational. This was not implemented because the participants would know what to look for in the game and they would expect to play an educational game, which may lessen their interest thereof. The weakness of the experiment, which was implemented, is that there would be a chance that the play or the control group is already knowledgeable in the field of information security. This potential problem is addressed by statistical methods, which is proven to be accurate, to a large degree, if the required amount of participants is gathered from the same background. Remuneration was given to the participants to motivate them to attend the experiment. The weakness of providing remuneration is that some participants may not be interested in the game, but only attended to receive the remuneration. Therefore, additional remuneration was on offer for the participants that did exceptionally well in the game. This was intended to motivate the participants to at least try and understand the game in order to play the game well.
Questionnaires served as a suitable medium to determine whether the prototype is educational. However, a questionnaire is not suited to record more detailed information of how participants played the game, because it was feared that having to continually record their actions would have a negative effect on the players’ concentration during game play. The prototype was linked to a database that recorded detailed information of user actions to overcome this problem. Multiple choice questions, in the questionnaire, were used to test participants on the knowledge they gained while playing the game. The alternative, open questions, would take too long to evaluate. This meant that participants could potentially guess the correct option. However, by using statistical methods it could still be determined whether participants had learnt information by playing the game.

Qualitative as well as quantitative measures were used to determine whether the game was enjoyable, by using questionnaires and observations. Questionnaires asked a series of questions where participants evaluated how much they enjoyed playing the game. Observations were used to record how many participants replayed the game, what was said about the game and what the attitude of the participants was toward aspects of the game. Formal interviews were not conducted, because it would take too much time to implement. In the play section of the experiment the participants were given remuneration when they had finished completing the questionnaire. However, they were encouraged to replay the game, for no additional remuneration. This was done to observe whether the participants enjoyed the game enough to play the game in their own free time. The weakness in this method is that participants may replay the game with the intent of receiving additional remuneration given to those who received top scores in the game. However, people are not likely to play a game that they do not enjoy if there is only a small chance of them gaining something from it. Therefore, this method was deemed suitable for the purposes of this study.

This section gave a brief overview of the strengths and weaknesses of the chosen methods. To strengthen the entire design process Hevner’s design-science guidelines were followed. The next section discusses these principles and how this project adhered to them.
5.4 Implementation of Hevner’s design-science

Hevner’s et al. (2004) design-science guidelines were followed to ensure that the study was designed in accordance with research requirements. The seven guidelines of design-science as described by Hevner et al. (2004) are:

- Design as an Artefact;
- Problem Relevance;
- Design Evaluation;
- Research Contributions;
- Research Rigor;
- Design as a Search Process;
- Communication of Research.

The following sub-sections explain how this study conforms to these guidelines.

5.4.1 Design as an Artefact

Hevner et al. (2004) state that the purpose of design-science is to create an artefact to "address an important organizational problem". An artefact could be a "construct, a model, a method, or an instantiation" (Hevner et al., 2004). The artefact produced by this project is the game prototype. This is an artefact because it is a construct that addresses the problem of information security education in organisations.

5.4.2 Problem Relevance

The problem that the artefact addresses must be a relevant business problem (Hevner et al., 2004). Section 2.3.1 argues that employees of an organisation must be aware of
information security, which is supported by references. Section 2.4 discusses four ways in which businesses currently address information security related problems, namely: risk management, implementing best practices, cultivating an information security culture and educating employees. Finally, section 3.5 highlights problems with educational programs on information security. Therefore, the problem that the prototype was designed for is a relevant one.

5.4.3 Design Evaluation

The artefact should be evaluated according to design principles. Hevner et al. (2004) states that: “evaluation of a designed IT artefact requires the definition of appropriate metrics and possibly the gathering and analysis of appropriate data”. Chapter 4 concludes by introducing a set of metrics that should be used to evaluate a computer game that seeks to educate its players on information security. These metrics are based on the research compiled by several sections in that chapter. Data gathering and analysis took place as two iterations of prototyping were conducted prior to the final experiment. The findings of these iterations are explained in Section 7.2.

5.4.4 Research Contributions

The study must provide contributions to the research field. This may be in three forms, namely: Design Artefact, Foundations and Methodologies (Hevner et al., 2004). This study contributes the designed artefact as it solves a business problem, but also contributes to methodologies as its results revealed the effects of educational and motivational techniques. These results can be used as guidelines for similar studies on not only information security, but also for studies about educational gaming in general.

5.4.5 Research Rigor

The construction and evaluation of the design artefact should be applied by implementing rigorous methods (Hevner et al. 2004). The study was implemented in accordance with design-science as described by Hevner et al. (2004), which is a
recognised research method. The artefact was created by using the prototyping development life cycle which undergoes several iterations of evaluation (Alavi, 1984). Finally, the results of the experiment were formulated by using statistical evaluations, which serve as rigorous methods (Hevner et al., 2004).

5.4.6 Design as a Search Process

A process should be incorporated into the design that seeks to find the most suitable design of an artefact to solve the problem. This can be accomplished by several iterations of a prototype where design alternatives are continuously introduced and evaluated (Hevner, et al, 2004). Section 4.4 started a search process by examining design techniques used by other designers. The prototype which this project produced implemented several of the techniques that were found. This study evaluated these techniques. Future work on this prototype may be used to evaluate a different set of design techniques.

5.4.7 Communication of Research

"Design-science research must be presented both to technology-oriented as well a management-oriented audiences" (Hevner et al., 2004). A paper describing the game prototype and the results of its evaluation was accepted and presented at the SAICSIT 2010 conference (Monk et al., 2010). The audience consisted of both technology- and management-oriented individuals.

By following design-science the artefact and the evaluation thereof are more research oriented. This had some impact on the design of the experiment. However, design-science did not provide exact details of how an experiment should be implemented.

5.5 Design of the research process

The research methods for this study included an experiment that uses a prototype and a questionnaire in conjunction with observations. The purpose of this section is to
indicate that these methods should produce solid research results. The following subsection describes, in detail, the different aspects of the experiment, why they were used, the data captured by it and how the data was analysed.

5.5.1 The prototype

A prototype was created in the form of a computer game to solve the problems this study addresses. This served as the artefact discussed in Section 5.4.1 required by design-science.

The prototype was developed by using Microsoft Visual Studio 2005, C# programming language and Microsoft Access as the database utility. Microsoft Visual Studio 2005 and C# were used because the developer was more familiar with them. Microsoft Access was used to manage the database because it is easier to setup than other database managers and its limited capabilities were sufficient for the purposes of the experiment.

The prototyping approach was used to develop the prototype. It should be noted that a research prototype can be developed by using the standard development life-cycle. However, prototyping provided greater benefits for this project. Prototyping may be used to develop a prototype that is used purely for testing purposes, but it can also be used to develop a fully functional system because a prototype can be continually refined into a finished product (Alavi, 1984). Therefore, by using prototyping, this system started as a proof of concept game and evolved into the final experimental prototype through periodic evaluations. Figure 5.1 depicts the stages involved by following either the prototyping or development life-cycle approaches.

The life-cycle approach consists of stages that take longer to complete than the prototyping approach, but only one cycle is required to produce the finished product. Prototyping consist of less time consuming stages, but takes multiple cycles to produce the end product. The benefits of prototyping include faster response to users’ requirements/evaluation and in addition, it offers an opportunity for experimentation (Alavi, 1984), which was suitable to this project.
The prototype went through three cycles. The number of cycles was not predetermined. The prototype was deemed to be ready for the final experiment when it was relatively understandable and free of errors. This ensured that research results would be attained from the study because if the participants could not play or understand the game then it

<table>
<thead>
<tr>
<th>Prototyping approach</th>
<th>Life Cycle approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify Initial User Requirements</td>
<td>Systems Analysis</td>
</tr>
<tr>
<td>Develop a Prototype</td>
<td>Requirements Specification</td>
</tr>
<tr>
<td>Use and Evaluate the Prototype</td>
<td>System Design</td>
</tr>
<tr>
<td>Revise the Prototype</td>
<td>System Development</td>
</tr>
<tr>
<td></td>
<td>Installation and Review</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
</tr>
</tbody>
</table>

Figure 5.1: The Information Systems Development Approaches - Adapted from Alavi (1984)
would be difficult to deduce conclusions from their responses. To address the problem of this study the prototype (game) needed to be designed to be educational and enjoyable.

Section 4.4 reviewed various design techniques that are used to create an educational game. From this review, the final prototype was decided to be a simulation game, which included reading/dialog and acquisition/testing teaching techniques. To make the game enjoyable it included: two-dimensional (2D) graphics with Windows Forms, a grading system and hidden content. In addition to these techniques the game was created to be as replayable as possible, which can be perceived as an educational as well as a motivational technique.

There are several reasons why these design techniques were chosen. A simulation game was used because of its strong appearance in other educational games as highlighted by Section 4.4. Reading/dialog was introduced to emphasize what the players should be learning while they played the game and acquisition/testing was used to verify whether they were learning the educational content.

“Force players to learn” was a factor discussed in Section 4.5.1, which ensured that, if players played the game well, it would mean that they were learning the educational content.

Many learning techniques accommodated various adult learning styles. However, it was decided not to employ more techniques as this could potentially result in a game which would be confusing to play. Therefore, the right balance between too many or too few learning techniques was sought.

In order to create a more understandable game 2D graphics with Windows Forms was chosen above 3D graphics, which would also have taken longer to implement. It was implemented as a digital board game as this would make the game more understandable (Newbould & Furnell, 2009). The game made use of hidden content as this would shift the focus of the player to the motivational aspects of the game instead of the educational ones, which should result in a more enjoyable game. A grading system was used to be able to show players each other’s scores as well as their own. This added to the motivational aspect of the game as this should make players motivated to achieve a
higher score than the other players. The grading system is a key element in creating a replayable game to ensure that players want to play the game again. The game needed to be replayable because it seeks to continually remind players about information security.

The scores, of the players, and some of their actions within the game were recorded in a database. This was done to enable players to view each other’s scores, which is a motivational aspect. However, this made it possible to reach conclusions from the scores of the players, as higher scores would suggest that players were learning from the game and lower scores would suggest that the players were not learning from the game. This made it possible to compare scores of the same player if they played the game multiple times. However, the total score in the game is only a reflection of how well they played the game. To evaluate more accurately whether players were learning from the game some of the actions of players were recorded by the program. Therefore, the database was used for further analysis on the effectiveness of the educational factors of the game. The implementation of this prototype is described in Section 6.4. The primary method used to analyse the educational and motivational aspects of the game was the questionnaire.

5.5.2 The questionnaire

After the game was played by the play leg participants they were required to complete a questionnaire. The questionnaire consisted of two sections. Section 1 contained thirty-three multiple-choice questions about information security. These questions were used to evaluate whether the participants had learnt the lessons intended by the educational content through playing the game. Section 2 contained four questions to evaluate whether the participants had enjoyed playing the game. The control group was not required to complete Section 2.

Section 1 included definition, short and scenario type questions. Seven information security related topics were covered in the thirty-three questions of Section 1. These topics are discussed in detail in Section 6.2. All of these were closed questions which presented the participants with a predetermined list of answers (Oppenheim, 1998, p.
112). These questions consisted of yes/no questions and multiple choice questions with either three or four answers.

Section 2 of the questionnaire contained three closed questions. These included two yes/no questions and a Likert scale question (Sapsford, 1999, p. 223) with four responses. The Likert scale question did not include a ‘neutral’ response, which forced the participants to make a decision (Sapsford, 1999, p. 227). The last question in Section 2 was an open question that asked the participants if they had any suggestions to improve the game. Section 2 records qualitative data because it deals with the perceptions of the participants. Therefore, qualitative methods are used to evaluate these responses. Quantitative methods were used to evaluate Section 1. The entire questionnaire was reviewed by a statistical consultant to ensure that quantitative results could be drawn from it.

A questionnaire and prototype were the main instruments used for the method of this study. However, an experiment took place that would use these instruments in a manner that would produce meaningful results.

5.5.3 The experiment

An experiment was conducted to test whether the goals of the project were met. This experiment consisted of two groups, the play group and the control group.

The participants in the play group were recruited and asked to gather at the computer laboratories at the Nelson Mandela Metropolitan University (NMMU) to partake in the experiment. These participants were informed about the experiment by means of the university email system. The email informed the participants that they would be testing a computer game and that they would receive a meal voucher, which served as remuneration, if they participated. Participants were told that they were merely testing a game because it could be much less enjoyable for them if they knew that they were supposed to be learning something from the game.
Before the participants started to play the game they were informed that those who achieved high scores would receive additional remuneration. This was done to prevent the participants from merely completing the game, without concerning themselves with playing it well. Players were encouraged by the additional remuneration to understand the game.

The participants were given instructions on how to copy the game from the network and how to get started with the game. They were required to play the game once and complete the questionnaire. An alternative to this approach would be to first let the participants complete the questionnaire, play the game and then complete the same questionnaire again. The advantage of this approach would be that if the ‘before and after’ questionnaires were compared, it would yield more accurate results because the same people were involved. However, this approach would not be feasible for this experiment because the participants would know what to look for in the game if they had already read the questionnaire and they would know beforehand that the game was educational.

Once a participant had completed the questionnaire, that participant was encouraged to play the game again, but the participant was given the clear option to finish his/her involvement with the experiment which meant that he/she would leave the laboratory with his/her remuneration. Participants were asked to play the game again to observe whether people would spend their own free time playing it. This would be another indication on how enjoyable it was to play the game. The internal database of the game would be able to record their scores which could be used to determine whether the same player was getting better at the game.

Observations were also used to uncover anything that was said or done to suggest how much the participants enjoyed the game. The facilitators of the experiment were instructed to record anything that could be an indication to this.

The control group who participated in the experiment merely completed Section 1 of the questionnaire which dealt with information security related questions. They did not need to complete Section 2 of the questionnaire that deals with game related questions. The experiment included a control group to verify whether education was conveyed by
playing the game. None of the students who had participated in the control group had played the game before. The questionnaires of the control group were compared to those of the play group by using statistical methods.

The statistical consultant who approved the questionnaire suggested that a minimum of 30 participants should be used in each group for the necessary statistical equations to compute. Thirty-six students participated in the play leg of the experiment while 40 students participated in the control group. All the participants were first year engineering students at the NMMU. This group was chosen because it was not difficult to get them involved and because everyone who participated needed to be computer literate. At the time of the experiment the participants had only studied for about three months towards their degree. Therefore, the group should not have been more knowledgeable on information security then regular company employees.

A t-test and chi-square statistical methods were used to compare the questionnaires of the play and control groups. A t-test was used to evaluate the hypotheses in small (N < 30) samples (Freund, 1988, p. 307) and it was used to compare the questionnaires of the two groups. A chi-square test was used because its confidence interval is applicable to small samples (N < 30) (Freund, 1988, p. 323) and it was used to compare individual questions of the two groups.

This section discusses how the research methods were designed and why they are appropriate for this study. However, every design has some limitations.

5.6 Limitations

There were some limitations that, if eliminated, could have provided more accurate results. It would be interesting to compare another group of participants who could play the game at least three times before completing the questionnaire. This could not be done because there was limited access to participants and money for remuneration.

The study could have tested whether the participants acted differently towards information security after they played the game. This would require a secondary
experiment where previous participants would be brought back to the laboratory. This was not done because of time and difficulty that this would incur. Therefore, it was decided that a behavioural investigation of the impact of the game would fall outside the scope of this project.

The results of earlier evaluation cycles of the prototype focused on what type of instructions people were likely to read. It would have been interesting if the database could record for how long participants had been reading educational content. This would give an indication to how effective the educational content was presented to the participants. This was not implemented because of time constraints.

Not all participants, who played the game multiple times, could be identified in the database as the same player. This was largely due to the fact that the participants’ anonymity needed to be protected. Therefore, the participants were required to enter on what computer they were seated in the game and on their questionnaire. Some participants entered this information incorrectly or illegible.

The participants could have been interviewed after they played the game to gain greater insight onto how enjoyable and educational the game was for them. This could not be implemented because of time and management constraints. Management constraints would include acquiring more experiment facilitators to carry out the interviews and stopping participants from leaving at the same time.

It would have been beneficial to acquire company employees from various backgrounds to be the participants for the experiment. This could not be arranged because of time and money constraints.

It would have been beneficial to acquire the help of educational experts to review the game before the final experiment. Unfortunately, access to these experts could not be gained.

Despite these minor limitations, the methods used were appropriate for this study and should be effective enough to yield interesting results. To ensure that legality would not be a limitation for this study, ethical considerations were explored.
5.7 Ethical considerations

Ethical clearances needed to be acquired for the final experiment because students are a sensitive group at the NMMU. The Research Ethics Committee (Human) or REC-H committee is responsible for granting ethical clearance at the NMMU. They reviewed this studies research methods and granted ethical clearance for it.

They specified that anonymity needed to be ensured. This was achieved by making no recordings of the participants on their questionnaire or to their game session. The email list and replies did include their identities. However, they remained anonymous throughout the experiment. They were only required to fill in the computer they were seated at on the questionnaire and game session. The high scores of every game were linked to the alias of the player.

The participants needed to sign a consent form that informed them of their rights during the experiment. The fact that their actions on the computer were going to be recorded was included in the consent form. It also stated that this study was approved by the REC-H committee, that participation was completely voluntary and that participants would remain anonymous.

5.8 Conclusion

This chapter discussed the methods of this project and why they were used. In short, an experiment was designed that consisted of a (game) prototype, questionnaires and observations. These were used to verify whether the game was educational and/or enjoyable to play.

Hevner et al.’s (2004) guidelines of design-science and the prototyping development life cycle were used to ensure that the prototype was designed according to researched methods. A single research method may not provide suitable rigor for this study. Therefore, several methods were used within the experiment to ensure that interesting results should be obtained. Educational aspects were determined by the statistical measurements from the questionnaire. If no clear conclusions could be attained from it
then the recorded actions of the players in the database could be inspected. The motivational aspects of a game are difficult to measure accurately. Therefore, the players were asked questions in order to evaluate the motivation of the game, their actions were observed and they were presented with the opportunity to play the game in their own time.

The next chapter examines how the questionnaire and prototype were implemented in the experiment.
Chapter 6: Implementation

6.1 Introduction

The success of any piece of software depends, heavily, on how well it is implemented. This is especially true for educational games, because it needs to be educational as well as entertaining to play (de Castell & Jenson, 2003). Design techniques as applicable to educational games, as discussed in Section 5.5.1, play an important part in educational games. However, these techniques should be implemented in a way that engages the players of the game. Therefore, the actual implementation of the game according to these techniques is important and it should be discussed in detail for the prototype used in this study.

The rest of this chapter explains how the prototype (game) used in the final experiment was implemented. The implementation process started with selecting educational content and developing a way to express that content as part of an educational game. To ensure that the game was ready for the final experiment it went through several evaluations.

6.2 Selecting the educational content

Careful consideration needed to be taken to decide what content the game would cover. Not only should this content include relevant knowledge about information security, the content should also be relevant to the target audience of the educational program as discussed in Section 3.7.

Van Niekerk & von Solms (2007) state that password protection, viruses and email usage should definitely be included in this type of a program. Deloitte (2009) identified the most common external security threats in their annual global security survey (Deloitte, 2009, p.31). These results are summarised in Table 6.1.
<table>
<thead>
<tr>
<th>Breach</th>
<th>One occurrence (%)</th>
<th>Repeated occurrences (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email attacks (i.e., spam)</td>
<td>10</td>
<td>24</td>
</tr>
<tr>
<td>Phishing/Pharming</td>
<td>7</td>
<td>22</td>
</tr>
<tr>
<td>Viruses/worms outbreaks</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>Employee misconduct</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Spyware</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>External financial fraud involving information systems</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Social engineering</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Physical threats</td>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 6.1: Top 8 repeated external breaches experienced - Adapted from Deloitte (2009, p. 31).

Table 6.1 indicates the percentage of single occurrences of threats to repeated occurrences of threats. Some of the results of single occurrences are close to repeated occurrences for the same threat, for example ‘Employee misconduct’ is 11% for single occurrences and 11% for repeated occurrences. “Indicating that, after the first occurrence, many companies were able to deal with the issue to prevent repeated occurrences” (Deloitte, 2009, p. 31). However, some of the threats, such as ‘Email attacks’, have a much higher percentage per repeated occurrences when compared to percentage of single occurrences.

Table 6.1 is arranged from the threat/breach that has the highest percentage of repeated occurrences to the lowest. The top repeated occurrences are those that companies find it more difficult to prevent. Therefore, these threats will be further examined as they should be dealt with in the implementation of the prototype. The following sub-sections discuss the threats identified in Table 6.1 and why they are difficult to prevent.

### 6.2.1 Email attacks (i.e. Spam)

Email attacks are the most occurring external security breach according to Deloitte (2008, p31). Any unwanted email received could be classified as an email attack. Spam is a large amount of unwanted emails.
Companies suffer from spam because employees might spend a substantial amount of time filtering through unnecessary emails. However, email attacks are typically not malicious. Therefore, one might argue that email attacks are not a threat to information and should not be listed in Deloitte’s survey. However, email attacks can lead to more harmful security breaches such as viruses and/or phishing (Brown & Howe & Ihbe & Prakash & Borders, 2008), which is discussed later in this section.

Employees can only receive email attacks if their email addresses are known by a secondary party. Many employees reveal their email address to secondary parties by registering on websites. Typically, registering on websites is not a requirement to carry out one’s job. Therefore, email attacks may be a result of employee misconduct, which is discussed later in this section. Employees should be educated on the dangers of such misconduct.

### 6.2.2 Phishing/Pharming

Phishing is when an email ‘lures’ a recipient to give away some of their personal information. The email involved claims from a perfectly legitimate person asking the recipients to enter some of their personal details on a website (Stamm & Ramzan & Jakobsson, 2007). The email links the recipient to a hoax website. The hoax website is often made to look exactly like the legitimate website that it is impersonating.

Phishing is often used to gain access to people’s bank accounts. In this scenario a person would receive an email from the ‘bank’ which indicates that their database, for example, has become corrupt and that if the recipient wants to continue to use online banking then he/she must enter their card and pin number at the linked website. The linked website is created to look exactly like the website of the bank. If the recipient enters his/her password then the phisher would gain access to his/her bank account along with his/her funds. A phisher can send the same email to as many email addresses as he/she desires.

Phishing relies on tricking the recipients to give away their information. It takes advantage of the users’ trust in computer systems. An untrained user might say that the
system told him/her to enter his/her bank details, not realising that in reality almost anyone can email them anything.

Pharming is similar to phishing, except that no emails are involved. A hoax website will exist that impersonates a real website or organisation. Persons may stumble across these websites by using a search engine, or by entering what they think is a legitimate web address. Pharming can be made more difficult to detect by changing router settings (Stamm & Ramzan & Jakobsson, 2007).

An example of pharming could be someone who wants to make a booking at a hotel. That someone finds the 'hotel’s website' through a search engine not knowing that it is a fake. Once that person makes a booking on the website and enters his/her credit card number the 'pharmer' has gained access his/her bank account. Pharming, like phishing, takes advantage of human misconceptions.

6.2.3 Viruses/Worms outbreaks

Computer viruses are programs that infect computers with malicious objectives. Viruses often use up processing power which slows the infected computers down. Viruses are capable of preventing an infected computer from starting up. Other malicious objectives of viruses include: information theft, rendering hardware useless and corrupting software.

Typically, viruses spread by means of computer networks. Most viruses are made to fulfil their objectives without the users knowing about it. This way a virus may remain secret so that it can spread to more computers. The first step towards removing a virus would be to gain knowledge of its existence on a computer or network.

Viruses need to be attached to some form of data in order to spread. This could be any file that is transferred from one computer to another, which would include email attachments (Moir, 2003). Therefore, in a computer network a virus cannot spread from one computer to another without a file being moved from one computer to another.
Worms, on the other hand, are similar to viruses with regards to malicious intent, but they can spread across computer networks, by themselves, without being attached to host files. Both viruses and worms can be removed from computers by using anti-virus software.

6.2.4 Spyware

Spyware, similarly to viruses, is software that spreads to computers through data communications. Spyware usually aims to collect information from a computer and then sends that information back to its creator (Moir, 2003). Changing computer settings is another objective for some spyware programs.

Anti-virus programs do not always detect spyware although, there does exist security programs, which will handle both virus and spyware threats. Usually, however, two separate programs will be used to keep a computer free of harmful programs. These security programs need to be updated regularly to be able to detect newly developed viruses and spyware (Moir, 2003).

6.2.5 Employee misconduct

Employee misconduct is a general security threat. However, employee misconduct can be viewed as a knowledgeable action that an employee performs that includes the use of a computer system in an incorrect manner. Therefore, incorrect use of passwords, emails and the Internet can be viewed as employee misconduct.

Organisations typically have very open and strict policies about password protection, proper email usage and how employees may use the Internet. However, some employees choose to ignore these policies. Employees often ignore company policies because they do not know how important it is to follow them. By not following these policies, employees incur several risks to organisations. The following paragraphs discuss some of these risks.
**Password protection**

Password protection involves selecting a suitable password and keeping it a secret. A suitable password for computer systems is one that is easy to remember, but difficult to guess. Yan, Blackwell, Anderson & Grant (2004) states that it is difficult to persuade users to use suitable passwords even if they are taught how to do so.

Symbols and numbers should be included in one’s password, which would make the password difficult to uncover by hacking programs. If a hacker knows the password of an employee then all the information that that employee has access to, is at risk. The hacker is then able to copy and manipulate information as the employee of the organisation. This gives the hacker the power to impersonate the employee on the network of the company. It is often the case that a hacker only needs one password to infiltrate the information of the entire company.

**Email usage**

Employees should not open emails from anyone they do not know, emails such as these should be deleted immediately. Furthermore, they should be trained to identify emails that are from illegitimate sources. Phishing, spam and virus infections could be caused by improper email usage. ISO 27002 (2005) describes the controls that should be implemented on all electronic messaging in Section 10.8.4, which includes email.

Employees should refrain from using their company email address for personal business. This should lessen the probability of threats to occur. However, employees should be aware of the company email policies and be taught how to follow them.

**Internet usage**

Employees of companies should be careful of how they surf the Internet. Viruses or spyware can be loaded onto a computer by browsing the Internet or by downloading software form the Internet. Viewing certain content on the Internet is a criminal offence and employees may be prosecuted for doing so.
Again, employees should refrain from using the Internet services of the company for personal usage to lessen the probability of threats. They should be aware of company policies that influence the way they may use the Internet (Young, 2010).

Employee misconduct is a problem which many companies face. However, home users can also benefit from being knowledgeable of these issues in order to protect their personal computers.

6.2.6 External financial fraud involving information systems

It is easier to hide one's identity when one uses information systems to communicate. Criminals can use this to their advantage as they try to steal money from businesses without getting caught.

South African law views fraud as “the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another” (Snyman, 2002). Take note that, therefore, fraud involves an intentional misrepresentation with the aim to cause harm.

The risk of external financial fraud can be greatly reduced if an understanding of “how the technology works” and “how the technology can be exploited” is obtained. Companies should ensure that the people they do business with are in fact who they say they are.

6.2.7 Social engineering

Social engineering is when a hacker gathers information from someone with the intention of committing a cyber crime with that information. One way of performing social engineering would be to call people via telephone and asking them about their personal information. Social networking programs, such as facebook or Mxit, are popular mediums for social engineering attacks. Phishing can be used as a social engineering technique through these programs (Brown et al., 2008).
Social networking programs enable their users to ‘chat’ to their friends and with other people across the world. A level of trust can quickly develop between people chatting over the Internet. Once some form of trust is established it is easy to be tricked into giving out information. Users of social networking programs should be very wary of how their information can be used if it falls into the wrong hands. They should also keep in mind that some information should not be revealed to anyone.

The information gathered by social engineers can be used to deduce user passwords, reveal company secrets or commit identity theft. The seriousness of these crimes emphasises how important it is to keep personal information secret.

6.2.8 Physical threats

Physical threats to computer systems can include theft of technology and also tampering with physical technology used for security. Physical technology used for security can include: code detectors, biometric scanners and RFID detectors. All of these security technologies can be used to prevent unauthorised persons from accessing rooms or containers. ISO 27002 (2005) describes the controls that should be implemented on physical equipment in Section 10.8.3.

It should be noted, from examining Deloitte’s top eight recurring external security breaches, that there are several ways to access information without physically stealing the medium that the information is stored on. Some researchers claim that it is much easier to gain information through people. This supports the argument that people are the weakest link in the information security chain.

The eight threats discussed above offered an appropriate base for the educational content for the game. However, some changes needed to be made to the list before it could be used for the game. The next section discusses how the content was converted to suit a game prototype.
6.3 Transforming educational content into game content

In order to place the threats identified in the previous Section into the game, the threats were somewhat refined to fit the purposes of this study. This refined list of threats served as the educational content of the game. The content of the game was conveyed through game scenarios. The following sub-sections describe these two steps.

6.3.1 Refining the list of security threats

The list of security threats identified by the previous Section is:

- Email attacks (Spam)
- Phishing/pharming
- Virus and worm outbreaks
- Spyware
- Employee misconduct (Password protection, proper email and Internet usage)
- External fraud involving information systems
- Social engineering
- Physical threats

Not all of these threats are as applicable to home users as they are to employees of companies. This project highlights the importance of home user education in Chapter 2 and it was decided that the game would not make a distinction between these two groups. Therefore, the list of threats mentioned above, needed to be refined.

Most of the threats are applicable to home users except for ‘employee misconduct’ and ‘external fraud involving information systems’. ‘Physical threats’ is arguably not as
important to home users as it is to employees. These threats should be examined individually to decide how they would fit into the content of the game.

Employee misconduct was broken down into ‘password protection’, ‘email usage’ and ‘proper Internet usage’ in the previous section. Email and Internet usage is a broad area which can relate to technical and operational controls. Operational controls dealing with these two threats are covered by other threats in the list. Technical controls may be enforced on employees by means of technology. The most important aspect of education under ‘employee misconduct’, for the means of this project, is ‘Password protection’. It is not essential for home users to configure their computers to be secured with a password. However, they may still need to know how to secure their Internet and email passwords as well as any passwords needed to access websites.

External fraud is mostly a case of a client of a business posing as someone he/she is not. This is not something a home user is likely to encounter. However, concepts of using information systems to hide one’s identity are covered under ‘phishing’ and ‘social engineering’. Home users and employees should be able to learn the lessons related to fraud through these two areas alone.

Physical threats are only targeted at home users in exceptional cases. For instance, burglars are more likely to break into a house to steal physical objects instead of stealing credit card numbers. Physical threats would be the only physical control in our list, which is otherwise comprised of operational controls. People do not require as much education about physical controls. Therefore, our education program will not teach learners about physical threats.

By changing the naming of ‘email attacks’ to ‘spam’, dividing ‘phishing/pharming’ as separate concepts and generalising ‘virus and worm outbreaks’, the following simplified list remains:

▲ Spam

▲ Phishing
This is the final list of content for the game. All of the listed security threats can be mitigated, or at least lessened in severity, if people are educated about the threats and their consequences. People are more likely to prevent security threats if they understand why they need to do it. Therefore, each of these concepts needed to be conveyed through the game. In order to achieve this game scenarios were created for the concepts.

### 6.3.2 Creating game scenarios

Once the final list of content was decided upon several steps took place to incorporate it into the game and the questionnaires in the final experiment.

The concepts that need to be understood by the learners, for each content item, were identified. For instance, for spyware the learners were taught what it was, how it was different from viruses and how to prevent/remove them from your computer. Concepts such as these were identified for each item of the content.

These concepts were used to create the questions contained within the questionnaire of the experiment. The questionnaire contained two pharming, five phishing, four spyware, three spam, ten virus, seven password and five social engineering related questions. Some questions related to multiple subjects. All of the questions were multiple-choice. These questions comprised Section 1 of the questionnaire. The questionnaire is added as Appendix A. The questionnaire contained yes/no question for some of the content, which is why the questionnaire contains more questions for some content items than others.
It was decided that practical training should be included in the game as well as textual information that the players could learn from. The questions in the questionnaire were covered in the game by using scenarios. All the scenarios in the game were done through a computer simulation. Therefore, players should be able to identify the correlation between a real world scenario and the one faced during the game. If the player worked through the scenario correctly then he/she proved that he/she understood what was being taught by that scenario. However, if the player worked through the scenario incorrectly then he/she was textually informed on his/her mistake and what he/she should learn from it.

Section 6.4.3 provides an in-depth discussion on how a scenario in the game works and how exactly a learner gains knowledge thereby. Once the educational content was decided upon, the implementation of the rest of the game could take place.

6.4 Implementation of the game

To solve the problems this project attempted to address a game was developed to educate learners about information security. This game needed to be enjoyable as well. This section describes how this game was implemented.

6.4.1 Overview

The game is called ‘Cash City’ and it is an educational game that seeks to educate its players about information security content. Cash City is similar to the well-known board game Monopoly. It is a computer simulation of a board game and the ultimate goal of the game is to make as much money as possible. The game hides some of its content, as discussed in Section 4.5.3, so although the game is about information security, there is a big money management aspect attached to it. Its main screen is depicted in Figure 6.1.

Cash City is a computer game based on a board game. It follows the movement rules of a regular board game. Players move around the board by rolling dice. The number the dice roll determines what square the player moves to. Different squares on the board have different functions. The squares are grouped into five groupings. These groupings
consist of Houses, Way to work, Businesses, Way back home and Mega stores. All the Houses are on the left side of the board, all the Businesses are on the right side of the board, the Way to work is at the bottom side of the board while the Way back home is on the top side of the board. The Mega stores are on each corner of the board.

![Figure 6.1: Main window of Cash City](image)

When a player moves to a square on the board, he/she is presented with options that are displayed in a panel to the lower right of the window. If the player is on a square with a Store on it, the main option displayed would be to enter that store. If the player is on a Business square, the main option displayed would be to go to work. If the player is on a House square, the main option displayed would be to sleep in order to start the next day. Completing a cycle around the board is equal to one day in the game.

The upper left panel of the window displays the top scores that players have obtained. There is a button titled “View Full Scores” that opens a new window where players can view all the scores recorded in the database of the game. The score of a player is calculated by adding the amount of money they obtained with each asset they own, which is converted to a monetary value.
The lower left panel of the window shows the statistics of the current game. Statistics such as “Money on hand”, “Assets” and “Current day” are displayed. The rest of the panels on the main screen provide general information about the game.

6.4.2 How the game is played

The player is presented with a short “How to play” tutorial when he/she starts playing the game. After completing the tutorial, he/she is introduced to the background story of the game. The player has the option to buy assets such as a “House”. Before the player can roll the dice for the first time they must acquire a job interview from the “Daily news” paper that appears at the start of every day.

After a job interview is obtained the player can roll the dice for the first time. If the player goes to a Mega store, determined by the dice roll, that player can buy goods on sale. This makes the Mega stores more special than regular stores. Players may spend as much money as they want on any number of items offered by the stores that they ‘land’ on.

The player needs to go through the “Way to work” squares before that player can start with his job. The “Way to work” squares are either Malls or Risks. Mall squares give the player the option to buy items from two different stores. In addition to these stores Mall squares also contain a Grocery store. Players need to buy food at these Grocery stores regularly. This was designed into the game to ensure that the player must spend some money and because a money management game should include some expenses.

Risk squares present the player with a random event, which is similar to the Chance cards in Monopoly. These random events include getting mugged or receiving a promotion. There is a higher chance that the player will face an event that will result in them losing money. Random events were handled in this fashion in the game because in an educational game it is very important to justify both reward and consequences. Players must understand that a random event happened because they landed on a certain square and not because they made an information security related mistake.
The player reaches the Business squares after going through the “Way to work” squares. The player rolls the dice until he is on the square representing the business he has made an interview with. At this square the player does a short interview that consists of a series of questions. How many of these questions are answered correctly will determine how much money he/she will earn at that job. After the interview, the players must login to their workstation to complete their work for that day. The workstation in the game is a simulation of a computer. The next sub-section discusses this simulation as well as how the game conveys educational content.

The “Way back home” squares are between the Business and the House squares. These squares work exactly the same as the “Way to work” squares.

When the player reaches the House squares, he/she may roll the dice until he/she reaches a House he/she owns. Once there, the player is required to “chat” with his/her “friend” on a social networking application, which is discussed in the next sub-section. After communicating with his/her in-game friend he/she can sleep in order to start the next day in the game. At home he/she can decide to use items that were bought previously from the stores visited. The next sub-section explains how educational content is learnt through playing the game.

### 6.4.3 How the game conveys educational content

All the educational content in the game is learnt either when the player is at the Business square where he/she has a job or at the House square where he/she sleeps. ‘Social engineering’ is taught at the House squares and ‘password protection’ is taught at the Business squares. All the other educational content is conveyed at the Business squares as part of missions.

Every day, in the game, the player must attempt to complete his/her job for that day. These jobs can be expressed as missions and all of them are related to information security. To complete the mission successfully the player must correctly implement information security practices. If this is not attained then he/she is educated about
information security and what should have been done. All of the missions are in the computer simulation within the game.

Figure 6.2: Desktop simulated in Cash City

This computer simulation, depicted in Figure 6.2, contains Internet, email, anti-virus, anti-spyware and phoning software as well as a business associate list. The players receive email every day that contains their job related tasks, which start the mission. After the day's mission is completed, the players logout of their workstation and roll the dice. At this point, the players will receive either a “Congratulations” or a “Fired” message. The Congratulations message indicates that the player completed his/her work successfully, received money for their work and, therefore, did not place the information of the company at risk. The Fired message, on the other hand, signifies that the player placed the information of the company at risk in some way, does not receive money for his/her work and needs to find another job. The message instructs players about what mistakes they have made, what they must do to rectify them in future and how the mistakes relate to information being threatened.
To explain what the players should do and how they learn by using the computer simulation an example will be worked through.

The players open their email program on the computer simulation and receive an email from their boss. This email is depicted in Figure 6.3.

![Email Program Example](image)

Figure 6.3: The email program with an example message

The email instructs the player to browse the Internet for a quote. When he/she navigates to the website, using an in-game simulation of the Internet, he/she receives an online message stating that he/she has spyware on his/her computer and that he/she can remove it by following the link provided. Receiving similar messages on the real Internet generally means that the computer browsing the Internet is already infected with spyware. Often when someone uses the link to remove the spyware it uploads even more spyware to his/her computer. Therefore, in this mission, after the player receives the quote and sends it back to their boss they need to use their anti-spyware program to remove any spyware. This program is depicted in Figure 6.4.
Once the program is opened the players should update their anti-spyware software and scan their computer to remove the spyware they have. After they have done, so they can logout of their computer and a “Congratulations” message will be presented to them. The Congratulations message is depicted in Figure 6.5.

Figure 6.4: The anti-spyware program within the game

![Anti-Spyware Program]

Figure 6.5: The “congratulations” message

Congratulations!

You successfully completed today’s work requirements without making any mistakes. R100 will be placed into your account.
Receiving a congratulations message means that the player completed the mission correctly and, by doing so, proves that he/she understand how to react to a spyware message from the Internet. If the player did not update their anti-spyware software and scanned for spyware then he/she will receive a “you are fired” message, which means that the player did not understand how to handle this type of security threat. When he/she receives this message he/she does not earn a salary for the day and he/she needs to find work somewhere else. The “you are fired” message, depicted in Figure 6.6, provides the player with information on why they were fired, what the lesson is that they should learn from this and detailed step-by-step instructions on what to do against similar threats. The “you are fired” message is the primary conveyor of educational content within the game.
This concludes the example of how missions work within the game. Password protection and social engineering are not taught through the game by using missions. However, they also use “congratulations” and “you are fired” messages.

Password protection is introduced in the game when the player logs into their workstation for the first time. He/she is required to select the default password to successfully log into their workstation, but is required to change his/her password before he/she leaves work that day. If he/she did not change their password to a secure one he/she will receive a “you are fired” message when they leave work. If he/she did not complete the daily tasks securely then he/she will receive an additional “you are fired” message.

Figure 6.7: The “Create New Password” window
In the game passwords are chosen and entered as a collection of bits of information, for example the player can select his/her password to be “the type of car they drive” followed by “their house number” and lastly “the star symbol”. All these bits of information are predefined. They are grouped into letters, numbers and symbols. Passwords were implemented as bits of information because this made it possible for players to reveal sections of their passwords in the game. Players could reveal the information in their password by falling victim to social engineering attacks.

Social engineering attacks can reach players of the game when they are at home. Before the player goes to sleep he/she must communicate with a “friend” Ted over a social networking application, which is similar to MXit, the popular mobile phone texting program. Ted will ask where a bit of information is in their current password in exchange for an investment opportunity. The idea is to give Ted information that the player has not used in his password to obtain some extra money. If the player does reveal information contained within his current password he will receive a “you are fired” message the next morning and will not receive money from Ted’s investment. If the player does reveal information that is not contained within his password he/she will receive some extra money the next day.

The way in which educational content is conveyed through the game, as discussed in this sub-section, was designed by following researched teaching methods. The following sub-section explains how these and other teaching methods were implemented in the game.

### 6.4.4 Teaching methods

Section 5.5.1 identified the design techniques that the game would use. The techniques that pertained to teaching were: simulation, reading/dialog, acquisition/testing, replayability and “force players to learn”. All of these techniques were implemented in the game.

As discussed in Section 6.4.1 the game simulates a day in the life of a person who uses a computer at work and at home. In addition to this it simulates a desktop environment as discussed in Section 6.4.2. Both of these simulations are environments that the players
should be familiar with and enables them to learn from feedback generated by the game. The desktop environment generates practical feedback that allows the player to learn how the technology works. Textual feedback is also provided.

Reading/dialog houses the textual feedback that the player receives. The player receives textual feedback from the “you are fired” messages discussed in the previous sub-section. A large red font stating “You are Fired!” is used to grab the attention of the player. The details in the message provide educational content. This message forms part of the acquisition/testing design element.

Acquisition/testing is used in the game to evaluate whether the player is learning educational content. When a mission is completed successfully the player understands the principles regarding the missions and is, therefore, rewarded for it by receiving money and a “congratulations” message. On the other hand, if the mission is not completed successfully then the player must receive consequences for his/her actions and he/she is presented with educational content by the “you are fired” message.

The game should force players to learn educational content. The player should not be able to receive a high score in the game without learning its educational content. This was implemented by greatly rewarding players who complete their daily jobs securely. The score of the players is determined by how much money is made and that is determined by how many jobs they complete, because that is the primary way players may acquire money in the game. Therefore, although there are other ways to make money within the game the emphasis is placed on completing jobs, which educates them about information security.

The game was created with the idea that it could be played several times by the same player. If the player continually plays the game he/she will continually be reminded of the risks associated with information security. For this reason, it was decided to implement a grading system within the game. As a grading system is tied strongly to the motivational aspects of the game it will be discussed in the following sub-section.
6.4.5 Motivational aspects

Along with the teaching methods, motivational aspects were used to create an educational game. Section 5.5.1 identified graphics, hidden content and a grading system to calculate competitive scores as the design techniques the game will use to be enjoyable.

Graphics were included in the game to give players a visual representation of its content. The use of graphics within games should not be underestimated, especially when it is considered that pictures are always more attractive to people than text. Windows forms were used as the platform of the game, and although not as attractive as 3D graphics, it did provide a clear environment for players to interact in. The whereabouts of the player is visually represented in the middle of the game board as depicted on Figure 6.1. Icons and a background are used to create the desktop environment as depicted on Figure 6.2. Many other icons and small pictures are used throughout the game to make it attractive.

The fact that the game is an educational one was slightly hidden from the player. At the start of the game there is no reference made to information security or even computer training. It is only after completing a job at work that the player should notice that the game focuses on these issues. By this time the player already knows how the game works and has been presented with the money management aspect of the game.

Cash City uses a grading system that enables players to receive a score after they have completed the game. The score of a player is calculated by adding up all the assets’ monitory value with all the money they own. Scores are recorded by the game, which make them comparable. When players view their previous scores, they are often motivated to play the game again to achieve higher score. Players may view the high scores of the other players, which motivate them to play the game to receive the highest score. This could also motivate the players to play the game repeatedly as discussed in the previous sub-section. The top 10 player scores can be seen in the top left corner in Figure 6.1. By clicking the button underneath it a window with the complete list of scores will appear.
After the game was developed by using these design techniques, evaluations were performed to ensure that they were implemented adequately.

### 6.5 Preliminary evaluations

Before the final experiment took place preliminary evaluations were performed to test whether the game was ready. These evaluations are part of the prototyping development life-cycle as discussed in Section 5.5.1. By continually evaluating and revising the prototype it should evolve into the finished product.

The first evaluation was conducted on five postgraduate students and four lecturers all of whom specialise in the field of information security. The main aim of this study was to determine if the game would be usable and understandable for the final participants. They were asked to note any errors while playing the game and whether the educational content was adequately conveyed through the game. A questionnaire with open questions was used to capture the feedback of the participants. An interview between the participants and the researcher was conducted as the participants played the game.

It was decided to conduct a secondary evaluation after the results of the first evaluation were addressed. A group of 43 fourth year students who attend information security lectures participated in this study. Its focus was to determine how usable the game was and whether it still had any errors. Another focus was to determine what type of instructions people prefer to use. The questionnaire used in this study included open and multiple choice questions.

A lot of errors were captured by the two evaluations and some interesting results were discovered. The detailed results for these evaluations are discussed in Section 7.2. The prototype was deemed to be understandable enough for the final experiment after the results of the evaluations were addressed.
6.6 Conclusion

Careful consideration was needed to select appropriate content for the game and the questionnaire. All the topics chosen have been identified by research as being current information security threats. Deloitte's Annual Global Security Survey (2009) provided the top information security concerns that could be refined into the final list of content that the game would address.

This chapter discusses how the game was implemented to convey the list of content and to motivate learners to play it. This included multiple educational and motivational design techniques, which were uncovered through literature and argumentation. However, even if these design techniques are recognised they still need to be implemented appropriately. This chapter indicates that the first secondary objective of this study was achieved which is to develop a computer game to educate users about information security related concepts.

Preliminary evaluations were preformed to ensure that these elements are implemented correctly in the game and that the game is ready for the final experiment. This followed the prototyping development life cycle approach. The next chapter will discuss the experiment that was carried out and will analyse its results in order to recommend guidelines for future educational game designers.
Chapter 7: Results and Discussions

7.1 Introduction

The aim of experimenting with educational games was to produce meaningful results. The previous chapter discussed how the experiment was designed to do this. The rest of this chapter reveals the results of the experiment and explains what can be learnt through them.

Preliminary evaluations were conducted to ensure that the final experiment would run without major problems. Therefore, the results of the preliminary evaluations had an impact on the results from the final experiment. The final experiment used a questionnaire to gather information of the participants. This questionnaire also had a big influence on the results reached by the experiment.

7.2 Results of the preliminary evaluations

Two preliminary evaluations were conducted prior to the final experiment. The first evaluation was performed by five postgraduate students and four lecturers to indicate whether the prototype was usable enough for the final experiment. The design of this evaluation is discussed in Section 6.5.

The results of the first evaluation revealed that the game could be more usable and that it did contain errors. Very little was relayed about its educational content. It revealed that people would rather skip long lists of instructions when it took them a long time to read. The participants did not really use the help features of the game, which were accessible through a question mark at the top right corner of every window. This made the game difficult to understand especially when it was played for the first time.

The game was changed to be more user-friendly and intuitive, and all the identified errors were addressed. A major concern was that the participants did not read important instructions which inhibited them from progressing in the game. It was decided to
change these instructions to short questions to motivate players to read the information. By asking players to respond to short questions should focus their attention on the information.

Initially, players struggled to understand the game. A 'help page' was introduced to help players understand the game. The help page is a hardcopy that would be given to future players of the game which contained short instructions on how the game should be played.

The second evaluation was performed by 43 fourth year students to determine whether the game had been changed to be usable enough and whether people would read the instructions of the game.

The results revealed that the game was usable enough except for a few errors that still existed within the game. How the participants indicated to have read the instructions of the game yielded more interesting results.

Fifty-one point two percent of the participants indicated that they used the help features in the game, 100% of the participants indicated that they read every item in the short question section at least once and 76.7% of the participants indicated that the help page did in fact help them to get started with the game. Therefore, it was deduced that people are much more likely to read instructions when they are presented to them as short questions and a help page would potentially be 25% more effective than the usual help features. It should be noted that normal help features for a game such as this may take hours to complete while the help page was written in about 20 minutes.

The few remaining errors were addressed before the final experiment took place. It was decided that the prototype was ready for the final experiment.

### 7.3 Results of the experiment

Thirty-six first year engineering students participated in the experiment. These participants played the game and immediately afterwards completed a questionnaire.
The results of the questionnaire are presented in the following section. A detailed design of the experiment is examined in Section 5.5.3.

After completing the game once, the participants were encouraged to continue playing the game, but were given the option to leave with their remuneration. It was noted that at least 17 participants (47.2%) voluntarily played the game a second time. It should also be taken into consideration that this experiment was conducted on a Friday afternoon before a long weekend.

Dialog that indicated interest was observed by the researcher, which included: “Did you make the game? Did you make it by yourself?” and “Where can I get the game? Can I copy it onto my flash drive?” Some comments that were recorded by the questionnaire included: “It is a good game to make a person remember things,” “...it taught me how to protect your PC and how to create a good and strong password.”, “Enjoy the game it make you wise in the workplace and how to use your money.” and “...its very interesting and makes us use our minds.” (Sic)

![Figure 7.1: Comparison of games scores to the amount of security mistakes made by players](image)

Figure 7.1: Comparison of games scores to the amount of security mistakes made by players
A database recorded information as the participants played the game. The game scores in the database were examined to uncover meaningful information. It should be noted that due to incomplete games, human error, people moving between PCs and illegible handwriting meant not every game could be examined in this regard and not every score could be linked to the participant who completed a questionnaire. The database stored the number of security mistakes that each player made, but scores were used for questionnaire comparison instead, because they reflect how much the players understand the game and its content. However, the amount of player mistakes was compared to the scores to indicate whether fewer mistakes would result in a higher score. Figure 7.1 reveals that fewer mistakes did in fact result in higher scores.

The amount of mistakes were grouped into ‘15 to 19’, ‘9 to 14’, ‘4 to 8’ and ‘4<’ to allow scores to be averaged to be representative of the groupings. Scores were used for the remaining two comparisons in this section.

The average score players received after their first round of game play was compared with the average score players received after their second round. The average score players received for the first round was 1481 from 32 participants. The average score for the players who completed a second round in the game scored 2679 from 10 participants. This yields a 55% increase from the first round to the second round.

Participants who obtained an 80% or higher score in the questionnaire scores were reviewed to indicate whether a good score in the game meant that the participants would learn more about information security. The average score for those participants was 2156 (11 participants) whilst the average score for all the identified participants was 1481 (32 participants). Only four participants who scored above 2000 points in the game did not reach a score of 80% for the questionnaire.

### 7.4 Results of the questionnaire

There were 76 students who completed the questionnaire. All of these participants were first year engineering students at the Nelson Mandela Metropolitan University. Thirty-six students played the game before they completed the questionnaire (the play group)
while 40 students only completed the questionnaire (the control group). The design of the questionnaire is discussed in Section 5.5.2.

Section 1 of the questionnaires of the two groups was statistically compared, by means of a t-test, to uncover by what degree the questionnaires differ. The t-test yielded no statistical significance.

Individual questions between the questionnaires were compared, by using a chi-square statistic, to uncover by what degree the answers differ. This test yielded no statistical significance for the 33 questions in Section 1.

The average score received for the questionnaire by the play group (36 participants) was 73%. The average score received for the questionnaire by the control group (40 participants) was 72.8%.

The sub-sections of the questionnaire were examined for any notable differences. The sub-sections of the questionnaire are: “Definitions”, “Short questions” and “Scenarios”. The scenario questions revealed a 7% increase for the play group. The other subsections did not reveal any notable difference.

The questions in the questionnaire were grouped by their information security topic. This would indicate whether certain topics were taught more effectively by the game. The information security topics covered in the game are: pharming, phishing, spyware, spam, viruses, passwords and social engineering. The play group scored an average of 48.6% for pharming related questions whereas the control group only scored 37.5%. The other topics did not reveal any notable differences.

Individual questions were examined to determine which questions were answered better by the play group.

- Question 1 “What is pharming?” was answered correctly by 38.9% of the play group, while the control group only scored 22.5% for this question.
• Question 6 “How can you prevent unwanted emails from reaching you?” was answered correctly by 30.5% of the play group, while the control group only scored 10% for this question.

• Question 16 “A virus checker aims to remove both spyware and viruses from a computer?” was answered correctly by 50% of the play group, while the control group only scored 37.5% for this question.

• Question 21 “Should a GOOD password contain symbols?” was answered correctly by 91.6% of the play group, while the control group only scored 75% for this question.

• Question 32, which was a scenario question concerning a virus causing an operating system error was answered correctly by 91.6% of the play group, while the control group only scored 72.5% for this question.

The play group had to respond to Section 2 of the questionnaire which consisted of questions that inquired how much they enjoyed playing the game. The first question indicated how much they enjoyed the game, where one point is allocated for “Not at all”, two points are allocated for “a little”, three points are allocated for “a reasonable amount” and four points are allocated for “a lot”. The average score for this question among the 36 participants was 3.4. The second question asked the participants if they would play the game at their university in their own spare time. All the participants answered “yes”. The third question asked the participants if they would play the game at home, if it was given to them free of cost. For this question, 33 of the participants (91.6%) answered “yes”.

The following section discusses the results of the experiment and the questionnaire.
7.5 Discussion of results

The results reached in the previous section need to be analysed to indicate how it addresses the goals of the project. The following sub-sections discuss these results as they pertain to the goals and what can be learnt from them.

7.5.1 Educational content

The experiment tested how educational the game was. The primary technique used to measure education was the questionnaire that the participants completed after they played the game. Two statistical methods were used to compare the results of the play and control group’s questionnaires. No statistical significance was found in the comparisons meaning that the game did not, notably, help the players to answer the information security questions in the questionnaire.

The final experiment was the first evaluation to verify the educational factors within the game. Therefore it should be expected that the balance between education and motivation might not be at a suitable level. This does not mean that the design principles behind the game are ineffective, but rather indicates that another combination of design principles might work better for the goals of this project. Further research may be needed to deduce what the right combination of design principles is for the purposes of this study.

The educational content and the questions in the questionnaire based on that educational content can be placed under scrutiny. This is indicated by the control group who scored an average of 72.8% for the questionnaire. Therefore, the control group knew a lot about information security. Perhaps if the educational content and the questions in the questionnaire were more difficult to answer, the study could yield different results. The fact that pharming (which is not a well known information security topic) questions were answered better by the play group supports this hypothesis.

The scenario type questions were answered better by the play group. This may mean that this type of game is better suited to teaching people what to do in certain scenarios.
This project aimed to educate people to the point where they understood why they needed to take certain actions in certain situations. However, training is also an information security concern which can be addressed by educational games. Perhaps a game that trains people should be developed prior to creating a game that educates people about information security.

The comparison of the play and control group’s questionnaires did not indicate that the game was educational. However, the play group only played the game once before they completed the questionnaire. The average score of the people who played the game for a second time is 55% higher than average first time scores. A higher score indicates that fewer information security mistakes were made in the game (Figure 7.1) and a higher score in the questionnaire. Therefore, there is an indication that players learn more from the game if they play it repeatedly. This game can be further experimented upon to test whether a play group who plays the game ten times, for instance, does significantly better than the control group in the questionnaire.

Prior to the final evaluation it was suggested that the design and implementation of the educational techniques used in the game would teach the participants information security content, but the results suggest otherwise. This sub-section discusses enhancements to future experiments which may indicate that the educational techniques are suitable for a game such as this. However, the results obtained by this experiment would suggest that these techniques may not be effective for information security education. In addition to testing how educational the game is, the experiment also tested how enjoyable (or motivational) the game is.

7.5.2 Motivational factors

Questionnaires and observations were used to determine whether the players enjoyed playing the game. The questionnaire asked the participants how much they enjoyed the game from a scale from 1 to 4. The average for this question was 3.4 out of 4. All the participants answered that they would play the game at the university in their spare time and 91.6% of them indicated that they would play the game at home if it was given to them free of cost.
These responses from the motivational questions in the questionnaire suggest that the motivational aspects designed into the game, as described in section 3.2.4, do indeed work and are suitable for this type of educational game. It can be argued that people will not necessarily do what they answer in a questionnaire. However, at least 47.2% of the participants did play the game for a second time although the experiment took place on a Friday afternoon before a long weekend. This indicates that people will use their own free time to play the game.

Some of the dialog observed by the experiment facilitators further promotes the motivational aspect of the game. These include:

- “Did you make the game?”
- “Did you make it by yourself?”
- “Where can I get the game?”
- “Can I copy it onto my flash drive?”

The first technique that will be discussed, which had an impact on the motivational aspect of the game, is *hidden content*.

### 7.5.3 Hidden content

The educational content in the game was hidden from the players to increase their motivation towards it. At no stage during the experiment were the participants told that the game was about learning information security content. The email sent to the participants labelled the experiment as a “play test” and the questionnaire they needed to complete was labelled “proper computer usage”. Participants could, however, figure out that the game is about information security after they played it for a while. The comments from the questionnaire suggest that the participants perceived the game to be about: proper computer usage, money management and how to keep a job. Some of the participants noticed that the game had educational value. Their comments were:
“It is a good game to make a person remember things.”

“...it taught me how to protect your PC and how to create a good and strong password.”

“Enjoy the game it make you wise in the workplace and how to use your money.”

“...its very interesting and makes us use our minds.”

As all these comments reflect positive emotions towards the game and the participants indicated that they enjoyed the game very much, strongly suggest that hidden content contributed to the motivational aspect of the game. The next sub-section discusses graphics as another motivational technique.

### 7.5.4 Graphics

Graphics are used to visually represent what is going on in games. It is generally accepted that better graphics (and sound) will result in a better game. However, some games rely more on graphics to be successful than others. Graphics were included in the game to enhance enjoyment, but it was not implemented to the same standard as those used in commercial games due to time constraints and the need to keep the interface simple for usability purposes. The graphics used were unanimated pictures and icons on a Windows Forms application. No sound was incorporated into the game because the computers in the venue of the experiment did not have speakers.

As the graphics of the game are not as good as commercial games some participants did state that it could be a possible improvement to the game. These comments asked for 3D graphics, animation and more pictures throughout the game. Therefore, the game can be improved to be even more enjoyable.

Despite the comments that the participants stated for graphics they still indicated that they enjoyed the game a great deal. Therefore, graphics is not a critical motivational factor in a game such as this and the graphics implemented are of sufficient quality. The third motivational technique discussed is competitive scores.
### 7.5.5 Competitive scores

Competitive scores were used to motivate the players to play the game again, to have an indication of how well they were doing and to make it possible to compare the scores with others. Obtaining one of the highest scores would mean that that player would get awarded with additional remuneration.

From observing the participants it became evident that they focused a lot of their attention on the scores and tried to do well in the game. They were proud to obtain high scores and compared their scores with their friends. Therefore, competitive scores were successfully designed and implemented into the game, especially with repeated play.

### 7.5.6 Repeated play

The game was made to be replayable to motivate learners to be reminded of the educational content. As players replay the game they should learn more about the content over a period of time.

The experiment did not test whether the participants learnt more from the game after playing it for a second or third time, due to time constraints. The game was designed to be played several times in a row. Therefore, further research might indicate that the game is educational although it needs to be played, say, ten times to effectively educate players.

As stated in a previous sub-section (Section 7.5.1) the 55% point increase from participants who played the game for the second time and the indication that a higher score influenced how well participants did in the questionnaire, support the notion that replayability was a successful educational technique. Replayability may be classified as a motivational technique, as well, because it was used with competitive scores. ‘Force players to learn’ was another educational technique employed by the game.
7.5.7 Force players to learn

Section 4.5.1 discussed this educational technique and its importance. It is used to ensure that a high score in the game means that players are learning educational content. Players should not be able to do well in the game if they are not learning concepts.

Figure 7.1 shows that the participants who made less information security mistakes in the game received higher scores in the game. Those who received higher scores in the game also received higher scores in the questionnaire. Therefore, this technique was properly implemented by the game. The next sub-section discusses the other educational techniques that determined how the game was played.

7.5.8 Simulation, knowledge acquisition/testing, reading/dialog (multiple teaching methods)

By comparing strengths and weaknesses of various educational techniques implemented in educational games (documented in Section 4.4) it was decided to create a simulation game that would present content by displaying text and *practically* testing whether players could do what they had learnt through reading. These three techniques acted as multiple teaching methods discussed in Section 4.3.3.

The play group answered the scenario questions better than the control group, which is an indication that they did read the text in the game which allowed them to complete game missions successfully. Therefore, it can be argued that the game trained the players to act appropriately. However, the game focused on educating the players to understand information security content to answer general questions about it, which is why the questionnaire did not contain many scenario questions.

The educational aspect of the game did not prove to be as effective as it was previously believed. Therefore, its educational techniques need to be scrutinised. As it does not appear to be due to the other educational techniques it seems as though the above mentioned techniques are to blame. Simulation, knowledge acquisition/testing and reading/dialog did not prove to be educational enough to yield statistical significant results for the experiment. They may prove to be significant enough if the game was
played several times in a row before the players completed the questionnaire. However, this can only be tested by further research.

In summary the following guidelines for educational games can be identified from the experiment:

- The use of a computer simulation in the game taught players what to do in certain scenarios;
- "Force players to learn", reward/consequences and reading/dialog techniques contributed towards the educational value of the game;
- Windows Forms may be adequate for an information security game, although other graphics and sound options could be more motivational;
- Competitive scores and playing the game repeatedly contributed towards the motivational aspect of the game;
- Hidden content can be used in the implementation of an information security game.

The following recommendations were identified that researchers should take into account if Cash City (or a similar game) is tested by future experiments:

- Participants should play the game repeatedly (the more the better) before they complete a questionnaire;
- The game should not take a long time to complete and it should be made so that players can quickly play a part of the game, and at another time they can continue to play the same game;
- The effectiveness of the educational techniques should be properly tested to verify the educational value of the game before the final experiment is conducted;
- Game play should be intuitive and only requires minimal help;
- All instructions to the players must be kept short. If this cannot be done the instructions can be transformed into questions.
7.6 Conclusion

The preliminary evaluations indicated that even students with a high degree of computer literacy benefit from using a 'help page' as they played the game. Therefore, a help page may guide players to better understand educational games. The fact that more players read the short questions than long lists of text, in the game, may help game designers to handle important instructions. The preliminary evaluations contributed towards the game being more intuitive, which resulted in a more enjoyable game.

This chapter documented the results of the final experiment/evaluation and then discussed what can be learnt from them. The individual educational and motivational techniques were analysed to determine how they influenced the results obtained.

The results indicated that Cash City was enjoyable, but that its educational value may not be at a suitable level. Therefore, the second secondary objective of the study to determine whether the game is “popular” enough for users to play it without external coercion was achieved as well as the third secondary objective to determine whether the game successfully conveys information security concepts. Indeed, the results of the third secondary objective indicated that the game was not educational. Nevertheless, interesting conclusions were extracted from the results, which brings us closer to designing and implemented a game that can educate learners about information security more effectively.

The results indicate that the game may be appropriate for user training and might be suitable for user education by further research.

The conclusions reached can be generalised to help educational game designers to create games that are not necessarily about information security. From the guidelines listed in the previous section only "Windows Forms may be adequate for an information security game, although other graphics and sound options could be more motivational" is directly relevant to an information security game. All the other guidelines should be addressed by educational games designers and researchers. These guidelines indicate that graphics and sound adequacy should be tested, before expensive alternatives are implemented.
From the recommendations listed in the previous section only “Participants should play the game repeatedly (the more the better) before they complete a questionnaire” **may not** be applicable to experiments conducted on educational games. All of the other recommendations should be taken in consideration when educational games are being evaluated. The researchers of these types of experiments should determine how applicable repeated play is for the success of their educational game.

The next chapter concludes this study.
Chapter 8: Conclusion

8.1 Introduction

The objective of this study was to indicate how computer games can be used to effectively educate users about information security. In order to achieve this objective an educational computer game about information security was developed. Furthermore, the educational and motivational aspects of the game were examined to determine how effective it is.

Various techniques designed into previously researched educational games were analysed in Chapter 4. From this analysis techniques were chosen to be designed in an information security game.

An experiment was conducted to determine how educational and motivational the game is. After the qualitative and quantitative results were examined the final conclusions could be deduced.

The conclusions reached are in the form of guidelines, which would be meaningful to other educational game developers and researchers. Only a few guidelines on the design of educational games were found in the literature review. Even fewer guidelines were uncovered for specific game genres and subject matter.

8.2 Summary

The primary objective of this research was to indicate how computer games can be used to effectively educate users about information security, as stated in Section 1.5.1. This section discusses the process that took place in order to meet that objective.

Chapter 2 examined information security, its problems and the role it plays within society. Many researchers agree that education plays a major part in protecting information, because it addresses the people who use the information, which is the
biggest threat to information. This study supports this belief by implementing an educational program. However, it also supports the idea that the general public has an increased responsibility with regard to information security in current society. Therefore, apart from being educational, the proposed program needed to be enjoyable so that the general public may willingly partake in it.

Chapter 3 discussed the underlying approaches used for educational programs about information security. Some problems were identified with current information security programs. The chapter concluded by presenting a set of criteria that educational programs about information security should adhere to.

Chapter 4 reviewed educational gaming and research that has been conducted on it. The literature regarding educational games suggests that they are difficult to design because they need to be enjoyable in addition to being educational. Furthermore, only a few guidelines were found that would help to design an educational game about information security. A qualitative content analysis was conducted to review educational and motivational techniques that education games (about any subject matter, not just information security) use. The chapter concluded by presenting factors that should be adhered to when creating an educational game that teaches information security content. These factors are built on top of the criteria uncovered in the previous chapter.

Chapter 5 discussed how the game and the experiment that tested it were designed. Hevner’s et al. (2004) design-science guidelines were used to design the game as well as the prototyping development life cycle, which consisted of three iterations. The research methodology consisted of an experiment. This experiment used the game prototype, questionnaires and observations to yield qualitative and quantitative results. The game was designed to meet the factors and best suited educational and motivational techniques that were brought forth by the previous chapter. Several limitations of the design were discussed that that if eliminated should result in a better study. These limitations are centred on having access to a variety of home users, employees and experts to further evaluate the prototype.

Chapter 6 described how the game was implemented to include the factors and techniques designed into it. This chapter also explained how the experiment was
implemented and how the information security content was chosen. Through the work in this chapter, and indirectly the previous chapters, the first of the secondary objectives of the study, which was to develop a computer game to educate users about information security related concepts, was met.

Chapter 7 discussed the results which indicated that the produced game was enjoyable, but not very educational. Therefore, it achieved the second secondary objective which was to determine whether the game is “popular” enough for users to play it without external coercion. It also achieved the third secondary objective which was to determine whether the game successfully conveys information security concepts; although these results indicated that the game was not educational enough. The individual motivational and educational techniques were examined to discuss why the experiment yielded these results. There is still an indication that computer games can be used to effectively educate users about information security, which is the thesis statement of this dissertation. Guidelines and future considerations were introduced that should produce a better game in the future. A paper describing the study which included these guidelines and future considerations was peer-reviewed and published as Monk, Van Niekerk and Von Solms (2010).

Through this process and attempting to meet secondary objectives the primary objective to indicate how computer games can be used to effectively educate users about information security was met, although effective education could not be proven, the study still indicated how future attempts could be improved.

This study did have some limitations, which included a lack of access to experts and external employees to evaluate the prototype. Education experts could have been used to ensure that the education aspect of the game should be effective before the evaluation. Employees of companies could have been used as participants in the evaluation, which is closer to the intended audience. If more time was available to complete the study these employees could be monitored, prior to the evaluation, to determine whether the prototype had any influence on their security behaviour in the workplace. Other limitations include time and development resources to develop a more functional game.
8.3 Possible Further Enhancements

Whether the game would be more educational if played repeatedly, should be investigated. If the results still indicate that the balance between motivation and education is incorrect then further research should be conducted. It would be interesting to examine whether continually playing the game would alter the way people use their computers, but this was beyond the scope of this project. Future attempts to improve the educational impact of the game should, if possible, involve researchers with a pedagogical background during the design phase, and not just information security specialists.

A different game genre can be used to create an information security game. *Adventure games* use dialog and storylines to capture audiences. A player progresses in these games by examining the situation, which involves talking to game characters and solving problems or puzzles. If an information security game was developed by following the adventure game genre then different situations, representing information security problems, can be worked through by players. On the completion of a situation the game can prompt the player about correct behaviour and similar security threats. Adventure games are suited for reading and learning. However, it does not have high replayability value as it is similar to rereading a novel. Scores are not used in adventure games, which was an effective motivational factor in this study.

8.3 Conclusion

Computer games are a fascinating method used to teach various concepts. It can be used to educate users about information security, which contributes to strengthening the weakest link in the security chain. Further research may be needed to produce an ideal information security game. However, this body of research may be a big step in the right direction.

This study indicated that information security can be presented though a game in an enjoyable manner. It discussed various aspects to consider when designing an educational game and produced guidelines researchers and developers should follow to create a similar game.
References


Appendices

Appendix A - Proper Computer usage Questionnaire

The questionnaire given to the participants in the experiment to determine if the game is educational and/or motivational.

Appendix B - Concealing the Medicine: Information Security Education through Game Play

Thomas Monk, Johan van Niekerk and Rossouw von Solms. Accepted and presented as research in progress at Information Security South Africa Conference 2009, Johannesburg, South Africa.

Appendix C - Concealing the Medicine: Information Security Education through Game Play

Thomas Monk, Johan van Niekerk and Rossouw von Solms. Accepted and presented as research in progress at South African Institute for Computer Scientists and Information Technologists Conference 2009, Johannesburg, South Africa.

Appendix D - Sweetening the medicine: Educating users about Information Security by means of game play

Thomas Monk, Johan van Niekerk and Rossouw von Solms. Accepted and presented as a full paper at South African Institute for Computer Scientists and Information Technologists Conference 2010, Bella-Bella, South Africa.
Appendix A

Proper Computer usage Questionnaire

The questionnaire given to the participants in the experiment to determine if the game is educational and/or motivational.
This questionnaire is done completely voluntarily. Participants are encouraged to complete the entire questionnaire, but may, if they choose to, decide to stop filling in the questionnaire at any stage.

Please complete ‘Section 1’ of the following questionnaire by choosing the most correct answer.

**Section 1**

<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
<th>Correct Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What is pharming?</td>
<td>a.) Growing plants that are harvested to be used in pharmaceutical products.</td>
<td>b.) A website that impersonates a legitimate website in order to gain private information from their users.</td>
</tr>
<tr>
<td>2. What is phishing?</td>
<td>a.) Catching fish that are harvested to be used in pharmaceutical products.</td>
<td>b.) A website that impersonates a legitimate email provider in order to manipulate Internet communications.</td>
</tr>
<tr>
<td>3. What is spyware?</td>
<td>a.) A type of computer virus.</td>
<td>b.) James Bond’s fashion line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>c.) A hidden program that monitors and steals user information.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>d.) A program that spreads through computer networks with malicious intent.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. What is spam?

| a.) The Security Program for AMateurs. |  |
| b.) An email that mocks you. |  |
| c.) A meat advertisement. |  |
| d.) Receiving lots of unwanted emails. |  |

5. What is a computer virus?

| a.) A computer program that copies itself to other computers often with menacing intent. |  |
| b.) Human viruses being instigated by using computers. |  |
| c.) Electronic information being absorbed by humans through wireless networks. |  |
| d.) Placing a magnet close to a computer. |  |

6. How can you prevent unwanted emails from reaching you?

| a.) Don’t give anyone outside the organization your work email address. |  |
| b.) Contact the server administrator to block all emails he/she thinks is unwanted. |  |
| c.) Ensure that all your emails are encrypted. |  |
| d.) Set windows firewall to protect you against harmful emails. |  |

7. When you receive an email from an unknown source you should?

| a.) Call the police. |  |
| b.) Delete it immediately. |  |
| c.) Reply to the email asking who that person is. |  |
| d.) Read it. If it is in good humor send it to your friends. |  |
8. How can you tell that a website is the official website of an organization, as oppose to a hoax website?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) The correct company logo is present.</td>
<td></td>
</tr>
<tr>
<td>b.) The ‘lock’ icon is present on the taskbar when monetary transactions are made.</td>
<td></td>
</tr>
<tr>
<td>c.) The website states that it is the official website.</td>
<td></td>
</tr>
<tr>
<td>d.) The web address (URL) is the same one given to you by the organization.</td>
<td></td>
</tr>
</tbody>
</table>

9. If you receive an email from the bank asking you to renew your details, you should:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) Follow all the procedures stated in the email.</td>
<td></td>
</tr>
<tr>
<td>b.) Call the bank to ensure that the email is legitimate.</td>
<td></td>
</tr>
<tr>
<td>c.) Reply to the email and ask why your details should be updated.</td>
<td></td>
</tr>
<tr>
<td>d.) Take legal action against the bank.</td>
<td></td>
</tr>
</tbody>
</table>

10. Can your computer get infected by a virus when you sneeze on it?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) Yes</td>
<td></td>
</tr>
<tr>
<td>b.) No</td>
<td></td>
</tr>
</tbody>
</table>

11. Can your computer get infected by a virus when you open email attachments?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) Yes</td>
<td></td>
</tr>
<tr>
<td>b.) No</td>
<td></td>
</tr>
</tbody>
</table>

12. Can your computer get infected by a virus when you browse the internet?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) Yes</td>
<td></td>
</tr>
<tr>
<td>b.) No</td>
<td></td>
</tr>
</tbody>
</table>

13. Can your computer get infected by a virus when you copy data from someone’s memory stick?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
14. Can your computer get infected by a virus when you send unencrypted emails?
   a.) Yes
   b.) No

15. Can your computer get infected by a virus when you install software from the Internet?
   a.) Yes
   b.) No

16. A virus checker aims to remove both spyware and viruses from a computer?
   a.) Yes
   b.) No

17. What is the best way to keep your computer virus free?
   a.) Format your hard drive often.
   b.) Renew your password often.
   c.) Use several virus checkers together.
   d.) Buy a new hard drive.
   e.) Update your virus checker often.
   f.) Update your spyware checker often.

18. What is the best way to keep your computer free of spyware?
   a.) Format your hard drive often.
   b.) Renew your password often.
   c.) Use several virus checkers together.
   d.) Buy a new hard drive.
   e.) Update your virus checker often.
   f.) Update your spyware checker often.

19. Why should people keep their passwords a secret?
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) If someone knows your password he/she can gain access to your data.</td>
<td></td>
</tr>
<tr>
<td>b.) Everyone will set their password to be the same as yours.</td>
<td></td>
</tr>
<tr>
<td>c.) You cannot gain access to your computer if someone else on the network has the same password as you do.</td>
<td></td>
</tr>
<tr>
<td>d.) All your emails will be sent to someone else.</td>
<td></td>
</tr>
</tbody>
</table>

20. Should a **GOOD** password be more than 8 keystrokes in length?
   - a.) Yes
   - b.) No

21. Should a **GOOD** password contain symbols?
   - a.) Yes
   - b.) No

22. Should a **GOOD** password contain numbers?
   - a.) Yes
   - c.) No

23. Should a **GOOD** password contain English words?
   - a) Yes
   - b.) No

24. Should a **GOOD** password be easy to remember?
   - a.) Yes
   - b.) No

25. Should a **GOOD** password be difficult to guess?
   - a.) Yes
   - b.) No

26. Is it alright to tell people your password over social programs or websites such as facebook or Mxit?
   - a.) Yes
27. Is it alright to tell people your mother's secret cake recipe over social programs or websites such as facebook or Mxit?
   a.) Yes
   b.) No

28. Is it alright to tell people what you are wearing over social programs or websites such as facebook or Mxit?
   a.) Yes
   b.) No

29. Is it alright to tell people about the projects you are working on at work over social programs or websites such as facebook or Mxit?
   a.) Yes
   b.) No

30. One slow day at work you stumble upon a website that has developed a system that offers daily horoscopes. The website states that the horoscope it generates isn't based upon planets or stars; it is based upon mind types. After completing a brain quiz you will receive an email everyday that states what events are likely to happen to you and what events you should be careful of. Registering for the website requires you to enter your email address. What do you do?
   a.) Enter your details and get ready to live a better lifestyle.
   b.) Ask your college to register so that you can see how it works.
   c.) Enter fake details including your email address.
   d.) Close the website and continue working.

31. You receive an email from someone stating that they went to the same school as you. That person goes on to describe how he has been doing and how he misses being at school. The email ends by asking you to reply to him in order to catch up. You can remember someone fitting the description giving; however, you are not certain that it is the right person. What do you do?
   a.) Delete the email.
   b.) Reply to the email asking further information.
c.) Forward the email to your friends and ask them if they can remember this person.

32. You start your computer at work and at Windows startup an error message pops up that you have never seen before. The last time you worked on the computer all you did was browse the Internet and copy something from someone else’s flash drive. What do you do?

| a.) Scan your computer for spyware and viruses. |
| b.) Request for the computer to be formatted. |
| c.) Ask the boss for a new computer. |
| d.) Restart your computer. |

33. While browsing the Internet you receive a message that says that you are a victim of spyware and that you should click ‘OK’ in order to remove it. What do you do?

| a.) Click the ‘OK’ button. |
| b.) Ignore the message. |
| c.) Close the browser and scan for spyware. |

Please complete ‘Section 2’ only if you played the ‘Cash City’ game at the computer laboratory on North campus.

**Section 2**

Enter the number computer where you played the game: _______________________
(It can be found on the top of the desktop and starts with “R”)

Mark with X

| 34. How much did you enjoy playing ‘Cash City’? |
| a.) Not at all |
| b.) A little |
| c.) A reasonable amount |
| d.) A lot |
35. Would you play ‘Cash City’, in your spare time, at the computer laboratories at the university?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) Yes</td>
<td></td>
</tr>
<tr>
<td>b.) No</td>
<td></td>
</tr>
</tbody>
</table>

36. Would you play ‘Cash City’ at home if it were given to you free of charge?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.) Yes</td>
<td></td>
</tr>
<tr>
<td>b.) No</td>
<td></td>
</tr>
</tbody>
</table>

37. Write down any suggestions you have to improve the game?
Appendix B

Concealing the Medicine: Information Security Education through Game Play

Thomas Monk, Johan van Niekerk and Rossouw von Solms. Accepted and presented as research in progress at Information Security South Africa Conference 2009, Johannesburg, South Africa.
Concealing the Medicine: Information Security Education through Game Play

Thomas Monk, Johan van Niekerk and Rossouw von Solms

Institute for ICT Advancement, Nelson Mandela Metropolitan University

s20520515@nmmu.ac.za, 0848425028, PO Box 77000, School of ICT, Nelson Mandela Metropolitan University, 6031
Johan.VanNiekerk@nmmu.ac.za, 0415043048, PO Box 77000, School of ICT, Nelson Mandela Metropolitan University, 6031
Rossouw@nmmu.ac.za, 0415043604, PO Box 77000, School of ICT, Nelson Mandela Metropolitan University, 6031

ABSTRACT

Many threats to Information Security can be avoided if proper information security processes are in place. However, one can only counter threats effectively once sufficient knowledge about information security has been attained. Consequently proper information security awareness through education is necessary. The problem with information security education is that many people are not motivated to attend education sessions, study related material or participate in online courses. Educational games have been around for quite some time, although they have been limited to a narrow range of subject matter. This paper will introduce a current, in progress, research project which focuses on the development of a computer game to teach basic information security knowledge to learners.

KEY WORDS

Information Security, Information Security Awareness, Educational Gaming
Concealing the Medicine: Information Security Education through Game Play

INTRODUCTION
The incorrect usage of information technology has become a huge problem in modern society. Securing informational assets is an essential part of proper information technology usage and thus crucial towards protecting users against risks. Being ignorant to these risks may lead to: A loss of assets, ruining company reputations (Ernst & Young, 2008) and businesses closing down.

Information security is the term used to describe how one can safeguard information assets. International practices and frameworks do exist that propose countermeasures that can greatly reduce the risks which threaten information (ISO/IEC17799, 2000; COBIT, 2001). Countermeasures often fail because people, in general, are not aware of the risks involved with information technology. People remain the weakest link for information security (Ernst & Young, 2008; Deloitte, 2009).

Numerous businesses have accepted that information security is a problem, but have not yet been able to solve the problem to an acceptable level. Formal ways to educate staff do exist, however it is exceedingly expensive for companies and businesses to send every employee, who works on a computer, for a training session.

Many people believe that the general public knows too little about information security (Siponon, 2001). Educating the general public about information protection may solve several basic problems associated with information security awareness. Problems such as phishing and password protection are essential in this respect, because these threats are a problem for the general public as well as for major corporations.

The main problem this paper addresses is that the general public and employees are generally not motivated to learn about safeguarding information. Companies sometimes use incentives in order to direct their employees’ attention towards information security, e.g. a piece of chocolate with a note attached about password protection (Albrechtsen, 2007). Security campaigns such as this often fail, because the motivation is directed towards the incentive instead of the information. Motivation needs to be linked to information security in such a way to ensure that knowledge is being gained by the employee. In other words, it should not be possible to eat the chocolate without learning about password protection.

This paper proposes the use of an educational computer game in order to motivate people to learn about information security.

RESEARCH DESIGN
The project will design and implement a game to teach information security concepts. Both qualitative and quantitative methods will be used to determine whether the game is both fun and engaging, as well as educational.
Initially a prototype will be developed. This prototype will conform to the design considerations outlined in the following section. Further prototypes should be developed against which the original game can be compared.

It is impossible to develop a prototype of every single game type known to man and it is also impossible for participants to play and evaluate every type of game. For these reasons it has been decided that only three games should be developed for this study. It is very difficult to evaluate how much fun something is, however, it can be determined what is more enjoyable between a small number of activities. In the same way it is very difficult to determine what game type is the most fun to play, however it is possible to determine which of these three types of games is more enjoyable for a given test audience. A relatively fun game is sufficient for the purposes of this study.

Although the second game will have the same features and lessons as the original game, it will not abide by the recursion principle mentioned in the following section. The game will not be limited to a time period, instead the game will continue until the player has game points (money) left. The score will be determined by how long the player had any game points left. This means that money threatening events will happen more often and will affect the player’s total amount of game points more severely as the game continues. One might argue that this is a better approach to teach someone a lesson.

The third game will also have the same features and lessons as the original game, however the game will explicitly tell the player what to do in order to progress in the game. A story should be linked to a game such as this. It can be argued that a lot of people do not want to guess what is right through experimentation but rather be told what to do. This game will test whether the previous statement is true.

These three games can be compared with each other because essentially it is the same game with just different ways of playing it. They can be compared to determine which game is more popular and thus making it more fun. This is accomplished by placing all three games on a network and digitally counting how many times the game was started and how many times the game was completed. It is possible that there will not be a clear-cut winner to the popularity test, in which case it is necessary to consider having multiple games as part of the solution.

After it has been determined which game is the most fun, a survey needs to be conducted to test what the players have learnt and what they thought of the game. At the start of the survey participants will be presented with a questionnaire asking them:

♠ How often do they play games?
♠ What game genres or style of game play do they like?
♠ How much do they know about information security?

Following the questionnaire, this group of participants should play the game a couple of times and answer another questionnaire asking them:

♠ What did they think of the game?
♠ How much have they learnt about information security?
Note that the questionnaires should not give the impression that the game is an educational game. Questions asking about information security knowledge should be carefully constructed and placed close to general questions which will hide the fact that the survey is mostly about what knowledge the player has acquired. It is also important to ask the same questions about information security before and after the study to ensure that knowledge is being increased.

A fundamental flaw with the solution proposed in this paper is that some people are not interested in games and thus not motivated to play them. The survey will also address this issue by determining what people who do not like games, thought about the game. The survey might show that those people changed their opinion based on this game or that more research should be conducted to motivate these people.

The main aim of the survey will be to determine whether the game is educational, thus proving that the game is fun and also teaches information security knowledge.

PROBLEMS IN CURRENT INFORMATION SECURITY EDUCATION AND AWARENESS

Information is a valuable asset to most businesses. Many ways exist that mitigate risks that threaten the safety of information assets. Several of these risks cannot be prevented if the users of the system are not educated to act securely (van Niekerk & von Solms, 2007). Users are often ignorant of the magnitude of their actions towards information systems.

Common methods that companies use to educate their employees on information security include: posters, training sessions and online tutorials. It can be argued that these methods cause several problems:

- Posters become part of the office sentry and only temporarily remind employees of a specific information security threat.
- Training sessions are usually expensive and waste time.
- Online tutorials are also time consuming and are difficult to govern.

These and other methods have an underlining problem of sometimes not motivating the employees enough for them to fully grasp the awareness aspect of information security.

The general public also suffers from a lack of information security awareness (Siponen, 2001). This is becoming an immense concern partly due to phishing attacks, the increasing use of email passwords and online banking.

Email services and bank websites usually instruct their users what not to do, however there are users who ignore risks thinking that nothing will happen to them. A user who does not care about information risks can be described as looking through rose-coloured spectacles (Siponen, 2001).

Again, the underlying problem can be largely contributed towards a lack of motivation.
In order to understand why motivation is lacking with respect to information security awareness the top information security threats should be identified. The top eight recurring external information security threats as described by (Deloitte, 2009) are:

- Email attacks, such as spam
- Phishing/pharming
- Virus/worm outbreaks
- Spyware
- Employee misconduct
- External financial fraud involving information systems
- Social engineering
- Physical threats

(Rothke, 2005) identifies a lot of the same threats stating that these are things that every employee should be aware of.

As mentioned earlier, the primary purpose of the research described by this paper is to design an educational game that will hopefully help address the motivational problems surrounding information security education.

The following section of this paper explains the process which should identify a suitable type of game to motivate people about information security. The process extends in order to prove that this game will make them aware of the top eight information security threats. This should play a role in the solution of widespread information security awareness.

**EDUCATIONAL GAMES**

Video games have been very successful in the last couple of years. Good games generate enough fun and enjoyment for the player to remain engaged for long periods of time. Educational games are games that have an added goal in mind: They also attempt to teach the player about a certain topic.

Educational games have been described as “edutainment” (Moreno-Ger & Burgos & Martinez-Ortiz & Sierra & Fernandez-Manjon, 2008) and “Serious Play” (de Castell & Jenson, 2003) and they have been used as a motivational tool for educators. Unfortunately some of them have also been described as neither fun nor educational (de Castell & Jenson, 2003). Being neither fun nor educational should constitute an educational game as being a complete failure.

There are mixed views of educational games in research, which indicate that although it is a good idea in principle, it is, however, not always implemented well enough. Here are two examples of security related educational games which have been successful.

- CyberCIEGE as described by (Cone & Irvine & Thompson & Nguyen, 2007) is an educational game that teaches the correct use of computer networks. The game uses a 3D environment to closely match what would happen in real life. CyberCIEGE has been used successfully to teach the US navy about proper network usage. This game
shows that security can be taught through game play, however it does not address our problem that relates to information security awareness.

- Anti-Phishing Phil as described by (Shreng, et al) is an educational game that teaches players to recognise potential phishing attack URLs. This piece of research produced fascinating results when it is compared to more traditional methods of phishing education. The research proves that a video game can be more effective at teaching phishing awareness than existing training material. However, the game is very specific and only teaches security prevention from phishing attacks. The game is also limited when it comes to further investigation by means of additional research.

THE GAME DESIGN

This paper proposes the design and development of a money management game to motivate people to learn about information security. The players will start the game with a small amount of money, after which they will be faced with decisions that affect the total amount of money they own. These decisions could be: investment decisions, banking decisions or job opportunities. Some decisions will result in gaining money while some decisions will result in spending money. Events are also prevalent where the game attempts to steal your money. These events can be mitigated if proper security processes are in place.

This is where information security awareness comes into play. Most of the threats on the player’s money will be related to information security. However, the game will not explicitly mention information security (the medicine). This is what is meant by “Concealing the medicine”. This technique is used because of the negativity surrounding information security and educational games (Moreno-Ger, 2008).

The game will be presented as a regular game with only one goal: To be entertaining. The players should be oblivious of the fact that it is indeed an educational game about information security.

In order to keep the game engaging while exposing content the following principles are proposed:

- The process of playing the game should directly relate to learning the educational content in the game. As explained in the above paragraph, in order to become good at the game the player must successfully secure his/her assets, which can only be done by having an understanding of information security. How tightly integrated the learning process is to the game play should directly relate to the overall appeal of the game. This also ensures that someone cannot “cheat” their way out of learning, in other words, to become good at the game is to become information security aware!

- The fact that the game is an educational game should be hidden from the player. This is called *stealth learning* (Prensky, 2001) or *concealing the medicine* by this author. As previously stated the player should feel more comfortable thinking that the aim of the game is to be entertaining. In the game money will represent information assets while many of the risks involved will deal with information security. It is not impossible that the player notices that educational content is being exposed through the
game which is not a problem. The biggest goal of this principle is not to give a negative first impression of the game.

♣ Learning should be gained through recursion and experimentation. A good way to learn something is to discover it yourself after gaining some experience. Making the game quick and easy will motivate the player to play it again and again, which is what is meant by recursion. Giving the player the option to do something the wrong way and clearly explaining why it is wrong will give the player a sense of experience as they experiment with their options. This process should make the learning experience more memorable because the student has learnt something by himself/herself and uses his/her findings several times.

However, some threats will not always penalise the player. In the game, if someone suspicious offers you a business proposal (pyramid scheme or otherwise), by buying into it will not necessarily cause a loss of money, but might bring the player high returns. This is essential to the overall appeal of the game because it keeps the player guessing by changing the game every time. This also maps closer to the real world. Indeed, to learn the lesson a high percentage of suspicious business proposals will be scams, thereby revealing that it is in fact a huge risk. What is being learnt by using the system is being aware of risks, which will still be accomplished by playing this kind of game.

♣ The game should make mundane tasks fun. Irritating events can spoil a good game, by making these events fun it can stimulate the players while they are learning. Password protection could be one such event. In the real world it is quite frustrating to enter one’s password into the computer every time you use it. Why should the same action put into a game be any different? Password protection is an important lesson to be learnt. Thus by making the process more fun, it should make the overall game play better while giving a positive reflection on tasks such as password protection.

♣ The game should make use of a points system. The player will have points added when they do things correctly and points deducted when they do things incorrectly. In the game presented above money will serve as these points. On completion of the game the final score (total amount of money) will be presented to him/her. The player can clearly deduce whether this score is better than his/her previous scores and whether this score is better than their friends’ or colleagues’ scores. What often follows is that the newly acquired score is less than the comparable scores, resulting in a desire to play the game again in order to receive a better score.

Note that these principles can be applied to other educational games, thus enabling further research being conducted, on these principles, in the future.

CONCLUSION

Information security awareness is a big problem. By implementing an educational game to spread awareness might be a big step in the right direction. Using techniques such as “Concealing the medicine” can be a key towards improving the quality of these educational games.
In order to test whether this educational game is successful, one has to test whether it is fun and whether it exposes educational content.

Not all people like video games, in this case the authors are “concealing the medicine in chocolate” for people who “do not have a sweet tooth”. However, it is the author’s opinion that good game principles can result in a game where quality may result in “chocolate” that may be irresistible to virtually anyone.
REFERENCES


Appendix C

Concealing the Medicine: Information Security Education through Game Play

Thomas Monk, Johan van Niekerk and Rossouw von Solms. Accepted and presented as research in progress at South African Institute for Computer Scientists and Information Technologists Conference 2009, Johannesburg, South Africa.
ABSTRACT
Many threats to Information Security can be avoided if proper information security processes are in place. However, one can only counter threats effectively once sufficient knowledge about information security has been attained. Consequently proper information security awareness through education is necessary. The problem with information security education is that many people are not motivated to attend education sessions, study related material or participate in online courses. Computer games can be used to simulate real world scenarios which should educate users better than traditional methods of teaching. This paper will introduce a current, in progress, research project which focuses on the development of a computer game to teach basic information security knowledge to learners.

Keywords
Information Security, Information Security Awareness, Educational Games, Computer Games, Video Games

INTRODUCTION
The incorrect usage of information technology has become a huge problem in modern society. Securing informational assets is an essential part of proper information technology usage and thus crucial towards protecting users against risks.

Computer security is essential to modern companies, because, although widespread access to business information may be necessary, misuse of that information must be prevented. People who want to gain access to business information include hackers, scammers and people who want to commit other criminal activities. When cyber criminals, such as described above, obtain information the consequences may include: a loss of assets, ruined company reputations and businesses closing down. Computer viruses can have similar consequences although viruses are generally not written to infect a specific institution.

Information security is the term used to describe how one can safeguard information assets. International practices and frameworks do exist that propose countermeasures that can greatly reduce the risks which threaten information [2][7]. Countermeasures often fail because people, in general, are not aware of the risks involved with information technology. People remain the weakest link for information security [5][6].

Numerous businesses have accepted that information security is a problem, but have not yet been able to solve the problem to an acceptable level. Formal ways to educate staff do exist, however it is exceedingly expensive for companies and businesses to send every employee, who works on a computer, for a training session.

Many people believe that the general public knows too little about information security [11]. Educating the general public about information protection may solve several basic problems associated with information security awareness. Problems such as phishing and password protection are essential in this respect, because these threats are a problem for the general public as well as for major corporations.

The main problem this paper addresses is that the general public and employees are generally not motivated to learn about safeguarding information. Companies sometimes use incentives in order to direct their employees’ attention towards information security, e.g. a piece of chocolate with a note attached about password protection [1]. Security campaigns such as this often fail, because the motivation is directed towards the incentive instead of the information. Motivation needs to be linked to information security in such a way to ensure that the employees are gaining knowledge. In other words, it should not be possible to eat the chocolate (in our example) without learning about password protection.

This paper proposes the use of an educational computer game in order to motivate people to learn about information security.

RESEARCH DESIGN
The project will design and implement a game to teach information security concepts. Quantitative methods will be used to determine whether the game is both fun and engaging, as well as educational.
Initially a prototype of the game will be developed. The prototype will contain information security content and will also try to motivate the player to continue playing the game.

At the start of the survey participants will be presented with a questionnaire that will determine how much they know about information security. After they have completed the questionnaire they will play the game. They will then be presented with a secondary questionnaire that will determine whether the participants have learnt any information by playing the game. The two questionnaires should ask the same questions in order to be comparable.

It should also be interesting to note whether the participants learn new information by playing the game a couple of times in a row. People remember better when something is repeatedly presented to them. If the players gain all the game knowledge by playing the game once then the content will be less memorable. However, if it is proven that more knowledge is gained by playing the game repeatedly then there is a greater chance of the information to be memorable, thus resulting in a better educational tool.

In order to test whether playing the game repeatedly will make a difference to the amount of knowledge gained, the participants need to be split into two groups. The sample group will submit their questionnaires, play the game three times and then submit their second questionnaire. The control group will submit their questionnaires, play the game once and then submit their second questionnaire. If the sample group has learnt more than the control group then it would prove that the game is more useful when it is played several times.

An incentive will be required to motivate NMMU students to participate in the survey. However the survey should also determine whether the game generates its own motivation. After the participants have submitted their second questionnaire an incentive will be given to them. The participants will then be given the option to leave with their incentive or continue playing the game if they wish. The only thing that will motivate the participants to continue playing is the game itself. This will make it possible to determine how fun the game is within this survey.

PROBLEMS IN CURRENT INFORMATION SECURITY EDUCATION AND AWARENESS

Information is a valuable asset to most businesses. Many ways exist that mitigate risks that threaten the safety of information assets. Several of these risks cannot be prevented if the users of the system are not educated to act securely [13]. Users are often ignorant of the magnitude of their actions towards information systems.

Common methods that companies use to educate their employees on information security include: posters, training sessions and online tutorials. It can be argued that these methods cause several problems:
- Posters become part of the office sentry and only temporarily remind employees of a specific information security threat.
- Training sessions are usually expensive and waste time.
- Online tutorials are also time consuming and are difficult to govern.

These and other methods have an underlining problem of sometimes not motivating the employees enough for them to fully grasp the awareness aspect of information security.

The general public also suffers from a lack of information security awareness [11]. This is becoming an immense concern partly due to phishing attacks, the increasing use of email passwords and online banking.

Email services and bank websites usually instruct their users what not to do, however there are users who ignore risks thinking that nothing will happen to them. A user who does not care about information risks can be described as looking though rose-coloured spectacles [11].

Again, the underlying problem can be largely contributed towards a lack of motivation.

In order to understand why motivation is lacking with respect to information security awareness the top information security threats should be identified. The top eight recurring external information security threats as described by [5] are:
- Email attacks, such as spam
- Phishing/pharming
- Virus/worm outbreaks
- Spyware
- Employee misconduct
- External financial fraud involving information systems
- Social engineering
- Physical threats

Rothke, [10] identifies a lot of the same threats stating that these are things that every employee should be aware of.

As mentioned earlier, the primary purpose of the research described by this paper is to design an educational game that will hopefully help address the motivational problems surrounding information security education.

Section five of this paper explains the process which should identify a suitable type of game to motivate people about information security. The process extends in order to prove that
the game will make them aware of the top eight information security threats. This should play a role in the solution of widespread information security awareness.

EDUCATIONAL GAMES
Video games have been very successful in the last couple of years. Good games generate enough fun and enjoyment for the player to remain engaged for long periods of time. Educational games are games that have an added goal in mind: They also attempt to teach the player about a certain topic.

Educational games have been described as “edutainment” [8] and “Serious Play” [4] and they have been used as a motivational tool for educators. Unfortunately some of them have also been described as neither fun nor educational [4]. Being neither fun nor educational should constitute an educational game as being a complete failure.

There are mixed views of educational games in research, which indicate that although it is a good idea in principle, it is, however, not always implemented well enough. Here are two examples of security related educational games which have been successful.

- CyberCIEGE as described by [3] is an educational game that teaches the correct use of computer networks. The game uses a 3D environment to closely match what would happen in real life. CyberCIEGE has been used successfully to teach the US navy about proper network usage. This game shows that security can be taught through game play, however it does not address our problem that relates to information security awareness.

- Anti-Phishing Phil as described by [12] is an educational game that teaches players to recognise potential phishing attack URLs. This piece of research produced fascinating results when it is compared to more traditional methods of phishing education. The research proves that a video game can be more effective at teaching phishing awareness than existing training material. However, the game is very specific and only teaches security prevention from phishing attacks. The game is also limited when it comes to further investigation by means of additional research.

Educational games are interesting ways of teaching users about information security because:

- They can be distributed to home users to increase their general knowledge about information security
- They are often self motivational
- They digitally place the user into real-world scenarios
- They can be used to verify whether knowledge has been gained

This is where information security awareness comes into play. Most of the threats on the player’s money will be related to information security. However, the game will not explicitly mention information security (the medicine). This is what is meant by “Concealing the medicine”. This technique is used because of the negativity surrounding information security and educational games [8].

The game will be presented as a regular game with only one goal: To be entertaining. The players should be oblivious of the fact that it is indeed an educational game about information security.

Designing and implementing a game to help solve the problems with information security awareness will pose interesting questions, such as:

- How will the game force the players to gain knowledge by playing the game? The process of playing the game should directly relate to learning the educational content in the game. As explained in the above paragraph, in order to become good at the game the player must successfully secure his/her assets, which can only be done by having an understanding of information security. How tightly integrated the learning process is to the game play should directly relate to the overall appeal of the game. This also ensures that someone cannot “cheat” their way out of learning, in other words, to become good at the game is to become information security aware!

The player should be given the option to do something the wrong way, in which case the game should clearly explain why it is wrong. This should give the player a sense of experience as they experiment with their options. Greater understanding should be gained by using this technique.

- How will the game prevent negative first impressions due to the negativity surrounding educational games and information security? The fact that the game is an educational game should be hidden from the player. This is called stealth learning [9] or concealing the medicine by this author. As previously stated the player should feel more comfortable thinking that the aim of the game is to be entertaining. In the game money will represent information assets while many of the risks involved will deal with information security.

171
How will the game motivate its players? The game should be made to be challenging, include three-dimensional graphics and use a point system in order to motivate a player to continue playing the game to attain the top score.

How will a points system be incorporated into the game? The player will have points added when they do things correctly and points deducted when they do things incorrectly. In the game presented above money will serve as these points. On completion of the game the final score (total amount of money) will be presented to him/her. The player can clearly deduce whether this score is better than his/her previous scores and whether this score is better than their friends’ or colleagues’ scores. What often follows is that the newly acquired score is less than the comparable scores, resulting in a desire to play the game again in order to receive a better score.

Note that these questions and answers can be applied to other educational games, thus enabling further research being conducted, on the chosen answers.

CONCLUSION

Information security awareness is a big problem. By implementing an educational game to spread awareness might be a big step in the right direction. Using techniques such as “Concealing the medicine” can be a key towards improving the quality of these educational games.

In order to test whether this educational game is successful, one has to test whether it is fun and whether it exposes educational content.

Not all people like video games, in this case the authors are “concealing the medicine in chocolate” for people who “do not have a sweet tooth”. However, it is the author’s opinion that good game design can result in a game where quality may result in “chocolate” that may be irresistible to virtually anyone.

REFERENCES


Appendix D

Sweetening the medicine: Educating users about Information Security by means of game play

Thomas Monk, Johan van Niekerk and Rossouw von Solms. Accepted and presented as a full paper at South African Institute for Computer Scientists and Information Technologists Conference 2010, Bella-Bella, South Africa.
INTRODUCTION

Educational game design

INTRODUCTION

Users of information resources need to be motivated to learn, and to be continually reminded how to protect information. Protecting information is known as Information Security. Information security is a multi-faceted discipline that depends on hardware, software and people. However, the users of the system are the main source of information security breaches [6] [7] and remain the weakest link in the security chain. Therefore, the users of the system need to be educated to enable them to protect confidential information. If confidential information is not protected there may occur a loss of information assets which could ruin the reputation of the company or even result in its closure.

Various methods exist that seek to educate information users on how to keep their data secure. One of these methods is the use of a computer game to teach information security content. Such a game should both teach information security concepts and motivate the players to play the game repeatedly to gain more knowledge. This should result in an educational program that people enjoy and, therefore, are reminded of information security every time they play the game.

The remainder of this paper will discuss the areas in which previous information security awareness techniques have failed and will motivate why gaming is a possible solution to overcome these problems. The paper will then examine the game that was developed to educate users about information security and finally the results of an experiment to verify the effectiveness of this game will be presented.

BACKGROUND

This section examines the problems with information security education as well as how this project aims to solve those problems.

Problems with information security education

A suitable information security education program should be created to effectively educate users about information security. Information security programs attempt [1] [17] to solve this problem by educating the users about information security. However, for various reasons these programs often fail. An in-depth discussion of current methods falls outside the scope of the current paper. However, the following sub-sections will briefly discuss the problems that should be addressed by educational programs that focus on information security.

Motivation

Motivation is a key concept when teaching learners about information security and it is often not taken seriously enough [20]. If the learners identify the benefits of attaining the knowledge they are being taught, then they are happy to learn about it. On the contrary, if the learners do not see how the educational content would benefit them, then they will be irritated when education is forced upon them.

Employees are often not motivated to attend information security seminars or view educational online material. Information security is viewed, by many, as a boring topic to study. Therefore, better motivational techniques should be implemented by educational programs on information security.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

ACM SIGSIT ’10, October 11–13, 2010, Bela Bela, South Africa.
Copyright 2010 ACM 978-1-60558-950-3/10/10…$10.00.
**Time and money**

Businesses have the option to pay for their employees to receive education during business hours. However, many businesses do not have the time and money available for this type of education. This is especially true for small businesses [9].

It is necessary that every employee within the organisation be educated about information security [11] [18]. Therefore, ample amounts of time and money may be necessary for an organisation to become adequately secure.

**Facilitates one form of learning**

Many information security programs only provide a single form of learning. The problem with this is that adults are already adapted to their own style of learning [15].

For example, someone in the company might come from a very technical background. He has learnt all his skills from people who verbally explained the machinery, or by viewing how people work with the machinery and from personal experience. If this person is given a book to read about information security he would not be expect to learn as much as he would from someone showing him how to perform these tasks and explaining them to him.

If an educational program supports different styles of learning, the chance of that program supporting the learning style of every participant increases. Therefore, educational programs aimed at adults must try to implement multiple learning styles.

**General public education**

General knowledge about information security needs to be increased for the public to become more aware of the dangers it involves [21]. There exist methods of spreading public awareness of information security, for example, radio programs and television talk shows. However, it is very difficult to create an educational program that will teach the general public about information security.

If the general public knew how to protect their electronic information then businesses would not need to additionally educate their employees. It is not easy to enhance general knowledge on certain topics. However, it is a factor that influences information security and many home internet users suffer from information security threats.

**An information security educational game**

The point of games is to provide enjoyment to its players. Games have existed since the early days of computing. Computer games have since emerged as a multibillion-dollar industry [10].

An educational game is known as ‘edutainment’ [14], ‘serious game’ [12] or even ‘digital game-based learning’ [23]. It is a game that seeks to be enjoyable to its players, but has an additional goal, which is to teach its players educational content. However, to incorporate these two objectives has proven difficult to accomplish [5].

Educational content and enjoyment must be carefully balanced when designing an educational game. In some cases this balance is nearly impossible to achieve. In this respect, creating an educational game can be like trying to sweeten medicine. The aim is to make difficult undertakings enjoyable, but sometimes this is just not achievable. However, in other cases educational games seem to work well [3] [4] [19].

Previous research exists that identifies guidelines for designing educational games [22]. However, these guidelines tend to be very broad. It seems that for different educational content, different design principles (guidelines) are needed to create a successful educational game. It is important to note how these guidelines are implemented.

The goal of the project is to examine how certain design principles affect the success of a game that seeks to educate users about various information security topics. How this game implements previously researched guidelines will be examined to verify whether they are suitable for this type of game.

The results will provide more specific guidelines that game designers can follow for designing similar games. These guidelines can, therefore, be generalised for games that convey educational content which involves how people use computers.

Educational games can be used to combat some of the problems of information security education, as identified by the previous section, in the following ways:

- Educational games can be made to be self-motivational. This factor can be exploited additionally by making the game appear to be a normal/non-educational game.
- An educational game should be less expensive than sending people for training. It can save the time companies spend on training staff members if their employees play the game when they are at home.
- Educational games can use diverse teaching methods. For an information security game, this should include written lessons that explain why the safety procedures should be followed and some practical ‘scenarios’ that test whether the player follows these safety procedures.
- Educational games can be spread to the general public. Due to the motivation people have to play games, it is possible to increase the general knowledge of home users by means of game play.

**RESEARCH DESIGN**

This section describes how the game was designed as well as the experiment which tested it. Two pilot studies were conducted prior to the experiment to ensure that no problems would occur during the final experiment.

**Pilot study**

**First pilot study**

A pilot study was conducted on five postgraduate students and four lecturers all of whom specialise in the field of information security. The main aim of this study was to determine if the game would be usable and understandable for the final participants. They were asked to note any errors while playing the game and whether the educational content was adequately conveyed through the game. A questionnaire with open-ended questions was used to capture the feedback of the participants. An interview between the participants and the researcher was conducted as the participants played the game.

**Second pilot study**

It was decided to conduct a second pilot study after the results of the first pilot study were analysed. A group of 43 fourth year students who attend information security lectures participated in this study. Its focus was to determine how usable the game is and whether it still had any errors. Another focus was to determine what type of instructions people prefer to use. The questionnaire used in this study included open-ended and multiple choice questions.
Results of pilot studies
The results of the first pilot study revealed that the game could be more usable and that it did contain errors. Very little was relayed about its educational content.

The pilot study revealed that people would rather skip long lists of instructions when it took them a long time to read. The participants did not really use the help features of the game, which were accessible through a question mark at the top right corner of every window. This made the game difficult to understand especially when it was played for the first time.

The game was changed to be more user-friendly and intuitive, and all the identified errors were addressed. A major concern was that the participants did not read important instructions which inhibited them from progressing in the game. It was decided to change these instructions to short questions to motivate players to read the information.

Initially, players struggled to understand the game. A help page was introduced to help players understand the game. The help page is a hardcopy that would be given to future players of the game which contained short instructions on how the game should be played.

The results of the second pilot study revealed that the game was usable and that a few errors still existed within the game. How the participants indicated to have read the instructions of the game yielded more interesting results.

Fifty-one point two percent of the participants indicated that they used the help features in the game, 100% of the participants indicated that they read every item in the short question section at least once and 76.7% of the participants indicated that the help page did in fact help them to get started with the game. Therefore, people are much more likely to read instructions when they are presented to them as short questions and a help page is potentially 25% more effective than the usual help features. It should be noted that normal help features for a game such as this may take hours to complete while the help page was written in about 20 minutes.

The game
Overview
A game was developed to address the goals of this project. The game is called ‘Cash City’ and it is an educational game that seeks to educate its players about information security practices and concepts. Cash City is similar to the well-known board game Monopoly. It is a board game and its ultimate goal is to make as much money as possible. Cash City is dissimilar to a regular board game because it verifies whether the player deals with information security problems in a correct manner. The game would be very complex for a secondary player to do these verifications. Therefore, at this stage, Cash City has been implemented as a computer game simulating a regular ‘cardboard’ board game.

The game makes use of stealth learning [16] so although the game is about information security, there is a big money management aspect attached to it. Its main screen is depicted on Figure 1.

Figure 1. Main window of Cash

Cash City is a computer game based on a board game. It follows the movement rules of a regular board game. Players move around the board by rolling dice. The number the dice roll produces determines what square the player moves to. Different squares on the board have different functions. The squares are grouped into five groupings. These groupings consist of Houses, Way to work, Businesses, Way back home and Mega stores. All the Houses are on the left side of the board, all the Businesses are on the right side of the board, the Way to work is at the bottom side of the board while the Way back home is on the top side of the board. The Mega stores are on each corner of the board.

When a player moves to a square on the board, the player is presented with options that are displayed in a panel to the lower right of the window. If the player is on a square with a Store on it, the main option displayed would be to enter that store. If the player is on a Business square, the main option displayed would be to go to work. If the player is on a House square, the main option displayed would be to sleep in order to start the next day. Completing a cycle around the board is equal to one day in the game.

The upper left panel of the window displays the top scores that players have obtained. There is a button titled “View Full Scores” that opens a new window where players can view all the scores recorded in the database of the game. The score of a player is calculated by adding the amount of money they obtained with each asset they own, which is converted to a monetary value.

The lower left panel of the window shows the statistics of the current game. Statistics such as “Money on hand”, “Assets” and “Current day” are displayed. The rest of the panels on the main screen provide general information about the game.

How the game is played
The player is presented with a short “How to play” tutorial when he starts playing the game. After completing the tutorial, the player is introduced to the background story of the game. The player has the option to buy assets such as a House. Before the player can roll the dice for the first time they must acquire a job interview from the “Daily news” paper that appears at the start of every day.

After a job interview is obtained the player can roll the dice for the first time. If the player goes to a Mega store, determined by the dice roll, that player can buy goods on sale. This makes the Mega stores more special than regular stores.
The player needs to go through the “Way to work” squares before that player can start with his job. The “Way to work” squares are either Malls or Risks. Mall squares give the player the option to buy items from two different stores. These squares contain a Grocery store. Players need to buy food at these Grocery stores regularly. This was designed into the game to ensure that the player must spend some money and because a money management game should include some expenses. Risk squares present the player with a random event, which is somewhat like picking-up a card in Monopoly. These random events include getting mugged or receiving a promotion. There is a higher chance that the player will face an event that will result in them losing money. Random events were handled in this fashion in the game because in an educational game it is very important to justify both reward and consequences. Players must understand that a random event happened because they landed on a certain square and not because they made an information security related mistake.

The player reaches the Business squares after going through the “Way to work” squares. The player rolls the dice until he is on the square representing the business he has made an interview with. At this square the player does a short interview that consists of a series of questions. How many of these questions are answered correctly will have an effect on how much money he will earn at that job. After the interview, players must login to their workstation to complete their work for that day. The workstation in the game is a simulation of a computer. This computer contains Internet, email and anti-virus software. The player receives an email every day that contains their job related tasks. These tasks relate to common information security threats. Players must select a suitable password, otherwise they will be fired. After the day’s tasks are completed, the players logout of their workstation and roll the dice. At this point, the player will receive either a “Congratulations” or a “Fired” message. The Congratulations message indicates that the player completed his work successfully, received money for their work and, therefore, did not place the information of the company at risk. The Fired message, on the other hand, signifies that the player placed the information of the company at risk in some way, does not receive money for their work and needs to find another job. The message instructs players about what mistakes they have made, what they must do to rectify them in future and how the mistakes relate to information being threatened.

The “Way back home” squares are between the Business and the House squares. These squares work exactly the same as the “Way to work” squares.

When the player reaches the House squares, he may roll the dice until he reaches a House he owns. Once there, the player is required to “chat” with his “friend” on a social networking application. Their “friend”, Ted, will offer financial advice if Ted is given some personal information. The idea is to give Ted information that the player has not used in his password to obtain some extra money. If the player does reveal information contained within his password he will be fired the next morning and will not receive money from Ted’s investment. If the player does reveal information that is not contained within his password he will receive some extra money the next day. This process tests the player against social engineering attacks. After closing the social engineering program the player may go to sleep to start the next day.

**Educational content**

Careful consideration needed to be taken to decide what educational content the game would cover. Deloitte [6] identified the most common recurring security threats in their annual security report. This list was slightly modified to produce seven topics of information security that a game could cover. The list is as follows:

- Spam;
- Phishing;
- Pharming;
- Virus outbreaks;
- Spyware;
- Password protection;
- Social engineering.

Out of these topics common scenarios were identified that players could work through to gain knowledge. These scenarios were converted into missions in the game, which players needed to complete as tasks in their job. All the jobs in the game are done through a computer simulation, therefore, players should be able to identify the correlation between a real world scenario and the one faced during the game.

**Teaching methods**

The scenarios work according to a reward/consequence style of teaching, which is documented by Squire et al [22]. A mission that is completed successfully, presumes that the player understands the principles regarding the missions and is, therefore, rewarded for it. If the mission is not completed successfully then the player must receive consequences for his actions and he is educated about his mistake. For example, a player in Cash City receives a phishing attack that contains a link to an obviously fraudulent URL. If that player deletes the email and logs out of his workstation, he will be given a salary as a reward for identifying a fraudulent URL. However, if players went to the link and entered private information they will be fired from their jobs and receive no salary. That player will be presented with a message stating what phishing is, that the URL was fraudulent and how they can identify phishing attacks and fraudulent URLs in the future.

All the topics are covered while a player is completing his job in the game except for social engineering which is covered when the player is at home. The way in which education is conveyed is implemented the same way whether the player is at home or at work.

Figure 2. Desktop simulated in the Cash City
The player should not be able to receive a high score in the game without learning its educational content. Bellotti et al [2] describe this practice as: the educational content needs to be “tightly bound” to the game. This means that the player needs to learn the educational content in order to progress in the game. It may appear obvious that game designers follow a tightly bound approach. However, educational games exist that are not tightly bound, where players may “skip” the educational content and still receive high scores in that game.

The game was created with the idea that it could be played several times by the same player. If the player continually plays the game he will continually be reminded of the risks associated with information security. For this reason, it was decided to implement a grading system within the game. The grading system allocates points to the scores of the players when they do something wrong in the game. Players often play the game repeatedly to try and beat their previous scores. By repeatedly implementing security practices in the game, players should get used to implementing these practices when they are performing their regular work on a computer. Therefore, people playing the game regularly should promote good information security practices amongst them.

Players need to be able to make the link between security practices in the game and real world security practices, for this concept to work. A simulation was used to achieve this.

Simulations as part of an educational game are discussed by Squire et al [22]. Cash City uses this technique to simulate a computer desktop as seen in Figure 2. The simulated desktop works similarly to a real one.

**Motivational aspects**

Graphics were included in the game to give players a visual representation of its content. The use of graphics within games should not be underestimated, especially when it is considered that pictures are always more attractive to people than text. Windows forms were used as the platform of the game, and although not as attractive as 3D graphics, it did provide a clear environment for players to interact in.

The fact that the game is an educational one was slightly hidden from the player. This is called ‘stealth learning’ [16] and it is a technique whereby players learn content from the game without being immediately aware of it. This is implemented to make the players feel like they should enjoy the game instead of learning something through it. When players feel that they need to learn content through a game they often feel opposed to it [12]. Therefore, stealth learning can be seen as a motivational aspect of the game. Stealth learning was incorporated into Cash City because information security is sometimes seen as a boring topic.

Cash City uses a grading system that enabled players to receive a score after they have completed the game. Scores are recorded by the game, which makes them comparable. When players view their previous scores, they are often motivated to play the game again to beat their previous high scores. Players may view the high scores of the other players, which motivates them to play the game to receive the highest score.

A background story was presented within the game. A story motivates players to work towards a cause, even when it is only a fictional one.

**Questionnaire design**

A questionnaire was created to test whether the game is educational. It included five definition questions, 23 short questions and four scenario type questions. These questions can also be divided into two pharming, five phishing, four spyware, three spam, ten virus, seven password and five social engineering related questions. Some questions related to multiple subjects. All of the questions were multiple-choice. These questions comprised Section 1 of the questionnaire.

The questionnaire included questions that relate to how much the players enjoyed the game. They were asked to indicate how much they enjoyed playing the game on a scale from 1 to 4, whether they would play the game on campus between classes and whether they would play the game at home if it was given to them free of cost. This was followed by one open-ended question that asks the players for suggestions to improve the game. These questions comprise Section 2 of the questionnaire.

The entire questionnaire was reviewed by a statistical consultant to ensure that there are no problems when analysing the data obtained from it.

**The experiment**

An experiment was conducted to test whether the goals of the project were met. Ethical clearance was acquired to run this experiment because university students were used as participants. The ethical committee of the Nelson Mandela Metropolitan University approved the experiment and the questionnaires used.

The statistical consultant who approved the questionnaire suggested that a minimum of 30 participants should be used in each group for the necessary statistical equations to compute. 36 students participated in the ‘play’ leg of the experiment while 40 students participated in the control group.

For the play leg of the experiment participants were taken to the computer laboratories at a university. Once there the students were given a help page that instructed them how to copy the game from the network and how to get started with the game. They were required to play the game once and complete the questionnaire.

Once a participant completed the questionnaire that participant was encouraged to play the game again, but the participant was given the clear option of taking his remuneration and leaving the venue of the experiment. Meal vouchers were used as the remuneration for participation in this experiment. All participants received the same remuneration for playing the game and completing the questionnaire, except for the participants who received top scores for the game. These participants received two or three meal vouchers instead of one.

Before the participants started to play the game they were informed that those who achieved high scores would receive additional remuneration. This was done to prevent the participants from merely completing the game, without concerning themselves with its content. Players were encouraged by the remuneration to understand the game.

Participants were encouraged to play the game again to indicate whether people, in general, would spend their free time playing the game.

The control group who participated in the survey merely completed Section 1 of the questionnaire which dealt with information security related questions. They did not need to complete Section 2 of the questionnaire that deals with game related questions. The survey included a control group to verify whether education was conveyed by playing the game. The questionnaires of the control group were compared to those of the play group to implement this verification.
RESULTS

There were 76 students who participated in the experiment. Participants consisted of first year students. The play group consisted of students who were invited to participate in the ‘play’ leg of the experiment. The play group consisted of 36 students.

The play group had to respond to Section 2 of the questionnaire which consisted of questions that inquired how much they liked playing the game. The first question indicated how much they enjoyed the game, where one point is allocated for “Not at all”, two points are allocated for “a little”, three points are allocated for “a reasonable amount” and four points are allocated for “a lot”. The average score for this question among the 36 participants was 3.4. The second question asked the participants if they would play the game at their university in their own spare time. All the participants answered “yes”. The third question asked the participants if they would play the game at home, if it was given to them free of cost. For this question, 33 of the participants (91.6%) answered “yes”.

After completing the game once, the participants were encouraged to continue playing the game, but were given the option to leave with their remuneration. It was noted that at least 17 participants (47.2%) voluntarily played the game a second time. It should also be taken into consideration that this experiment was conducted on a Friday afternoon before a long weekend.

Dialog that indicated interest was observed by the researcher, which included: “Did you make the game? Did you make it by yourself?” and “Where can I get the game? Can I copy it onto my flash drive?”

The control group consisted of IT students who were invited for the questionnaire leg of the experiment. They were notified about the experiment during one of their classes. None of them had played the game before. The control group consisted of 40 students.

The questionnaires of the two groups were statistically compared, by means of a t-test, to uncover by what degree the questionnaires differ. A t-test is a statistical measure used to evaluate the hypotheses in small (N < 30) samples [8]. The t-test yielded no statistical significance.

Individual questions between the questionnaires were compared, by using a chi-square statistic, to uncover by what degree the answers differ. The chi-square test was chosen because its confidence interval is applicable to small samples (N < 30) [8]. This test yielded no statistical significance for the 33 questions.

The average score received for the questionnaire by the play group (36 participants) was 73%. The average score received for the questionnaire by the control group (40 participants) was 72.8%.

The subsections of the questionnaire were examined for any notable differences. The subsections of the questionnaire are: “Definitions”, “Short questions” and “Scenarios”. The scenario questions revealed a 7% increase for the play group. The other subsections did not reveal any notable difference.

The questions in the questionnaire were grouped by their information security topic. This was done to indicate whether certain topics were taught more effectively by the game. The information security topics covered in the game are: pharming, phishing, spyware, spam, viruses, passwords and social engineering. The play group scored an average of 48.6% for pharming related questions whereas the control group only scored 37.5%. The other topics did not reveal any notable differences.

Individual questions were examined to determine which questions were answered better by the play group.

- Question 1 “What is pharming?” was answered correctly by 38.9% of the play group, while the control group only scored 22.5% for this question.
- Question 6 “How can you prevent unwanted emails from reaching you?” was answered correctly by 30.5% of the play group, while the control group only scored 10% for this question.
- Question 16 “A virus checker aims to remove both spyware and viruses from a computer?” was answered correctly by 50% of the play group, while the control group only scored 37.5% for this question.
- Question 21 “Should a GOOD password contain symbols?” was answered correctly by 91.6% of the play group, while the control group only scored 75% for this question.
- Question 32, which was a scenario question concerning a virus causing an operating system error was answered correctly by 91.6% of the play group, while the control group only scored 72.5% for this question.

A database recorded information as the play group played the game. The game scores in the database were examined to uncover meaningful information. It must be noted that due to incomplete games, human error, people moving between PCs and illegible handwriting meant not every game could be examined in this way and not every game could be linked to the participant who completed a questionnaire. The average score players received after their first round of game play was compared with the average score players received after their second round. The average score players received for the first round was 1481 from 32 participants. The average score for the players who completed a second round in the game scored 2679 from 10 participants. This yields a 55% increase from the first round to the second round.

Lastly, participants from the play group who obtained an 80% or higher score in the questionnaire scores were reviewed to indicate whether a good score in the game meant that the participants would learn more about information security. The average score for those participants was 2156 (11 participants) whilst the average score for all the identified participants was 1481 (32 participants). Only four participants who scored above 2000 points in the game did not reach a score of 80% for the questionnaire.

DISCUSSION

One aspect the experiment did not take into consideration is whether the game is more educational should it be played several times. The experiment did not test whether the participants learnt more from the game after playing it for a second or third time, due to time constraints. The game was designed to be played several times in a row. Therefore, further research might indicate that the game is educational although it needs to be played, say, ten times to effectively educate players. The 55% point increase from participants who played the game for the second time and the indication that a higher score influences how well participants did in the questionnaire, supports the notion of studying this aspect of the game further. These two results indicate that the ‘reward/consequence’ and ‘tight bound content’ educational aspects of the game had influenced the participants.
This experiment was the first test to verify whether the game is educational, therefore it should be expected that the balance between education and motivation might not be at a suitable level. This does not mean that all the design principles behind the game are ineffective, but rather that another combination of design principles might work better for the goals of this project. Further research may be needed to deduce what the right combination of design principles is for the purposes of this study.

The educational content and the questions in the questionnaire based on that educational content can be placed under scrutiny. This is indicated by the control group who scored an average of 72.8%. Therefore, the control group already knew a lot about information security. Perhaps if the educational content and the questions in the questionnaire were more difficult to answer, the study may yield different results. The fact that pharming (which is not a well known information security topic) questions were answered better by the play group supports this notion.

The scenario type questions were answered better by the play group. This may mean that this type of game is better suited to teaching people what to do in certain scenarios. This project aimed to educate people to the point where they understand why they need to take certain actions in certain situations. However, if the game can be used to train people how to react in these situations it may still be of use.

The positive response from the motivational questions in the questionnaire indicates that the motivational aspects designed into the game, as described in section 3.2.4, do indeed work and work in this type of educational game. It can be argued that people will not necessarily do what they answer in a questionnaire. However, at least 47.2% of the participants indicated that they will play the game for a second time although the experiment took place on a Friday afternoon before a long weekend. This indicates that people will use their own free time to play the game.

In summary the following guidelines can be identified from the experiment:

- The use of a computer simulation in the game taught players what to do in certain scenarios;
- Tightly-bound content and reward/consequences techniques contributed towards the educational value of the game;
- Windows forms may be adequate for an information security game, although other graphics and sound options could be more motivational;
- Competitive scores and playing the game repeatedly contributed towards the motivational aspect of the game;
- Stealth learning can be used in the implementation of an information security game.

The pilot studies indicated that even computer-oriented students benefit from using a ‘help page’ as they played the game. Therefore, a help page may guide players to better understand educational games. The fact that more players read the short questions than long lists of text, in the game, may help game designers to handle important instructions. The pilot studies contributed towards the game being more intuitive, which resulted in a more enjoyable game.

The following key recommendations were identified that researchers should take into account if Cash City (or a similar game) is tested by future experiments:

- Participants should play the game a couple of times before they complete a questionnaire;
- The game should not take a long time to complete and it should be made so that players can quickly play part of the game and at another time they can continue to play the same game;
- The effectiveness of the educational material should not be assumed. Proper tests must be conducted to verify the educational value of the game;
- Game play should be intuitive and only requires minimal help;
- All instructions to the players must be kept short.

CONCLUSION

The researcher thought that the game would be educational prior to the experiment of the study being conducted, but maybe it would not be motivational. However, the results indicated that the game was motivational, but not very educational. It was assumed that implementing a simulation that uses rewards/consequences would convey educational content.

It would seem that when security programs are created by security specialists without asking educationalists to review them, those programs are likely to fail.

Whether the game is more educational if it is played repeatedly, should be investigated. If the results still indicate that the balance between motivation and education is incorrect then further research should be conducted. It would be interesting to examine whether continually playing the game would alter the way people use their computers, but this was beyond the scope of this project. Future attempts to improve the educational impact of the game should, if possible, involve researchers with a pedagogical background during the design phase, and not just information security specialists.

The game may not be ready for distribution, but the study still produced an enjoyable game that includes various information security related content, which may in the future contribute to solving many problems related to information security.

REFERENCES


