# 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

## 1 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.

## 2 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.

## 3 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 though 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.

## 4 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.

## 5 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.

## 6 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.

# 7 REFERENCES

Albrechtsen, E. (2007). A qualitative study of users’ view on information security. *Computers & security 26 ( 2007 ) 276 – 289.*

COBIT. (2001) Governance, control and audit for information and related technology (COBIT). *3rd ed. IT Governance Institute, ISACA, ISACF, ISBN 1-893209-13-X.*

Cone. B. & Irvine. C. & Thompson. M. & Nguyen. T. (2007). A video game for cyber security training and awareness. *Computers & security 26 ( 2007 ) 63 – 72.*

de Castell, S., & Jenson, J. (2003). Serious play. *Journal of Curriculum Studies, 35(6), 649–665.*

Deloitte. (2009). The 6th Annual Global Security Survey.

Ernst & Young. (2008). Global Information Security Survey.

ISO/IEC177799. (2000). Information security management – part 1: code of practice for information security management.

Moreno-Ger, P., & Burgos, D., & Martinez-Ortiz, I., & Sierra, J., & Fernandez-Manjon, B. (2008). Educational game design for online education. *Computers in Human Behavior 24 2530–2540.*

Prensky. M. (2001). Digital Game-Based Learning.

Rothke, B. (2005). Computer security: 20 Things every employee should know, Second edition.

Siponen, T. (2001). Five Dimensions of Information Security Awareness. *Computer and Society*.

Sheng, S., & Magnien, B., & Kumaraguru. R., & Acquisti. A., & Cranor. L., & Hong. J., & Nunge. E. (2007). *ACM International Conference Proceeding Series; Vol. 229 88-99*

van Niekerk, J., & von Solms, R. (2007). A web-based portal for information security education.