Back to Basics: Information Security Education for the Youth via Gameplay

Rayne Reid, Johan Niekerk

Back to basics: Information security education for the youth via gameplay

Rayne Reid[1] and Johan Van Niekerk[2]

[1,2] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
s208045820@live.nmmu.ac.za, Johan.VanNiekerk@nmmu.ac.za

Abstract. Cyber technology and information resources are both fundamental components of everybody's daily life. This means that both society's adults and youths are exposed to both the benefits and dangers that accompany these resources. Cyber security education is becoming a necessary precaution for individuals to learn how to protect themselves against the dangers of the technologies and resources. This is particularly important for the current and future youth who are the most technology literate generations. This paper presents a novel educational approach that can be used to introduce information security concepts to the youth from a very young age.

Keywords: Information security education, Case study, Educational Gameplay, Brain-compatible Education

1 Introduction

The 21st century has witnessed numerous technological innovations and developments. Several of these developments have involved information technology (IT) infrastructure. These information technologies and their companion "cyberspace" have gradually become commonplace in many aspects of modern life. As a result users are becoming increasingly dependent on these technologies and cyberspace.

Unfortunately although cyber space provides many advantages to a user, it is also introduces many dangers to the user. The exposure of people, old and young, to the online and interactive world has resulted in them becoming potential targets for a vast array of information security threats. Examples of potential threats may include online attacks, exposure of personal information and many possible scenarios in terms of which other people pose a threat to the user by their using technological channels to reach an intended victims [1]. It is, thus, essential that individuals learn to protect themselves against these dangers. This is particularly important for the current and future youth who have grown-up in this technology-saturated environment.

The current youth are often more technology literate that the older generations. Generation Y (born 1977-1990) and the online teens (born 1991 – now, including generation Z) account for over 30% of the internet user population [2]. Similarly Generation Z (born 1995 – 2012, over 23 million people) are often already using the internet and other technologies. Generation Z has grown up in contact with highly sophisticated media and computer environment and will be more Internet savvy and

expert than even Generation Y [3]. This trend has persisted since the start of the development of most modern technologies. It has thus resulted in the question of "How can the youth be educated about cyber security?"

Traditionally children have looked to their parents to teach them how to cope with danger. However in the case of technology- related lessons, parents are often less technology literate or educated than the youth. As a result they are seldomly equipped to teach kids cyber safety. A more creative and semi-/fully- formalized information security education approach is therefore needed.

This paper examines a novel approach, which introduces a brain-compatible information security game. It will focus on the introduction of information security awareness games, which were accompanied by information security awareness talks into a primary school class as a case study environment. The games themselves will be created to comply with the brain-compatible pedagogy.

2 Background

2.1 Information Security Education

Information security is a multifaceted problem and a comprehensive solution to this problem will normally encompass physical, procedural and logical forms of protection against threats [4]. Information security education provides the knowledge and skills needed to implement information security practices.

Traditionally formal information security education programs have mainly targeted organisational audiences. However recent national legislation and cyber awareness campaigns (such as the campaigns run in the UK and USA) target the general public[5, 6].This implies the inclusion of the youth as well. Cyber security education that is appropriate for organizational environments would be less effective for educating the youth; therefore a more 'fun' approach is required.

2.2 Children and educational play

Traditionally formal education approaches have been adopted for information security education; however this may not be an effective approach for a *very young* target audience. A more fun approach is may be more suitable for such an audience. However should a fun approach be adopted, it should still implementable in a formal education environment. This would take advantage of the fun aspect as well as the formal education environments tendency to augment and build upon fundamentals taught using the fun approach. An educational game may therefore be an effective solution.

The young of many species learn skills though gameplay e.g. lion cubs learn to hunt and fight through mock battles and hunts with litter mates and later 'practice prey'. Similarly young humans learn skills through 'make believe' and educational games which enable fun learning.

Admittedly this learning is not completely sufficient for current life; however it is the basic building blocks, which provide the foundation knowledge which may be augmented by formal education. It is therefore the focus of this research for introducing knowledge to the youth.

'Fun' Education is an effective mechanism for people, especially of children, as it has the added benefit of holding their attention, being fun, engaging their interest, and preventing the children from disassociating from what is being learnt and done [7]. It does however require structure to be effective as an education toll. This can be accomplished through the introduction of pedagogy to the game, so as to help promote learning. One, tried and tested, pedagogy is brain-compatible education.

2.3 Brain-compatible Education (BCE)

Brain-compatible education may be defined as learning based on the educational principles, methods and techniques which endeavour to teach subject-matter in a manner and format which is naturally complementary to the physical and psychological processing functions of the brain [8, 9].

This means it is an approach that manipulates education presentations and environments to appeal to natural learning processed. To achieve this brain-compatible educators design and orchestrate life-like, enriching, and appropriate experiences for learners [10]. This means that instructional strategies are employed to allow all students may process information more effectively so as to ensure maximum understanding, retention and recall [11].

Brain-compatible principles and techniques have been effectively used in real-world classrooms and some online environments in the presentation of formal lessons. Its implementation is guided by a number of principles some of which are presented in Table 1.

Table 1: Brain-compatible principle applied in the design of the artefact [7]

1	A learning experience should be as multifaceted as possible, catering for as many learning styles as possible and providing as many opportunities for each learner to develop as possible
2	Positive emotions should be used to aid recognition and recall
3	Relate all new material back to old material and thereby build new knowledge on old knowledge
4	The search for meaning is innate and occurs through patterning
5	Every brain simultaneously perceives and creates parts and wholes during the learning process
6	It is necessary to review material repetitively to solidify recall and recognition.
7	Both the focused and peripheral attention of a learner should be involved in the learning process
8	Allow learners to progress through the course at their own pace.

These simple and neurologically sound principles are the general theoretical foundation of brain-compatible education [10]. When applied to educational material the brain-compatible principles guide educators in the definition and selection of appropriate educational programmes and methodologies and presentation techniques. Some of these principles will be applied and explained in the creation of the research artefact. The relevant principles are presented in Table 1. The next section will examine the case study portion of this research.

3. Case Study

3.1 Methodology

This research will follow various procedures of the case study protocols described by Yin [12] and Creswell [13]. The structure of the paper will be to firstly provide the context of the case study and its experiment; secondly to describe the research artefact, thirdly to describe the research instrument and fourthly to describe the implementation of the case study experiment. Finally the results and analysis of the research will be presented with accompanying conclusions which have been reached.

3.2 Description of the Context

Cyber security is a topic that is seldomly addressed in current South African school environments. Until recently this has been an acceptable practice. However because cyber technologies and information facilities have integrated into the daily lives of many people, including children of all ages, it has become necessary to educate children about cyber awareness and security. The subject matter should therefore be gradually introduced to the young target audience.

The context in which this case study occurs is at a primary school level (ages 7-13), using educational gameplay as the first subject matter primer. A fun information security game (research artefact) therefore had to be developed. The design of the artefact had to be carefully considered, this is discussed in the next sub-section.

3.3 The Artefact (Creation of BCE Information Security Board Game)

The artefact is targeted at a primary school audience. Therefore considerations in the design of the game included: age appropriateness content and delivery, inductivity or familiarity of use, ease of understanding, level of learnability and the potential for compliance with brain-compatible education principles. Existing children's games, which targeted this age group, were considered as the basis for the artefacts design.

'Snakes and Ladders', a popular board game played by children in many cultures, was chosen as the foundation game on which the information security educational game would be based. Numerous reasons accounted for this decision. Firstly the

game, having existed since the 2nd century in India, is a popular game whose gameplay and rules is probably known to the target audience [14]. Secondly its original purpose of teaching children the difference between 'good and evil' is similar to teaching children good and bad information security behaviours [14]. Thirdly, it currently targets children from age 7+. Fourthly pedagogical principles and appropriate information security educational content could be easily incorporated into the design. The design, content, and game play rules will be discussed in the below sub-sections.

3.3.1 Design

This section will present the reasons why 'Snakes and Ladders' was selected as a good redevelopment candidate for this research. These reasons will also be linked to implementation considerations from a brain-compatible educational perspective. The focus of this section is therefore the presentation design.

Firstly the game had to cater for multiple learners learning rates. Brain-compatible education advocates self-paced progression (Principle 8) therefore this had to be catered for in the game environment. This was achieved by presenting the content in a game format which required the players to take turns, and to move according to a dice throw. This therefore allowed the learners to play and learn at their own pace, but ensured that the dice regulated the general pace of the entire the game. In brief it prevented overly long pauses, such as those experienced in games such as chess.

Secondly the design, or redesign of the game had to maintain the interactivity and "fun feel" of the game. This was necessary to ensure a mental and physical involvement in the game, a social and communicative experience, and a fun, peer-supported learning experience. This was considered essential as it implements Principle 1 by appealing multiple learning styles, especially those favoured by kinaesthetic and auditory (social) learners.

Thirdly the game had to be entertaining enough to hold the player's focused and peripheral attention. This was necessary so as to comply with Principle 7. The abovementioned interactivity and social nature of the game would help achieve this. Interactivity combined with the "fun factor" of the game, the learner would become emotionally stimulated, and this would cause further interest and encourage focus.

The "fun factor" of the game also appeals to the learner's positive emotions. Principle 2 advocates that a learner is more likely to learn and retain content if they are experiencing positive emotions. Negative emotions may result in distraction, disinterest and the prevention of knowledge retention. Many aspects of gameplay appeal to this principle. Firstly a game, by its nature is fun, with its design encouraging changes in the emotional state e.g. happiness for ascending a ladder. Secondly the interaction between learners enables fun communication and competitiveness. Finally winning as incentive, increases the fun factor and appeals to Principle 2, it also encourages progression throughout the game (Principle 8). This emotional appeal is also further encouraged through the use of colour on the board.

Colour was used to influence the emotional state of the learners and also their focus – Principle 2. The background of the board's lesson material was coloured

various shades of yellow and green (see figure 1). Yellow; the first colour to be distinguished by the brain; elicits positive moods and attracts the learners' attention [15]. This change to the material also relates to principle 7 and the enhancement of the learners' attentiveness. Green encourages productivity and long-term energy and is, thus, an appropriate colour for a classroom activity [15]. The colours used also implemented principle one, by engaging visual learners. This type of learner is particularly drawn to colours, graphics and written concepts. These learners would therefore be the most likely to focus and benefit from the built-in education mechanisms of the "Snakes and Ladders" game.

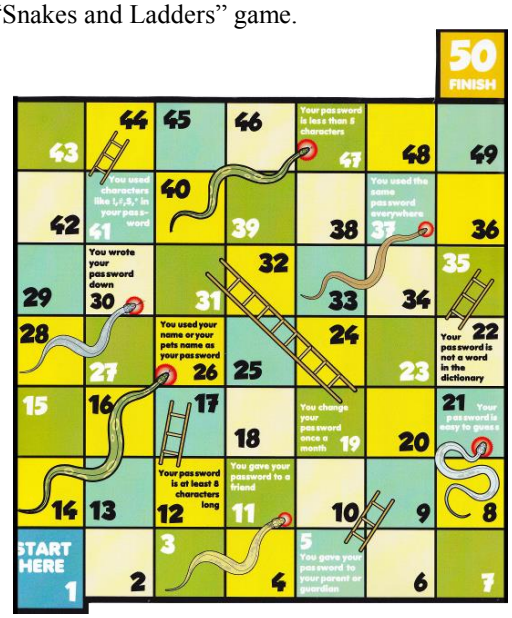

Figure 1: The Research Artefact - Snakes and Ladders Password Board

The final design considerations relate to the educational reinforcement mechanisms. As an educational tool the game has to provide consequences and rewards for lessons learned during the game. This was easily introduced into "Snakes and ladders" as its original purpose was to teach the difference between good and evil, and such mechanisms were therefore already inherent.

Information Security lessons/messages was placed above snakes and below ladders on the board (see figure 1). Positive lessons were reinforced by enabling ascension of the board via ladders. Conversely negative lessons were reinforced by forcing the player to descend down the board via snakes. This design associated negative consequence with negative message and positive consequence with positive message, and thereby enabled behaviour patterning (principle 4). This patterning also enabled principle 5 by creating knowledge components around a central topic which the player learned as a whole concept.

The snakes and ladders where placed randomly throughout the board, alongside information security lessons. These designs, and other similar designs, were used to present a number of different topics. The content presented in this case study will be addressed by the next section.

3.3.2 Content

Multiple games were created for many different topics. Examples of topics included social networking, password security, and virus security. Each of the boards had a similar design, but different content. The board presented, which relates to the results reported by this paper, taught password security content.

The content included within the game was topic related, in this case pertaining to secure password management. Various rules specifying the do's and don'ts of password security were placed above snakes and below ladders (see figure 1).

The do's and don'ts included lessons such as: the creation of a strong password, the frequency of change required to ensure a secure password, whom the password may possibly be shared with etc. They were written in a format that the player had/had not complied with a 'rule' of secure password management. The 'learner-centric' perspective serves to conform to Principle 3 of brain compatible education of contextualising lessons from a learner's viewpoint.

The do's were placed below the ladders e.g. "Your password is at least 8 characters long". The don'ts were placed above snakes e.g. "You gave your password to a friend". A complete list of the lessons presented in this particular password board is presented in Table 2.

Table 3: Password lessons of do's and don'ts

Do's	Don'ts
You gave you password to your parent or guardian	You gave your password to a friend
Your password is at least 8 characters long	Your password is less than 5 characters
You change your password at least once a month	You wrote your password down
Your password is not a word in the dictionary	You used your name or your pets name as a password
You used characters like !,#,$ in your password	You used the same password everywhere
	Your password is easy to guess

These lessons were then learnt in accordance with the rule of the 'Snakes and Ladders' gameplay. These rules will be presented in the next section.

3.3.3 The Rules of play

The 'Snakes and Ladders' games can be played by 2-6 players. Each player has a token which the place and move on the board. Play begins with everyone's token being placed at the start of the game. The first player then rolls the dice and moves the token along the sequential squares according to the number thrown.

If the square a player lands on contains an information security educational message, they read it out loud and perform the accompanying action. The verbal sharing of the message helps the learners to cognitively consider the lesson (principle 1). If the message was a do not lesson, they are swallowed by the snake and move

their token to the square which contains the snakes tail. If the lesson was a do they ascend the ladder and place their token in the square at the top of the ladder.

Players take sequential turns to roll the dice and move their tokens. The first player to reach the 50th square (Finish) is the winner.

The effectiveness of this research artefact as an information security educational tool will be determined through a survey. The survey (research instrument) used to do this will be presented in the next section.

3.4 Research Instrument

Part one of the research instrument consisted of a survey designed to acquire quantitative data about whether the learners had gained knowledge about secure password management after playing the game. The questions on the survey dealt with the subject area on which the game focussed. They were close-ended, multiple choice questions which related to a few select lessons that were included on the board. These tested student knowledge gain.

Part two of the research instrument consisted of a few interview questions targeted at teachers who allowed their classes to play the game. The interview questions tried to determine the teacher's perceptions of the effectiveness of the game as a teaching tool and it's the perceived effect on the learner's knowledge and behaviour

Both parts of this research instrument were implemented alongside the research artefact in the context of the case study. This is presented by the next section.

3.5 Implementation (experiment)

The research artefact was freely distributed to many primary schools within South Africa. Some of the schools targeted in the distribution were also given an introductory information security awareness talk and lesson using the research artefact. However for the purposes of this case study, two schools were selected as a target group and their data was gathered.

At School-A a grade 5 class of eleven students between the ages of eleven and twelve participated. At School-B a grade 3 classes of fifteen students between the ages of nine and ten participated. Both class teachers ran the survey in their classes, and then were themselves interviewed by the researcher. The research was conducted in this manner to comply with ethical research policies.

In relation to ethical research, children are classified as a vulnerable target group. Therefore due to ethical considerations both internal at Nelson Mandela Metropolitan University (NMMU) and externally at the target schools, the researcher did not interact directly with the students.

Surveys were provided to the target school's teachers. The teachers first had the children answer the surveys before playing the game. After the answer session, the children were then asked to play the game. After the game had been played they answered the survey questions a second time. The children were not allowed to share or discuss their answers. The researchers later interviewed the teachers.

This implementation was used as this research is the first stage of a larger research goal. The results presented are relevant to each case, however due to a lack of double blind testing they are not formal enough for statistical significance. A statistically significant approach will be conducted in the next stage of this research.

3.6 Results and Analysis

Within the survey, three questions, which related to the lessons presented in the game, were asked. These questions were asked before and after the game activity to determine whether there had been a change in the learner's knowledge and response. The results showed a definite positive trend which confirmed that the learners had gained knowledge relevant to secure password management (see Table 3).

Table 3: Aggregated Learner Survey Results

Question Number	Before playing the Game		After playing the Game	
	Correctly Answered (%)	Incorrectly Answered (%)	Correctly Answered (%)	Incorrectly Answered (%)
1	53.33	46.67	92.31	7.69
2	34.62	65.38	73.07	26.93
3	66.67	33.3	88.46	11.54

The interview questions aimed to determine: whether the teachers perceived the game as an effective teaching tool; and whether they perceived the learners to be more aware of the matters which the game taught after the game had been played.

Both of the teachers felt that the learners had definitely learned valuable lessons, relating to the topic, via the game. They also observed that the learners had undergone small behaviour changes which indicated a higher awareness of the issues. Both of the teachers concluded that they perceived the 'Secure Password – Snakes and Ladders' game to be an effective education tool.

4. Conclusions

Information security education is necessary for today's youth. Gameplay is an effective knowledge delivery system for youth, and can be used as a delivery mechanism for information security educational lessons. Such education does not have to be in an online environment. This case study has shown how a traditional board game approach could be effectively used in classrooms for such education. The case study has shown that the playing of this game lead to information security knowledge gain and to a certain amount of retention amongst the case study's students. It is therefore the conclusion of this author that gameplay in this format could be a viable option for the education of the future generation. Further research should be done to further improve the process.

5. Future Work

The research shown in this paper forms the preliminary starting stage of a larger information security education research plan. The next stage will prove effectiveness via controlled studies in order to prove statistical significance.

6. Acknowledgement

Professor R.Von Solms is acknowledged for his game content contribution.

7. References

1. Atkinson, S., Furnell, S., Phippen, A.: Securing the next generation: enhancing e-safety awareness among young people. Computer Fraud & Security.13-19 (2009).

2. Jones, S., Fox, S.: Generations Online in 2009 Generational Differences in Online Activities Generations explained. , Washington, D.C (2009).

3. Schroer, W.J.: Generations X,Y, Z and the Others, http://www.socialmarketing.org/newsletter/features/generation3.htm.

4. Furnell, S.M., Gennatou, M., Dowland, P.S.: Promoting security awareness and training within small organisations. 1st Australian Information Security Management Workshop University of Deakin Australia (2000).

5. The UK Cyber Security Strategy, (2011).

6. White House: The National Strategy to Secure Cyberspace, (2003).

7. Reid, R., Van Niekerk, J., Von Solms, R.: Guidelines for the creation of brain-compatible cyber security educational material in Moodle 2 . 0. Information Security South Africa (ISSA). pp. 1-8. , Johannesburg (2011).

8. Jensen, E.P.: Teaching with the Brain in Mind. New Directions for Adult and Continuing Education. 2008, 49-60 (2008).

9. Caine, R.N., Caine, G., McClintic, C.L., Klimek, K.J.: 12 brain/mind learning principles in action: The fieldbook for making connections, teaching, and the human brain. Corwin Press., Thousand Oaks, Calif (2005).

10. Caine, R.N., Caine, G.: Making Connections: Teaching and the Human Brain. Association for Supervision and Curriculum Development, Alexandria, VA (1991).

11. Banikowski, A.K.: Strategies to Enhance Memory Based on Brain-Research. Focus on Exceptional Children. 32, (1999).

12. Yin, R.K.: Case Study Research: Design and Methods. Sage Publications, Inc, Thousand Oaks, CA (2009).

13. Creswell, J.W.: Qualitative inquiry and research design. Sage Publications, (2007).

14. Avedon, E.: Snakes& Ladders or Chutes and Ladders, http://www.gamesmuseum.uwaterloo.ca/VirtualExhibits/Whitehill/snakes/index.html.

15. Taylor, A.: How the Brain Learns Best. Journal of Adventist Education.42-45 (2007).