E –learning and Password Games

R.Gardner and S.Atkinson

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

This research built a password game on a current smart phone that aimed to educate children within the topic of security awareness. The pedagogy used in the game is stated as having behaviourist tendencies. Children reported some informed opinions on passwords and used this knowledge to solve clues on appropriate use within a game of hangman. Early indications are that the game performed well and the novelty of the method used in an informal learning scenario is promising. Mobile learning and the topic of games and learning are both under presented in literature, despite the pedagogical benefits that could be brought to students by playing immersive activities that are able to motivate learners.

Keywords

E-learning, mobile learning, games, passwords, security awareness and children.

1 Introduction

This project considers the evaluation of an e-learning game that aimed to educate children in the area of passwords. The device chosen to implement the game was a current generation smart phone; such devices allow users to complete many different tasks and applications and can be considered relatively powerful. Objectives of research also included gauging the attitudes of children in the area of security awareness and measuring the effectiveness of e-learning games.

Passwords are still (despite their age) a very popular method for authenticating users as they engage with technology, in a variety of locations including the internet. Browne (1972) wrote about the commonality of passwords almost forty years ago. There have been different approaches to the means of controlling access such as by using smart cards, tokens or biometrics (Furnell, 2007). However, these options are expensive and not easily implemented for today's internet user. As we use the web we may have a number of usernames and passwords that apply to us and as such form part of our virtual identity. This may cause us some difficulty as we have to remember them, as we go about our tasks and it has not gone unnoticed within the human computer interaction community. Nielsen (2005) states the cognitive problems that result from having to handle this scenario. Password usage is something that may come up as an issue for adults in the work place as companies have an obligation to look after data responsibly under the laws of data protection. The Computer Misuse Act (1990) also reminds us that access to resources must be

"within rights". What though do home users and children in particular know about the importance of passwords?

Although children will be using computers from a very different perspective for example: enjoyment, social networking, games and personal use, passwords remain something that must be looked after. Within computer security the password can be considered the "only line of defence from system intruders" (Bunnell et al, 1997). Through a lack of security awareness and misuse of the password there may be some worrying issues for children, Mark and Ratliffe (2011) defined cyberbullying as:"name-calling, threats, spreading rumour, sharing another person's private information, social isolation and exclusion".

Learning games are a relatively small research area in comparison to the topic of games at large, and require input from several disciplines if they are to work well. For example computer programmers, graphical designers and educators are needed as a minimum. Rooney et. al (2009) used two full time student programmers in their learning game that was based on a 3D graphics model and had graphical input as well as the perspective of lecturers in the area of learning. Brown (2008) records some attributes of game playing that may be utilised in the ultimate learning game; the desire of students to out perform their peers, be immersed in activity for long periods of time, paying great attention and meeting learning objectives as well. Learning games may also be described as serious games and come under the umbrella of e-learning in general. E-learning is a growing industry that has been born out of the popularity of the internet and the changing needs of its users, there are many ways in which it can be implemented. Andrade (2008) defines e-learning as: "the application of information and communication technologies in a wide array of solutions that improve knowledge and performance". Computers have been used in education for much longer than the duration of the internet however, Twining et al (2005) remark that computers have been in the classroom since the 1960s in the United States and within UK schools since the 1970s. Chambers and Spreecher (1980) found using such technology to be of value to learners of all abilities, the student who could learn quickly and those in need of more time; the computer was capable of handling both. However, as with any other form of information technology intervention appropriate software design is important. The term pedagogy is found in literature to describe the theories of learning and teaching, good pedagogy achieves good results for recipients. The internet is a very powerful resource and one in which people have become used to using for information. One form of e-learning is described as "shovelware" and this term from Teo and Gay (2001) merely describes the posting of electronic documents onto the internet. It is not the most valid means of e-learning but is a start.

Educators may have a good understanding of the term pedagogy and so perhaps they should have a role in the process. There are quite grounded methods however across the whole spectrum. The format of the rest of this paper is as follows: firstly the methodology behind our work is presented, a description of the 'password hangman' game designed to meet the security awareness, pedagogical and technical needs of the project is discussed. A brief synopsis of learning theories that we feel have contributed are shown. An evaluation of our results is documented and we close with a short conclusion and statement of further work.

2 Methodology

There were three phases in the project. In the first phase a literature review was undertaken across areas that were considered to be relevant to the research, computer security, games and learning, e-learning, perspectives on learning from the fields of education and psychology. Suitable methods to implement a learning game were investigated, eventually the choice of a smart phone was chosen as these devices support the notion of "anywhere any time learning". Development of the software commenced and although the researcher had a computing background with some commercial experience this was the first time that a major application (or game) had been written on a smart phone. It was ensured however that the pedagogical features were justifiable from ideas that where found in literature. Gaming theories from authors such as Prensky (2001) were also reviewed to ensure that when testing occurred typical features of games such as rules, goals, outcomes and competition were present in the prototype. The learning curve was therefore quite steep. Phase one also sought to find a suitable group of children to test the game. Resources and time available within the scout group restricted testing to four scouts but fourteen members of the scout group were kind enough to complete a password usage questionnaire. These data together provided some interesting points for discussion and cited much of the documented evidence we where able to find across literature. It is not claimed these data are significant but to back our theories we have looked to other work whenever possible. It should be stated that mobile learning is itself a research area Blunt (2009) records the same conclusion for game based learning. Therefore evaluating work is not as straight forward as was hoped. Phase two of the project tied up ethical approval to work with the scouts and finally during phase three write up of work was completed.

3 Description of Password Hangman

To enable children to learn about security awareness some well known principles for good password use (clues) were found from open literature (Furnell, 2007; Cazier and Medlin, 2006) and from publications such as Action for Children (2011) and the UKCCIS (2009). Eleven clues were stored inside the game so that the hangman game had some questions for children to evaluate. When the child did not choose an appropriate letter the game constructed the "hanging post" and hangman character "limb by limb" until the child had either correctly guessed the word or lost their ninth life. The answer to the clue was drawn on the screen as a series of dashes with each letter (or hint) filled in appropriately. Each incorrect guess of letter or word resulted in the loss of a life. By the ninth life the drawing of the frame and hangman character was complete and the game was lost. Upon the placing of the final letter or by taking a straight guess correctly the game was won. An animated graphic showed the result and a more detailed explanation of the question and answer was then presented. In the case of a win this reinforced the answer and also showed some reasoning. The same notion was provided when the child lost.

1. Who can you tell your password? (NOBODY)
2. At all times your password must be what? (CONFIDENTIAL)
3. This kind of password is difficult to guess (STRONG)
4. Don't choose a word found in one of these (DICTIONARY)
5. This word describes password theft. (ILLEGAL)
6. These people may steal passwords (HACKER)
7. With someone else's password you can _ _ _ _ _ _ _ _ to be them. (PRETEND)
8. Change your passwords at least this often. (YEARLY)
9. Don't use this date as a passcode. (BIRTHDAY)
10. This kind of password is difficult to guess (RANDOM)
11. Don't _ _ _ _ _down a password (WRITE)

Figure 1: Questions and answers held within the game

At any time children were able to skip the current clue and move on to the next without penalty. The game did not show the answer that was being skipped (and associated reasoning) but on reflection should have done so as not all learning goals could be met if the children skipped questions.

4 Learning Theory

Behaviourist learning theory represents an established set of principles that can be traced back to the time of Pavlov a Russian psychologist and beyond. He was interested in the notion of stimulus and response, tested with a group of dogs that were trained to salivate upon the ringing of a bell when food was present. Pavlov (Wollard, 2008, p.14) discovered that for a time even when no food was present the dogs would still salivate. The dogs recognised the bells that resulted in the reward of food and were even able to recognise combinations of sound and the shining of light, such that when a light was shone without the bell they would still expect food. Crawford (1998) records also the benefits to human learning when we are rewarded, learning is reinforced. The other side of the theory states that rewards can be withdrawn when we do not meet the learning goal (or a child misbehaves for example). Thus the child in need of reward reverts to good behaviour again. Rooney et al. (2009) cites that games can be very rewarding for players, through scoring and competition. Most behaviourist theory is not concerned with how we may store knowledge the presence of a changed behaviour is sufficient. Constructivists however, consider the acquisition of knowledge to be relative to our existing ideas and experience. Angela (2011) feels that students build up their own knowledge and should be encouraged to solve problems using the theories they currently hold. Constructivism sees the role of educators as one of a tutor guiding students through the course of learning. This can occur through the discussion and modification of existing ideas.

A combination of ideas from these theories, present how learning could be achieved within password hangman. By evaluating the clue children were consistently reinforcing the question being presented and the answer that was being sought. Reward was presented by way of a good score in the game, the opportunity to reach the top of the leaderboard the chance to better a friend. Constructivist theory was also in part used as children were given very little by way of prior knowledge it tested where they were at.

Analysis of the password use questionnaire would later suggest that the children knew enough to play the game. Other theory regarding the use of our senses is also considered relevant to the playing of the hangman game. Visual Auditory Kinesthetic learning (Kátaia, Juhászb and Adorjánia, 2008) considers how we use our senses and any preferences we may have to help us learn. Some may learn best through sound, visual cues or by actually touching and doing the task (kinaesthetic learning). Work by (Fernandez, Simo and Sallan, 2009) found that by using a combination of VAK elements that students were able to enhance their own learning experience (). Password hangman was able to provide children with the opportunity to touch, through the tapping of keys on the screen, and watch the visual reaction within the game. There were limited system noises that also informed users of errors.

5 Results and discussion

A summary of questions and responses used to gauge children's awareness of password safety are shown in the figure below. The small number of respondents (questionnaire n=14, game evaluation n=4) in our sample means that a detailed quantitative analysis of data is not required. The figure below presents an overview of results from the questionnaire.

1) Do you think passwords are important?	Yes (13)	No (1)
2) Why?	Account access	(2)
	Security	(3)
	Protection ->people	(2)
	Information /identity	(2)
	Safety	(5)
3) Where do you use passwords	Laptop	(12)
	Computer	(3)
	School Computer	(7)
	Games website	(10)
	Facebook	(7)

	All above	(5)
4) Do you use a password in >1 place?	Yes (7)	No (7)
5) Do you find it hard to remember passwords?	Yes (3)	No (11)
6) How do you remember passwords?	Memory	(5)
	Kept simple	(3)
	Write down	(2)
	Pet's name	(2)
	Other	(2)

Figure 2: Summary of questionnaire data

When these results are combined with game evaluation data this work has more standing. The first question asked if passwords were felt to be of importance. Reference can be made to computer security literature such as Furnell (2007) who found that users sometimes traded their passwords for rewards such as pens, suggesting that passwords are not always felt to be of value by users. In this work all but one child at least on paper felt passwords were important.

Many of the children were able to refer to the various underpinnings of security that passwords represent. The idea of having an online existence by children was also recognised. Children were able to associate passwords with key terms such as account access, securing information, protecting themselves, and the general principle that passwords make things safe.

These findings have come out of a coding analysis of the response to question two: "please explain why you think passwords are important". From the perspective of the game evaluation it was reassuring that children in the sample agreed. If not, it would have rendered the game pointless.

A later question found that despite being important children did share passwords, with friends and family (going against the advice of Furnell, 2007; Action for Children, 2011). Children were then asked to record details of their use for passwords. A key theme in response from this was twofold firstly that many children used laptops and all children said they used passwords in more than one place. Some children (over a third) remarked that they used passwords in all of the locations that were suggested (laptop, school computer, games website and the social networking site facebook). There were ten additional areas found in the free text response for other password uses. Frequency of password use was noted in literature (Gibson, Renaud, Conrad and Maple, 2009). Using passwords in multiple locations is generally frowned upon, half of the children admitted to this but over three quarters also said that they did not find handling multiple access difficult as noted in literature (Renaud and De Angeli, 2009). Next an open question regarding how they achieved this was posed, with responses generally agreeing with the opinions of literature. Children relied on their memory, (Cazier and Medlin, 2006; Furnell, 2007) kept passwords simple (Bunnell et. al, 1997) and used familiar words such as the name of pets (Cazier and Medlin, 2006).

The second part of our work was able to evaluate the performance of the game itself. Tests were undertaken at the scout meeting an informal experience, with scouts who were not playing the game taking part in their regular activities. The group were used to having useful activities presented within their meeting, recent other activities had included map reading and camping advice. Four volunteers agreed to test the game and were handed a simple instruction sheet that explained their role and key functions that were available within the game. Testing was undertaken for a period of almost two hours although the game was only active for some twenty-five minutes of this period. As noted by Sharples (2009) a log file recorded system activity in black box style, every interaction and game state. The four testers were able to correctly guess the answers to security awareness questions thirteen times. This included the realisation that passwords were confidential (n=4), you should tell "Nobody" your passwords (n=3), hackers may attempt to get hold of your password (n=2) with a password you can pretend to be someone else (n=1), your password should be changed yearly (sic) (n=1), password theft could be illegal (n=1). A full list of clues are given in Figure 1.

Our analysis was able to show that some of the children were also quite persistent in their use of the game as demonstrated by their spelling out of the word "confidential" in answer to the question 'at all times your password must be what?' This was the longest word held within the game and may not have come to mind, however there is not a connection between the difficulty of the clue and length of word being guessed. A short word can be difficult to guess if only one or two letters have been confirmed. One child guessed the word 'hacker' in only 80 seconds, 'confidential' was guessed in 137 seconds. Conversely, another guessed 'confidential' in only 39 seconds with 'nobody' taking 170 seconds.

All of the four testers gave positive reactions as noted was often the case with this form of learning (Schwabe and Goth, 2009; Sharples, 2009). Interesting comments were received by email from one evaluator who provided a reflection about their experience. They wrote that they had learnt about passwords, stated that the game had a good layout, liked the element of competition (Prensky, 2001) liked the collaborative feature of scoring against friends but also asked for increased difficulty and variety in the task. Even though the game had not managed to ask each clue to evaluators during testing, when the clues were repeated over the telephone a month later scout GK was able to give accurate answers to eight of the eleven questions stored within password hangman, a month after the original activity. It is not claimed that this is statistically significant but it would be nice to think that mobile learning could be an immersive technology that is able to facilitate one to one communication and find ways of introducing topics that could be considered dry within the classroom, this hope is shared by Zyda (2007) who would like learning done this way and by Dalsgaard (2005) who hopes for better pedagogies to be forthcoming from e-learning.

6 Conclusion

A description of a relatively new method for education, password hangman has been described and although the use to date has been limited and tested on a small number of children we are encouraged by the results. Games and learning is a promising field for some students who perhaps do not do well using traditional pedagogical approaches. There is also the opportunity that the student who is doing well can do better, become more immersed in activities and see materials from a fresh perspective. Zyda (2007) shares this great optimism. Dalsgaard (2005) sees the chance to improve education through the adoption of e-learning. The resources in this work were by no means exhaustive and the programming skills of a computing masters student where able to build a smart phone game. This ran in an informal environment prompting a group of willing evaluators to consider some security awareness ‘clues’ as noted in publications and literature. Mobile learning and games are still under presented within literature, perhaps because learning and psychological theories and programming can be daunting to those outside of the relevant fields. To this end we strongly suggest a multidisciplinary approach. A brief description of the pedagogical features within the game has been stated. While not perfect, features have built on the notion of reward as suited to games (Prensky, 2001) and behaviourism (Crawford, 1998). Children were able to state their knowledge of passwords on a written questionnaire before trying the game. Not only were they able to play the game using their existing knowledge (known as constructivism) the questionnaire data from fourteen students stated some refined opinions about passwords. Children were (as was anticipated) leading lives requiring credentials in multiple places, much to the displeasure of their memory. For the moment at least the future for the password looks to be secure, no pun intended.

7 References

Andrade, J., (2008) 'Guidelines for the development of e-learning systems by means of proactive questions'. Comput. Educ., 51 (4). pp 1510-1522.

Angela, T. (2011) 'A constructivist approach to new media: An opportunity to improve social studies didactics'. Procedia - Social and Behavioral Sciences, 11 pp 185-189.

Brown, G. (2008) 'The serious side of games'. e.learning age, pp 22-22.

Browne, P. S. (1972) 'Computer security: a survey'. SIGMIS Database, 4 (3). pp 1-12.

Bunnell, J., Podd, J., Henderson, R., Napier, R. & Kennedy-Moffat, J. (1997) 'Cognitive, associative and conventional passwords: Recall and guessing rates'. Computers & Security, 16 (7). pp 629-641.

Cazier, J. A. & Medlin, B. D. (2006) 'Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times'. Information Systems Security, 15 (6). pp 45.

Chambers, J. A. & Sprecher, J. W. (1980) 'Computer assisted instruction: current trends and critical issues'. Commun. ACM, 23 (6). pp 332-342.

Crawford , R. (1999) Teaching and learning IT in English state secondary schools: towards anew pedagogy? Journal of Education and Information Technologies: Official journal of the IFIP technical committee, 4 (1). pp. 49-63. ISSN 1360-2357

Dalsgaard, C. (2005) 'eleed-Pedagogical quality in e-learning'. Eleed-e-Learning and education,(1).

Fernandez, V., Simo, P. & Sallan, J. M. (2009) 'Podcasting: A new technological tool to facilitate good practice in higher education'. Comput. Educ., 53 (2). pp 385-392.

Furnell, S. (2007) 'An assessment of website password practices'. Computers & Security, 26 (7-8). pp 445-451.

Gibson, M., Renaud, K., Conrad, M. & Maple, C. (2009) 'Musipass: authenticating me softly with "my" song'. Proceedings of the 2009 workshop on New security paradigms workshop. Oxford, United Kingdom: ACM, pp 85-100.

Gilbert, J., Morton, S. & Rowley, J. (2007) 'e-Learning: The student experience'. British Journal of Educational Technology, 38 (4). pp 560-573.

Kátaia, Z., Juhászb, K., and Adorjánia, A.K. (2008) 'On the role of senses in education'. Comput. Educ., 51 (4). pp 1707-1717.

Mark, L. & Ratliffe, K. T. (2011) 'Cyber Worlds: New Playgrounds for Bullying'. Computers in the Schools, 28 (2). pp 92-116.

Nielsen, J. (2005) 'Ten Usability Heuristics'. 2005. [Online]. Available at: http://www.useit.com/papers/heuristic/heuristic_list.html (Accessed: 26th January 2011).

Prensky M (2001) Digital Game-Based Learning New York: McGraw-Hill.

Rooney, P., O'Rourke, K. C., Burke, G., MacNamee, B. & Igbrude, C. (2009) 'Cross-Disciplinary Approaches for Developing Serious Games in Higher Education'. Proceedings of the 2009 Conference in Games and Virtual Worlds for Serious Applications. IEEE Computer Society, pp 161-165.

Renaud, K. & Angeli, A. D. (2009) 'Visual passwords: cure-all or snake-oil?'. Commun. ACM, 52 (12). pp 135-140.

Sharples, M. (2009) Methods for Evaluating Mobile Learning. In G.N. Vavoula, N.

Pachler, and A. Kukulska-Hulme (eds), Researching Mobile Learning: Frameworks, Tools and Research Designs. Oxford: Peter Lang Publishing Group, pp. 17-39

Schwabe, G. & Goth, C. (2005) 'Mobile learning with a mobile game: design and motivational effects'. Journal of Computer Assisted Learning, 21 (3). pp 204-216.

Teo, C. B. & Gay, R. K. L. (2005) 'Content authoring system to personalize e-learning'. Proceedings of the 5th WSEAS Int. Conference on Distance Learning and Web Engineering. Corfu Island, Greece: World Scientific and Engineering Academy and Society (WSEAS), pp 105-110.

Twining, P., Evans, D., Cook, D., Ralston, J., Selwood, I., Jones, A., Underwood, J., Scanlon, E., Kukulska-Hulme, A., Dillon, G., McAndrew, P. & Sheehy, K. (2005) 'Should there be a future for Tablet PCs in schools?'. Journal of Interactive Media in Education,

UKCCIS (2009) 'Click Clever Click Safe: The first UK Child Internet Safety Strategy'. [Online]. Available at: http://media.education.gov.uk/

Wollard, J. (2010) Psychology for the Classroom:Behaviourism. Routledge.

Zyda, M. (2007) 'Creating a Science Of Games'. Commun. ACM, 50 (7). pp 26-29.