A Wolf, Hyena, and Fox Game to Raise Cybersecurity Awareness Among Pre-school Children

D. P. Snyman, Günther R. Drevin, Hennie A. Kruger, Lynette Drevin, Johann Allers

A Wolf, Hyena, and Fox game to raise cybersecurity awareness among pre-school children

DP Snyman[0000−0001−7360−3214], GR Drevin[0000−0002−9173−9542], HA Kruger[0000−0001−8514−4422], L Drevin[0000−0001−9370−8216], and J Allers[0000−0002−6896−4020]

School of Computer Science and Information Systems
North-West University, Potchefstroom, South Africa
dirk.snyman@nwu.ac.za

Abstract. Currently, children have a greater exposure to cyberspace and cyber threats than any previous generation. Digital technologies are evolving continuously with the result that cell phones, tablets and similar devices are more accessible to both young and old. Technological advancements create many opportunities, however it also exposes its users to many threats. Pre-school children are especially vulnerable to these threats, as they are rarely made aware of, or empowered to defend themselves against these threats. An approach to solving this problem is to create a mobile serious game that promotes cybersecurity awareness among pre-school children. The focus of this paper is the part of the game that promotes the use of strong passwords and not sharing these passwords with one's friends.

Keywords: Serious mobile games · Strong passwords · Raising awareness with storytelling · Online safety for pre-school children.

1 Introduction

Most of the technological advancement taking place in Africa and especially in South Africa, is in the mobile sphere [13]. This is mainly due to the fact that currently young people are the main clients of the digital uptake in developing countries and that mobile devices are easier and cheaper to acquire than other digital devices [5]. The result is that the younger generation has more exposure to technology than previous generations. This provides a big driving force for technological advances in developing countries.

The advancement in technology has many advantages to developing countries and it presents the younger generations with many new opportunities. The downside of these advantages and opportunities is that they are often accompanied with danger. This increases the likelihood that young people will be exposed to negative online experiences and cyber threats. The threat to young people is greater than it is to other groups due to the fact that they have insufficient

know-how of how to be digitally safe [5]. Being digitally safe involves the ability to distinguish between opportunities and threats or dangers as well as to act responsibly when online [13].

In the case of pre-school children, their risk to the threats and dangers of cyberspace is much higher as they are exposed to these threats from a very young age without being equipped with the knowledge and ability to protect themselves against these threats [13]. A large amount of cybersecurity educational material and awareness strategies exist, however very few of these resources are aimed at pre-school children. The problem is that pre-school children have different and specific requirements when it comes to learning. As most pre-school children are not able to read or write, it is necessary to use different ways to present information and include different methods of learning. Content also needs to be presented in a way that is fun and easy to understand thereby ensuring the children's interest and motivation to participate.

The use of mobile devices, by pre-school children, to access cyberspace poses a security risk for the children. However, the opportunity is also presented to use these devices as a tool to educate them about the dangers and threats of cyberspace. Children learn through playing games [14], therefore using a serious game on a mobile device can be a viable approach to introducing them to cybersecurity concepts.

A serious game is an approach whereby serious aspects, with the intention to instruct, are presented in the guise of a video game [3]. It could be possible to educate pre-school children about the dangers of cyberspace by using a serious game that is appealing to them and to deploy it on the mobile devices that they are familiar with. In this way it could be possible to enable them to act and protect themselves against these dangers.

The purpose of this paper is to present a proof of concept of a serious game that can be used to promote awareness of cybersecurity among pre-school children in the context of developing countries, specifically South-Africa. This paper is based on a Master's dissertation [2][1].

The remainder of the paper is structured as follows: In Section 2, a cursory discussion on cybersecurity is presented, followed by cybersecurity awareness for children in Section 3. Section 4 is dedicated to existing serious game implementations for cybersecurity awareness for pre-school children. The implementation of the game in this research is discussed in Section 5. A reflection on the implementation of the game is provided in Section 6 and Section 7 ends with a conclusion and future work.

[1] This study was conducted with ethical approval of the Faculty of Natural and Agricultural Sciences Ethics Committee of the North-West University, ethics number NWU-01159-20-A9.

2 Cybersecurity

Cyberspace has become a vital and irreplaceable part of modern society. Not only do billions of users visit it daily, but it also contains data and information of, and on, people, companies, and governments. This information includes sensitive data such as, protected health information, personal information, intellectual property and governmental and industrial information systems.

As threats in cyberspace can affect personal and private information, a form of digital security must be implemented by users of cyberspace to ensure that a safe cyber environment is maintained.

A common approach to protect assets from unauthorised access in cyberspace is the use of some form of authentication and verification to prove that the user, who is attempting to gain access, does indeed have the right to do so. The most common implementation of this method is the use of passwords. Creating strong passwords is a very simple, yet crucial step in protecting assets in cyberspace. Criteria that are commonly used to evaluate strong passwords are length, complexity and randomness [9].

3 Cybersecurity awareness for pre-school children

The purpose of creating awareness of cybersecurity is to focus an individual's attention on issues regarding cybersecurity. These awareness activities are aimed at enabling individuals to recognise cybersecurity threats and to respond to them in an appropriate way [11]. Cybersecurity awareness is aimed at users of cybertechnology and therefore the human element of cybersecurity is addressed.

There are a number of elements that need to be considered when developing a cybersecurity awareness campaign. One of these elements is simplicity. For an awareness campaign to be successful, it is important that the user feels in control of the situation and can follow specific behaviours [1]. By keeping the rules simple and consistent, the user's perception of control will make it easier to accept the new behaviour [4]. Another element is the use of engaging material that is appropriate for the target group [4]. This presents a challenge when the awareness campaign is aimed at a very specific audience, such as pre-school children. Some examples of awareness campaigns for children are presented in the following sub-section.

3.1 Example resources from literature

Cyberspace can be dangerous and therefore children, and more specifically pre-school children, need to be made aware of the dangers from a young age, but relatively few resources are available for use with this target demographic. Three examples from literature to increase awareness of cybersecurity issues among children (some without the specific focus on pre-school children) are given in Table 1.

Table 1: Cybersecurity resources for children [2]

Title	**Content**
Digital wellnests: Let us play in safe nests [8]	A book that consists of concepts, poems and messages set in the animal kingdom. It also inludes a number of digital wellness and cybersecurity morals.
Be Internet awesome [2]	Resources that explore four different in-game worlds that teaches the user cybersafety lessons on issues such as responsible communication, recognising potential scams, using strong passwords, and taking action against inappropriate behaviour. It also includes a curriculum for educators.
Savvy Cyber Kids [3]	A book series aimed specifically at children, in which the following digital wellness and cybersecurity elements are identified, *viz.* online anonymity; online bullying; and limiting screen time.

When comparing the above mentioned resources, the work of Fischer and Von Solms [8] has the best alignment with the aim of this study. Their book identifies relevant cybersecurity topics and is specifically aimed at pre-school children, while in comparison, *Internet awesome* and *Savvy cyber kids* identify a smaller number of core issues. In *"Digital wellnests: Let us play in safe nests"* simple explanations are used and the main characters are depicted using animals that children are familiar with and can relate to. There are four main sections in the book. The first section has a foreword and introduction aimed primarily at the parent, guardian or teacher. A few technology-related concepts are discussed and illustrated, using drawn representations, in the second section. The third section contains a number of poems which form the main content of the book. These poems feature animals that are busy interacting with technology and each poem ends with a moral lesson. The following is an example of a typical cybersecurity scenario (in this case, the use of strong passwords) that is addressed by the poems in the book:

> *Three friends, Wolf, Hyena and Fox, discuss how to create strong passwords. Wolf recommends that they share each other's passwords and Hyena agrees, until Fox warns them to never share their passwords with others.* — The moral of the story is to create strong passwords and to keep these passwords a secret from others. Good password practices are a big part of cybersecurity and it is essential to improve one's online security.

[2] https://www.google.ch/goodtoknow/web/curriculum/
[3] https://savvycyberkids.org/families/kids/

Finally, the fourth section of the book consists of 14 short, easy to remember, messages that serve as important cybersecurity-related lessons. The messages loosely match the lessons presented by the poems. The following example is the message that closely matches the lesson given by Wolf, Hyena and Fox:

> *"Remember, remember to never forget. A strong password is not the name of your pet. It's letters and numbers all mixed together. Hard to guess, but easy to remember."* [8, p. 38].

To better understand how to raise awareness of cybersecurity among pre-school children it is necessary to identify how pre-schoolers learn and develop important skills.This is addressed in the following sub-section.

3.2 Play as a mode of awareness and knowledge acquisition

Children, especially pre-school children, use the following five ways to become aware of, and learn to interact with their environment [12]:

- Observation - Learning visually using observation and imitation;
- Listening - Auditory learning;
- Exploring - Investigative learning;
- Experimenting - Learning by trial and error; and
- Asking questions - Inquisitive learning.

However, not all children learn in the same way. While some children respond better to teaching modes that involve observing and listening, others receive more stimulation from practical experimentation and asking questions. At their age, pre-school children learn through play [14] as it is a fun way to learn and presents the opportunity to observe, listen, explore, experiment and ask questions to solve problems, irrespective of a child's preferred learning mode. All forms of learning can therefore be stimulated using a single learning medium.

As a child's parent, teacher or guardian knows how the child learns best, their involvement is important to guide the child to optimize learning.

From the discussion above, it is clear that play can encompass many modes of learning at once. In the next section, the use of serious games, as a form of play with the intention of teaching and learning, is discussed.

4 Serious games for pre-school children

Pre-school children learn through play [14], therefore educators and parents are given the opportunity to use games to assist in teaching children new skills and knowledge. As children are already exposed to digital technology [6], the use of games for teaching and spreading awareness appears to be a viable approach. This is evident by the number of serious games aimed at young children.

A non-exhaustive list of serious games targeted at young children with the goal of teaching or spreading awareness of cybersecurity is given in Table 2.

The games listed here serve as a reference when creating a serious game on cybersecurity for children in general. A gap exists in the current literature as are no games with a focus on pre-school children [10] and, therefore, the novelty of this research is the creation of such a game to contribute to filling this gap.

Table 2: Serious games for children [2, 10]

Game name	**Cybersecurity topics**
Interland [4] (Serious game implementation of the "Internet awesome" resources from Table 1)	- Communicate responsibly; - Know the signs of a potential scam; - Create a strong password; and - Set an example and take action against inappropriate behaviour
Carnegie Cadets [5]	- Staying safe online - Protection against viruses and malware - Using social networks responsibly
CyberKids [6]	- Strong passwords - Vulnerability identification
PBS Cybersecurity Lab [7]	- Staying safe online - Spotting scams - Defending against cyber attacks

In an attempt to create a framework for games aimed specifically at pre-school children, Callaghan and Reich [6] identified the following educational design elements based on how they learn:

Clear and simple goals – Children learn best with clear instructions and modelling which allows them to draw connections to their existing beliefs and frames of reference [7];

Quality of feedback and rewards – Using feedback is important tool to encourage children and notifies them if they are doing something wrong. Visual and auditory feedback can be combined to make it easy for the child to understand and should therefore rather be used as most pre-school children are unable to read;

Structure of challenge – The structure of a challenge should match the level of performance of the target audience. The level of a challenge can be increased gradually as the child understands more of the material. Furthermore, its difficulty should be decreased when the child appears to struggle; and

Motion based interactions – Motion-based interactions can serve as an alternative to complex touch screen activities that might be too difficult for many children. Game interaction should be aligned with the physical capabilities of

[4] https://beinternetawesome.withgoogle.com/en_us/interland
[5] http://www.carnegiecyberacademy.com/
[6] doi: 10.1109/SCCC51225.2020.9281253
[7] https://www.pbs.org/wgbh/nova/labs/lab/cyber/

pre-school children. Touchable object sizes, simplified touchscreen motions, etc. will improve the total experience of the child.

All these elements are necessary for a game to be appropriate for pre-school children and should therefore be implemented in the mobile serious game that is to be created for this study.

5 Serious game implementation

In this section, an overview of the serious game that was developed in this study is given by discussing the layout and function of each scene and its components.

The game starts with the main menu which serves as a selection screen for choosing a story scene which includes a poem and related quiz and game to be played. A screenshot of the main menu scene is given in Figure 1. The two green arrows pointing left and right are used to navigate through the poems. The story currently shown is that of Wolf, Hyena and Fox as shown in the center of Figure 1, and is an animation that can selected. When this part of the screen is tapped, focus will be switched to the chosen story.

Fig. 1. Application main menu

Once a story is selected in the main menu scene, the related poem's first scene will be displayed and read out loud to the child. This specific poem forms the basis for the related cybersecurity theory on password complexity [9], presented at the appropriate level [13]. The poem progresses by tapping anywhere on the screen to move to its next screen. The purpose of this scene is to make the child aware of the dangers of cyberspace in an enjoyable way.

Once the moral and reflection questions in the poem scene (Fig.2) is completed, the quiz scene (Fig.3) is entered. In this scene it is determined whether or not the child understands the issue that was described in the poem by motivating him/her to answer four questions, about the topic, that are chosen randomly from a question pool. The random selection of questions is done to provide a form of replayability and thereby to ensure that no pattern is memorised when answering the questions. Progress is not blocked if the questions are answered

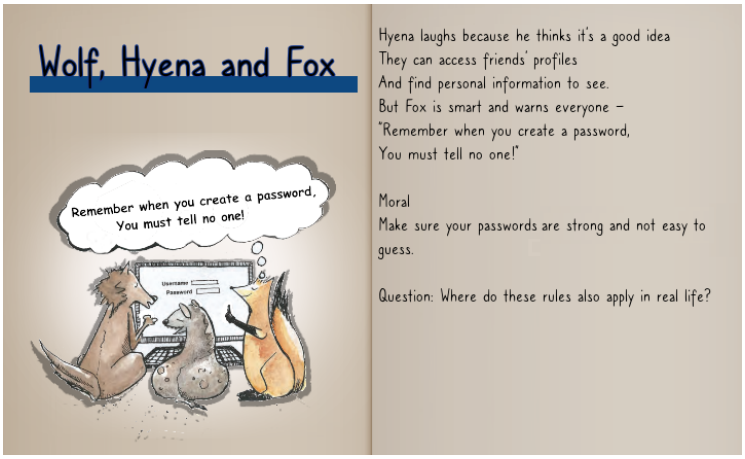

Fig. 2. Poem scene (page two of two)

incorrectly. The first reason for not blocking progress, is the objective of the game is not a formal assessment of the child's understanding of the dangers, but rather the raising of awareness on the matter. Secondly, the quiz is only a tool for the parents, teachers and guardians to be used to encourage the child and also to keep track of their effort and progress.

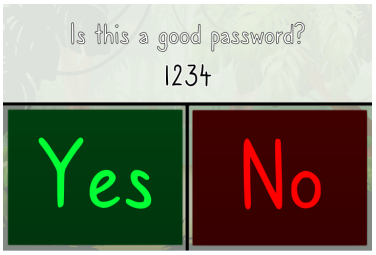

Fig. 3. Quiz question screen showing one of five possible cybersecurity questions based on the poem topic

The final scene allows the child to play a mini-game which is based on the poem that was selected. The game serves as a fun reward for completing the poem and quiz scenes. Before the game starts, the instructions and goal of the game are displayed on the screen and it is read out loud (Fig.4). A slider is used to set the difficulty level of the game.

In the Wolf, Hyena and Fox game (Fig. 4) the child has to flip over tiles to reveal the images underneath. If two tiles with non-matching images are flipped, they are flipped back. If the images match, the tiles are left facing upwards

permanently. The images are spread randomly between the tiles and each tile has exactly one match. The goal of this game is to match each tile with an identical tile. There is no scoring in the game and, therefore, it cannot be lost. The game is an exercise in memory and the theme of the message of the game is to remember the passwords that one creates. The number of tiles increase if a higher difficulty level is selected.

Fig. 4. Wolf, Hyena and Fox game

After completing the game, a message is displayed to indicate success or failure. This message is accompanied by an animation that relates to the poem. An option is presented to play again or return to the main menu. If the user decides to play again, the user is redirected to the level selection screen. The following section is dedicated to a reflection on the game.

6 Reflection

The aforementioned game design elements that were identified from the framework of Callaghan and Reich [6] are revisited in this section and used to reflect on the success of the implementation of the game:

Clear and simple goals – The aim of the game is to introduce the pre-school player to cybersecurity concepts at an appropriate level. Some specific activities that are used to meet this aim include listening (poem scene), reflecting (quiz scene), and playing (game scene). The goals for each of these activities are restricted to one outcome each, simple to understand, and the associated completion time of the activities are kept short to match the attention span of pre-school children.

Quality of feedback and rewards – During the reflection activity, real-time feedback is provided on the answers on the quiz with large recognisable symbols (ticks and crosses), accompanied by auditory feedback in the form of easily recognisable chimes. The game further rewards the player with an array of icons, once more featuring the characters from the poem, that indicate the level of

performance in the reflection activity. Depending on the outcome of the playing activity, a completion screen reaffirms the positive or negative result upon completing the game.

Structure of challenge – The challenge level of the final activity can be adjusted to match the relative ability of the player to play the game. As a player becomes more familiar and skilled, the difficulty can be increased accordingly to provide an ongoing challenge.

Motion based interactions – Motion interaction with the game remains a challenge to implement. Motion input is typically associated more with arcade style games, rather than serious games. Therefore, the input is restricted to tapping and touching gestures. The interface, however, has been designed with the pre-schooler in mind and incorporates bigger touch elements and simple actions appropriate to a player with developing motor skills.

Apart from this cursory reflection on how the game meets the required game design elements, further evaluation was performed in the form of an expert review of the game in its entirety and not only on the implementation of the poem aimed at strong passwords. This review was done by six experts in the field of pre-school education in the form of a questionnaire with a predetermined scoring system for evaluating the game, followed up by a telephonic interview for qualitative feedback. The reviewers believed the game to be an overall success and scored the game highly (average score of 4.5/5) on factors such as fun, suitability for pre-school children, and the effectiveness of conveying cybersecurity awareness. Due to space considerations, the full review is not shown here and the reader is referred to related work that describes this in detail [2].

This study is concluded in the following section.

7 Conclusion and future work

The aim of this paper was to to present a mobile serious game that is appropriate to promote awareness of cybersecurity issues among pre-school children. An overview of cybersecurity awareness for children and related resources were provided, followed by a brief discussion on the relevant learning modes that relate to children. Existing serious games for the promotion of good cybersecurity practices among children were discussed. Subsequently, the implementation of a serious game, specifically for pre-school children was described. The specific example regarding the use of passwords was used as an example of one of the topics that is covered in the game and the book that it is based on. The paper is concluded by contributing a reflection on the success of the implementation, based on a framework of educational design elements from literature and a short summary of an expert evaluation of the game.

Future work include the expansion of the game to include more information security scenarios, characters, and games.

References

1. Ajzen, I.: Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. Journal of Applied Social Psychology **32**(4), 665–683 (2002). https://doi.org/10.1111/j.1559-1816.2002.tb00236.x
2. Allers, J.: A mobile serious game to promote digital wellness among pre-school children. Master's thesis, North-West University, South Africa (2021)
3. Alvarez, J., Djaouti, D., et al.: An introduction to serious game - definitions and concepts. Serious Games & Simulation for Risks Management **11**(1), 11–15 (2011)
4. Bada, M., Nurse, J.R.: The social and psychological impact of cyberattacks. In: Benson, V., Mcalaney, J. (eds.) Emerging Cyber Threats and Cognitive Vulnerabilities, pp. 73–92. Academic Press (2020). https://doi.org/10.1016/B978-0-12-816203-3.00004-6
5. Burton, P., Leoschut, L., Phyfer, J.: South African Kids Online : A glimpse into children's internet use and online activities. Tech. rep., UNICEF (2016), http://www.cjcp.org.za/uploads/2/7/8/4/27845461/south_african_kids_online_brochure.pdf
6. Callaghan, M.N., Reich, S.M.: Are educational preschool apps designed to teach? an analysis of the app market. Learning, Media and Technology **43**(3), 280–293 (2018). https://doi.org/10.1080/17439884.2018.1498355
7. Cowley, B., Charles, D., Black, M., Hickey, R.: Toward an understanding of flow in video games. Computers in Entertainment **6**(2), 1–27 (2008). https://doi.org/10.1145/1371216.1371223
8. Fischer, R., Von Solms, S.: Digital wellnests. African Centre of Excellence for Information Ethics (2016)
9. Furnell, S.: Password meters: inaccurate advice offered inconsistently? Computer Fraud & Security **2019**(11), 6–14 (2019). https://doi.org/10.1016/S1361-3723(19)30116-2
10. Hill Jr, W.A., Fanuel, M., Yuan, X., Zhang, J., Sajad, S.: A survey of serious games for cybersecurity education and training. In: KSU Proceedings on Cybersecurity Education, Research And Practice. pp. 1–15 (2020)
11. Kissel, R.: Glossary of key information security terms. Tech. Rep. Revision 2, National Institute of Standards and Technology, Gaithersburg, MD (2013). https://doi.org/10.6028/NIST.IR.7298r2
12. Matthews, D., Lieven, E., Tomasello, M.: How toddlers and preschoolers learn to uniquely identify referents for others: A training study. Child Development **78**(6), 1744–1759 (2007). https://doi.org/10.1111/j.1467-8624.2007.01098.x
13. Von Solms, S., Fischer, R.: Digital wellness : Concepts of cybersecurity presented visually for children. In: Furnell, S., Clarke, N.L. (eds.) Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017). vol. 11, pp. 156–166 (2017)
14. Yogman, M., Garner, A., Hutchinson, J., Hirsh-Pasek, K., Golinkoff, R.M.: The power of play: A pediatric role in enhancing development in young children. Pediatrics **142**(3), e20182058 (2018). https://doi.org/10.1542/peds.2018-2058