State of the Art on Serious Gaming & Internet Safety Skills

Innovation Frontiers IKE

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1. Introduction

[*2-3 paragraphs - a) introduction to the topic, b) importance of the topic, c) summary of the report*]

The Internet can be a wonderful place to learn, shop, play games, and talk to your friends. Unfortunately, there are also predators, identity thieves, and others online who may try to harm you. In order to be safe online, it's important to be aware of the dangers. Many kids are confident that they know how to be safe online. However, there are a few reasons kids are often more at risk. They may not always think about the consequences of their actions, which can cause them to share too much information about themselves. Kids also are sometimes specifically targeted by cyberbullies or predators.

Children need to be made aware of these dangers by so they can use the valuable resource for their educational needs without falling prey to any kind of cybercrime. More and more schools are coming up with special campaigns to teach the importance of Internet safety for students, resources that can shared by teachers, students and parents alike so that there is a comprehensive protection formed for all users.

The first section of this report consists of applications of serious games to enhance Interned Safety. The training approaches to teaching Internet Safety Skills are presented in the second section. Finally some recommendations are presented in the third section.

2. Application of serious games to enhance Internet Safety Skills

[1-2 pages - empirical studies that have been conducted in your country or existing resources, projects or platforms related

The concept of serious games for cybersecurity awareness initially was one part of a broader awareness campaign led by governments, corporations, cyber education organizations to teach basic information assurance concepts such as: confidentiality,

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

authentication, integrity, and availability to informal learners (people with no prior knowledge or limited knowledge). When it comes to formal learners or Computer Science students in a higher education setting, the use of games as a supplemental educational material has been investigated and utilized 4 . Nevertheless, the mass adoption of serious games to teach cyber security in general, has not yet materialized. Studies have shown that today's schools face major problems when it comes to holding student motivation, engagement and focus for an extended period of time . Because learners of this generation are "digital natives", it has also been argued that using games is more in tune with their general habits6 . In comparison to traditional teaching methods, game-based learning allows students to make mistakes and learn from them in a risk-free environment 7 , 8 . Students are free to re-enact a precise set of circumstances multiple times. Thus, they can explore the consequences of different in-game actions which are not repeatable in most school settings.

Gamification has been explored to various extents in prior work. Serious games for general security awareness are arguably the most popular. Anti-phishing Phil for instance is one of the most well-known games that has sought to educate people about detecting phishing attacks. The domain of phishing attracts a large amount of gamification research, likely due to the prominence of phishing and its perception as a user-oriented threat. Beyond phishing, topics such as password security and cryptography also feature. Sholefield and Shepherd design a role-playing quiz application (RPG) to educate the general population about good password practices. Their evaluation highlights the im portance of games as an enjoyable way to learn, but also the difficulties in such pursuits (e.g. challenges in implementing effective leader boards). Similar positive findings are found by Deeb and Hickey as they explore the use of a 3D escape room game to teach students about cryptography. Offline serious games present another way to engage individuals. Riskio is a tabletop game to raise awareness of cyber security concepts for those in business and for those studying security at university. It is oriented around playing the roles of attackers and defenders within an organisational security context. Crypto Go is another physical card game proposed which can be used for educating about security, particularly cryptography. Through user workshops, researchers found that the game improved

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

motivation to study the topic and the understanding of the field. Focusing specifically on formal teaching contexts, Jin et al. situate their research on the growing need for a security workforce and use games to educate high school students. They propose and evaluate four cyber security education games (e.g. using virtual reality and tower defence) to teach topics such as security foundations, secure online behaviour, cyber-attack and defense methods and social engineering. Results were highly positive, and games were favoured by students and staff. Mostafa et al. also explore multiple games for teaching security through their testing of six games and how well they were received by university students. The games spanned topics such as network attacks, key management and web security, were implemented as image puzzles, simulations, role playing and action/adventure genres. Based on a user study, they conclude that the games could contribute greatly to the educational process. Lastly, capture the flag (CTF) games and exercises are extremely popular in cyber security. They allow participants (many of which may be students new to the field) to learn about the technical aspects of security, including finding and exploiting vulnerabilities (thus capturing ‘flags’). Sv´abensk`y et al. provide a ˇ recent overview of the field and highlight the various types of challenges implemented to teach security. A key finding of their work is that while CTFs clearly are an attractive proposition alongside traditional lectures, they currently predominately focus on technical knowledge but often neglect the human aspects of security; this is clearly a shortcoming given how much cybercriminals use these factors. More specifically, we have seen CTFs applied for introducing new students to security, formative assessment, and as part of teaching in online universities. This spread of application areas demonstrate the use of these exercises within education.

3. Training approaches

[1-2 pages – Conduct a brief desk research to answer the following questions:

1.Which approaches have been used to support training in Internet Safety Skills?

2.Which tools have been used during the training?

3. What learning difficulties in that subject have been reported?]

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Here are some training approaches for Internet Safety on Students:

CREATE A SCHOOL POLICY, AND HAVE STUDENTS SIGN IT

The first thing you'll need to do is create a school policy about internet usage. Lay everything out in clear, easy-to-understand terms. Describe how you expect the students to use the internet, what they should avoid and how they should communicate with others online. Then, share this policy with students and require them to sign in before using IT facilities at school. Having a policy will help pupils understand how seriously they should be taking their online safety.

TEACH STUDENTS ABOUT ONLINE PRIVACY

Kids these days often know better than to share passwords or their addresses online; however, there are new threats that they may not understand. Take the time to have a conversation with your students about how their favorite sites and apps store their information. Do they know that Snapchat, for example, keeps messages on a server for 30 days?

CREATE AN EFFECTIVE CYBERBULLYING REPORTING SYSTEM

"Cyberbullying is a common problem that nearly every school is dealing with," says educational expert Janet Moran from Elite Assignment Help. "You need to be able to support your students when it happens and educate them on the correct way to use the internet. Create a good reporting system that both students and parents can use to report cyberbullying, and follow through on any reports that you get."

GET STUDENTS INVOLVED

When you're creating new technology usage guidelines or introducing new hardware or software, ask students for their input. They're much more likely to work with you if they feel as though have some ownership of the process. They can also inform you of devices, apps and programs that you may not have known about.

KEEP UP WITH TECHNOLOGY

Teens often turn to their friends for advice online because they may feel more comfortable talking to peers or think their parents and other adults are unaware of the current technology landscape. Keep yourself up to date about online developments, and make

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

sure that students can come to you about any concerns they have. The more you know, the more you can help.

PROVIDE RESOURCES TO STUDENTS

There’s lots of educational services out there, but not all of them are trustworthy. Research educational resources before recommending or using them to make sure others have had a positive experience from a security, online safety and privacy perspective.

KNOW THE LAWS ON SEXTING

Sexting has become a real problem, and there have been many instances in which private photos and messages have been shared more publicly than the senders had originally intended. Look into the laws on sexting, and ensure the whole school staff know what to do if they discover evidence of it in your school. Then, talk openly and honestly with students and parents about it. Give the students the information on the law, and ask their parents to discuss with them. Teens are much less likely to engage in risky behavior if their parents are open with them.

4. Conclusions and recommendations

[Summarise your results and draw some conclusions based on the results. Include also some reccomendations for the learning design concept of the game based]

We propose the creation of a serious game to teach students Internet Safety Skills. Specifically we propose the development of a serious game in the form of an escape room game in which students will need to solve quizzes so as to escape from each rooms. The rooms will be have quizzes based at least on the following topics.

-Grooming

-Fake news

-Cyberbullying

- Phishing

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Through playing that game students will learn about Internet Safety through a playful way that will be a stealth environmnent that will hide knowledge in the game.

5. References

Aguilera-Hermida, A.P.: College students' use and acceptance of emergency online learning due to covid-19. International Journal of Educational Research Open 1, 100011 (2020) Barata, G., Gama, S., Jorge, J., Gon¸calves, D.: Engaging engineering students with gamification. In: 2013 5th International Conference on Games and Virtual Worldsfor Serious Applications (VS-GAMES). pp. 1–8. IEEE (2013)

Chicone, R., Burton, T.M., Huston, J.A.: Using facebook's open source capture the flag platform as a hands-on learning and assessment tool for cybersecurity education. International Journal of Conceptual Structures and Smart Applications (IJCSSA) 6(1), 18–32 (2018)

Chothia, T., Novakovic, C.: An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In: 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE

15). USENIX Association (2015), https://www.usenix.org/conference/3gse15/ summit-program/presentation/chothia

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Deeb, F.A., Hickey, T.J.: Teaching introductory cryptography using a 3d escapethe-room game. In: 2019 IEEE Frontiers in Education Conference (FIE). pp. 1–6. IEEE (2019)

Ford, V., Siraj, A., Haynes, A., Brown, E.: Capture the flag unplugged: an offline cyber competition. In: Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education. pp. 225–230 (2017) SherLOCKED: A Serious Game for Security Education

Fortes Tondello, G., Premsukh, H., Nacke, L.: A theory of gamification principles through goal-setting theory. In: 51st Hawaii International Conference on System Sciences (2018)

Gonz´alez-Tablas, A.I., Gonz´alez Vasco, M.I., Cascos, I., Planet Palomino, A.: Shuffle, cut, and learn: Crypto go, a card game for teaching cryptography. Mathematics 8(11), 1993 (2020)

Hart, S., Margheri, A., Paci, F., Sassone, V.: Riskio: A serious game for cyber security awareness and education. Computers & Security 9 licencja: CC-BY 4.05, 101827 (2020)

IX Liceum Ogólnokształcące im. Kazimierza Jagiellończyka w Toruniu

Innovation Frontiers Mind is the limit

technologos pushing the boundaries

WSEI

9

This project has been funded with the support from the European Commission (project no: 2020-1-PL01-KA226-SCH-096462).This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.