The Use of Gamification for Adult Education in Cybersecurity

Aneta Zemanova[1], Jaroslav Burcik[2]

[1]Czech Technical University in Prague, Faculty of Electrical Engineering, Department of telecommunications engineering

Abstract

In this work, we present a new game scheme designed in this project. It can teach even non-experienced users some hard-to-understand technical topics, such as cybersecurity. By means of the game, we simulate the behavior of real characters and the environment in which players encounter some cyberattacks. Thus, a player can experience, what it is like to lose their password or money from their account. With this personal experience, it is possible not only to learn the problem, but having this experience, some potential future dangerous situations can be avoided or evaluated correctly.

Keywords: E Learning, Avatar, User Experience.

Designed platform

Gamification is one of the most efficient ways in adult education. It has been widely used in HR, PR and marketing. The platform is based on some experience, achieved by a specially designed game. Players watch their sensitive information and experience a cyberattack. Therefore, we created a board game where players in the assigned roles can try to watch their sensitive data, face danger situations and some of the most common threats, and defend themselves in the best possible way.

The most significant problems can be split into 3 main areas: 1. Lack of knowledge about the environment (what one should care about, identification of possible danger) 2. Lack of knowledge about threats (the forms of cybercrime, possible defense) and 3. Lack of knowledge about valuable information (what can make a profit nowadays, what kind of information can be traded).

Educational goal	Asset	Educational significance	Game
Who and how is at risk?	Character cards	Identifying dissimilar groups of people and specifying their weaknesses / strengths.	Every character has got a short BIO + description of attacks immunity level.
What are the threats and risks?	Threat cards	What to watch out for.	The character is related to possible threats and risks.
What are our weaknesses?	Vulnerability cards	They show the real impact and risks of threats.	Vulnerability increases the possibility of attack (weak password, phishing, etc.).
How can we defend?	Fix cards	They demonstrate some "correct behaviour" (system updates, antivirus purchase, regular password changes).	It allows one to eliminate or reduce vulnerabilities, for example, thanks to some preventive security features.
What are the types of attacks and what are their consequences?	Attack cards	They show the most common types of attacks.	Thanks to them, we get sensitive data about others.
What can we lose?	Sensitive date cards	They explain the interests of hackers, and what is valuable nowadays.	The player must watch over their sensitive data, otherwise it is lost.

Conclusion

This project deals with one of the most common problem of today's world. The number of cyberattacks increases every year. The attacks are not related only to large institutions, but also to individuals. It is necessary to realize that everyone is a potential attack target. It is difficult to defend unless you know who is on the other side (it is difficult to identify the attacker). We expect an increase in efficiency of the educational process (through gamification, transfer of game principles to a non-gaming environment based on personal experience). We also expect that learning the problem in practice (in everyday use) could help to use a personal/work phone/laptop in a safe way or to carry out secure online payments on the Internet. We also expect increased cyber-immunity across the entire organization (safety is not only focused on the IT department, but on every ordinary employee, from an assistant to the director; everyone should be aware of the risks). Last but not least, reduction of economic or reputational consequences of cyberattacks on employees (end users) of an enterprise are expected.

References

- Whitney, K. (2007, March 14). Cisco illustrates how gaming could work for corporate learning, [online], [cit. 1. 1. 2019]. Available: https://www.clomedia.com/2007/03/14/cisco-illustrates-how-gaming-could-work-for-corporate-learning/

- KAPP, K., M. The gamification of learning and instruction: game-based methods and strategies for training and education. San Francisco: Pfeiffer, 2012, xxxiii, p. 302, ISBN 978-1-118-09634-5.

- NIST, Information technology security training requirements: A Role -Based Model for Federal Information Technology/Cybersecurity Training SP 800-16, USA [online]. [cit. 1. 1. 2019]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf

Acknowledgments

The project is held at the Department of telecommunications, Faculty of Electrical Engineering, CTU in Prague under supervision of Jaroslav Burcik, PhD. The project is supported by Operational HYPERLINK "http://penizeproprahu.cz/"Programme Prague – Growth Pole of the Czech Republic under the grant No. CZ.07.1.02/0.0/0.0/17_049/0000824.