RAISING AWARENESS OF CYBERCRIME - THE USE OF EDUCATION AS A MEANS OF PREVENTION AND PROTECTION

Julija Lapuh Bele[1,2], Maja Dimc[1], David Rozman[1] and Andreja Sladoje Jemec[1]
[1]B2 d.o.o., [2]MLC Faculty of management and Law

ABSTRACT

The widespread use of mobile devices that enable Internet access increases the exposure of both individuals and organizations to cybercrime. This article addresses the issue of strategic prevention of cybercrime with the key focus on the measures to prevent cybercrime related to children and teenagers. The primary tool for such prevention is undoubtedly education aimed at establishing greater awareness and knowledge regarding illegal Internet content and cybercrime among children and teenagers, as well as parents and educators. As many children have Smartphones, special attention should be paid to Smartphones and other mobile devices. Awareness-raising can only be achieved with a combined effort of key stakeholders, which we attempt to achieve though interactive educational modules. Therefore, we have prepared blended learning courses aimed at raising the awareness of the stakeholders (i.e. children, teenagers, teachers, and parents) based on theoretical background, practical experience, and an analysis of questionnaires. Face-to-face lectures are combined with courses conducted with LMS system eCampus, which is developed for use on mobile devices and PC computers, thus ensuring extended effects of the developed modules on the level of awareness of children and teenagers, as well as parents and teachers.

KEYWORDS

Cybercrime prevention; information security; blended learning; m-learning

1. INTRODUCTION

The increasing integration of web technologies in everyday life, along with the popularity of social networks and the development of mobile technology, contribute to the creation of an optimal environment for various types of cybercrime and the dissemination of illegal Internet content. Both children and teenagers represent not only the most avid users of new technologies and functionalities, but also the most naïve segment of the population. The general public is also not sufficiently aware of the severity of the problem.

As part of the General Programme on Security and Safeguarding Liberties, the European Commission established the Prevention of and Fight against Crime Programme; the project “Education as a Strategic Method against the Illegal Use of Internet” is funded within the framework of this programme with the key goal of increasing the awareness of the general public, children and teenagers in particular, on the issues related to cybercrime and illegal use of the Internet.

The project addresses the issue of strategic prevention, with emphasis on the fight against cybercrime related to children and teenagers by using education in order to establish greater awareness and increase the knowledge of children and teenagers, as well as parents and educators, regarding illegal Internet content and related activities. Existing initiatives in this field are primarily focused on presenting information in various forms. However, we believe that developing an educational module and actively implementing it in primary schools will contribute to increased awareness of both children and adults. Such a programme will have the following benefits:

- increased level of uncovered illegal content,
- faster and easier work of law enforcement agencies due to greater awareness of cyber victims and increased reporting of incidents,
- decreased number of cybercrime cases due to enhanced information system security.

Awareness-raising in of crucial importance when it comes to cybercrime prevention, and in the field of cybercrime related to children this issue is even more important, since the EU Kids Online survey found that only one-third of 9-16 year olds (33 percent) believed that their parents know more about the Internet than they do (Ólafsson & Livingstone, 2013). Therefore, we believe that all target groups need to substantially improve their knowledge regarding Internet safety and issues of illegal Internet use.

2. CYBERCRIME PREVENTION

In addition to its many benefits, the Internet increases users' exposure to various forms of crime. Indeed, the Internet has given rise to certain criminal offenses that were unimaginable or didn't exist in the past. Levels of privacy have decreased substantially as the Internet-using public's willingness to publish personal information has increased. Once something is posted on the Internet it can never be erased, a fact that the general public, and children and teenagers in particular, easily forget. Furthermore, fraud and scams are designed to take advantage of the virtual environment in which boundaries and time are irrelevant. Young Internet users should be made aware of the threats to their identity and assets, as well as the potential future ramifications of their activities on the Internet. Furthermore, core rules of etiquette in the virtual environment should be communicated to all users (Shea, 1994). Through raising the level of awareness of our children now, we will be moving toward the creation of an information-secure culture in the future.

2.1 Information Security Issues

Information security covers a very broad area. It encompasses both technical security and threats posed by users themselves, whether due to general lack of knowledge or to naivety when exposed to social engineering. In terms of technical security, IT professionals can install firewalls, antivirus software, and enable regular updates of the operation system and antivirus software. However, there is no software to protect the system from its weakest link – the human being. It is possible for parents to select appropriate software that will improve the security on a child's computer or mobile phone. However, it should be noted that mere supervision is not sufficient; a child should be appropriately educated to be aware of the dangers in the virtual environment and should know the basic self-protection techniques.

2.2 Cybercrime and its Impacts on Young People

Children and adolescents represent a vulnerable group of users who spend a lot of time on the web and on social networks. They are exposed to the same threats as adults, but the effect on them can be even more devastating. Due to the seriousness of the consequences, we have focused on the following forms of cybercrime that disproportionately effect young people:

- Cyberbullying – bullying of children and teenagers (threats, harassment, humiliation, embarrassment, etc.) carried out by children and teenagers with the use of the Internet, digital technologies, or mobile phones.
- Online sexual harassment and grooming – includes all actions that aim at lowering the child's inhibitions in order to sexually assault the child.
- Child pornography and the dissemination of inappropriate content – all materials showing children or teenagers in inappropriate sexual contexts[1].

[1] UNICEF estimates that more than four million websites showing juvenile victims, even children younger than two years, can be found on the Internet (Cehovin, 2010). The experience of abuse causes long-term effects on a person's later life, both physical and psychological. The latter includes feeling of guilt or responsibility for the abuse, low self-esteem, feelings of inferiority and depression. With Internet pornography, one must also realize that the child is victimized each time anybody watches material depicting his/her sexual abuse. Due to the ease of disseminating materials on the web and the impossibility of removing material once it is published, it is very difficult to stop the circle of abuse (Dimc & Dobovsek, 2012).

3. PROJECT DESCRIPTION

In order to ensure the use of effective and modern learning methods, we use state-of-the-art LMS application eCampus to create hypermedia e-learning content and deliver it through a blended learning approach to approximately ten percent of Slovenian primary schools. Prior to the development of suitable e-content adapted to specific groups of learners, we performed a preliminary research in order to identify their existing level of knowledge. Furthermore, we also performed extensive theoretical research of the field.

The developed e-courses are interactive, multimedia (i.e. featuring animations, simulations, video), and therefore promote active learning. The interactive modules simulate real life circumstances and, though interaction, the participants actively learn how to appropriately react when faced with cybercrime or illegal internet content.

The developed modules are implemented with a blended-learning method; namely via face-to-face workshops with each of the target groups (children, teenagers, parents, educators), which will be followed by online e-educational activities. Active involvement of the target groups will be promoted also through a competition among schools based on the highest number of active participants that will reach the highest level of knowledge. At the end of the experiment, we will perform a general evaluation of the project and measure the level of knowledge acquired.

The educational modules include information system security, cybercrime victim protection and support, online safety, online activities and communication via mobile technology, etc. As mentioned, we strive to achieve the active involvement of all participants with special attention paid to the youngest target group (third and fourth graders) by designing learning content specifically for their level of understanding and even providing different case studies for boys and girls.

The objectives and methods of the project include:

- overview and analysis of critical areas of cybercrime related to children and teenagers,
- preliminary research which aims to identify the stakeholders' previous knowledge, behaviour in virtual world, and awareness of Internet frauds,
- development of e-learning materials to be included in the educational modules,
- development of blended learning methods (combination of e-learning and face-to-face learning) in order to achieve active involvement of participants,
- implementation of educational modules in selected schools, and,
- evaluation of results.

To achieve these objectives, various expert areas are incorporated in the project: educational, technological, psychological, sociological, and legal. These experts are involved in the project in order to ensure an all-inclusive cohesive content and an interdisciplinary approach. All experts involved in the project have long-standing experience and expertise in their particular field.

Target groups include selected groups from different primary schools: pupils, parents and teachers. The effect of the educational activities will be evaluated through comparison of a questionnaire/exam prior and following the course, coupled with a questionnaire/exam one month after the course that will also be given to a control group. Since the implementation involves ten percent of Slovenian primary schools, critical mass is sufficient to create the multiplier effect and lead to the long-term success of the project.

4. CONCLUSION

Preliminary research displayed a need for additional education regarding the dangers of cybercrime and the importance of information safety for all target groups. In order to successfully address the issue of cybercrime, it is important to implement successful preventive techniques in all target groups. Therefore, we concluded that continuous education plays an important role in raising the awareness of all users and in encouraging them to implement preventive techniques in everyday life. In order to evaluate the effects of the educational module implementation, an evaluation will be performed following the conclusion of each educational module. Through implementation of these educational modules targeting the youngest Internet users, we will be making the first step toward the creation of an information security culture.

REFERENCES

Cehovin, G., 2010. *Otroška pornografija na internetu*. FDV, Ljubljana, Slovenia.

Gartner, Inc., 2013. *Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013*. Available online: http://www.gartner.com/newsroom/id/2408515 (26.08.2013)

Gregoric, U., 2010. *Socialni inženiring v spletnih socialnih omrežjih*. Available online: http://www.fvv.uni-mb.si/dv2010/zbornik/informacijska_varnost/gregoric.pdf (14.04.2013).

Dimc, M., Dobovsek, B., 2012. *Kriminaliteta v informacijski družbi*. Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenia.

Maurel, L., 2009. *L'identité numérique, bientôt saisie par la loi ?*. Available online: http://scinfolex.wordpress.com/2009/07/17/lidentite-numerique-bientot-saisie-par-la-loi/ (26.08.2013)

Ólafsson, K., Livingstone, S. 2013. *Haddon with members of the EU Kids Online network.: Children's Use Of Online Technologies*. The London school of Economics and political science. Available online: http://eprints.lse.ac.uk/50228/ (26.08.2013).

Rosen, C, 2007. *The new Atlantis. Virtual Friendship and the New Narcissism*. A Journal of tehnology&society.A vailable online: http://www.thenewatlantis.com/publications/virtual-friendship-and-the-new-narcissism (06.04.2013).

Shea, V., 1994. *Netiquette*. San Rafael, CA: Albion Books, Available online:http://www.albion.com/netiquette/index.html (21.08.2013).

Spletno oko, 2013. *Starši in otroci, zavarujte se pred zlorabami na internetu*. Available online: https://www.spletnooko.si/r/9/75/Novice/%20Starsi_in_otroci_zavarujte_se_pred_zlorabami_na_internetu/ (27.08.2013)

Safe.si, 2013. *ABC varnosti in zasebnosti na mobilnih napravah*. Available online: https://www.varninainternetu.si/content/uploads/2013/01/Varnost-in-zasebnost-na-mobilnih-napravah.pdf (31.03.2013).