Blended Learning as a Strategic Method Against the Illegal Use of Internet

Julija Lapuh Bele[1,2], Andreja Sladoje Jemec[2], David Rozman[2] and Maja Dimc[2]
[1]*Faculty of Management and Law, Ljubljana, Slovenia*
[2]*B2 d.o.o., Trzaska cesta 42, Ljubljana, Slovenia*

Keywords: Cybercrime Prevention, Information Security, Blended Learning.

Abstract: The article addresses the issue of strategic prevention and fight against cybercrime related to children and teenagers with the use of blended learning in order to establish greater awareness and increase the knowledge of children, teenagers as, parents and educators regarding illegal internet content and related activities. Based on the theoretical background, practical experience and the analysis of questionnaires, we have prepared blended learning courses for each target group, which aim to raise the awareness of stakeholders (i.e. children, teenagers, teachers, parents) and contribute to cybercrime prevention and victim assistance.

1 INTRODUCTION

The increasing integration of web technologies in everyday life together with the popularity of social networks and development of mobile technology contributes to the creation of an optimal environment for various types of cybercrime and illegal internet content. Children and teenagers represent the most avid users of new technologies and functionalities, while they are at the same time the most naïve. Moreover, the general public is not aware of the severity of the problem.

As a part of the General Programme on Security and Safeguarding Liberties, the European Commission established the Prevention of and Fight against Crime Programme in order to contribute to the strengthening of the area of freedom, security and justice. 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 knowledge and awareness of the general public, children and teenagers in particular, regarding the issue of cybercrime and illegal use of Internet.

The project includes the development and dissemination of best practices in the field of protection and support of cybercrime victims. Existing initiatives in this field are primarily focused on presenting information in different 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 consequently resulting in:

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

We believe that only active involvement of the target groups will produce effective results.

In the EU Kids Online survey, only one third of 9-16 year olds (33 percent) stated that their parents know more about the internet than they do (Ólafsson and Livingstone, 2013). We thus believe that all target groups need to substantially improve their knowledge regarding internet safety and the issues of illegal internet use.

The main aspect of our project is to develop and implement an innovative educational module that will result in active involvement of the target groups in the activities of prevention and fight against illegal internet content and related activities. Namely, the educational modules teach the target groups how to protect themselves, as well as how to appropriately react when faced with illegal internet use, with emphasis on raising the level of reporting to relevant agencies. Additionally, the project

Lapuh Bele J., Sladoje Jemec A., Rozman D. and Dimc M..
Blended Learning as a Strategic Method Against the Illegal Use of Internet.
DOI: 10.5220/0004837401250130
In *Proceedings of the 6th International Conference on Computer Supported Education* (CSEDU-2014), pages 125-130
ISBN: 978-989-758-021-5

addresses the issue of the protection and support of victims of these types of cybercrime not only through the establishment of clear guidelines and recommendations, but also with the establishment of an online cybercrime victim "hot-line".

2 CYBERCRIME PREVENTION

In addition to its various benefits, the internet also contributes to increased exposure to different forms of crime. Today, the Internet enables certain offenses, which were unimaginable in the past. The level of privacy has substantially decreased as the general public willingly publishes personal information, which, of course, once published can never be erased – the fact that the general public, children and teenagers in particular, seem to easily forget. Furthermore, fraud and scams are successfully abusing the virtual environment in which boundaries and time are irrelevant.

Young internet users should be aware of the threats to their identity and wealth, as well as potential future impact of their actions. Furthermore, the core rules of etiquette in the virtual environment should be communicated to all users. Through raising the level of awareness of our children, we will be moving toward the creation of an information security culture in the long run.

2.1 Information Security Issues

Information security is a very wide area. It encompasses both technical security, as well as the threats posed by the users themselves, whether that is due to the lack of knowledge or naivety when exposed to social engineering. In relation to the assurance 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. As the success of a social engineer is the result of greediness, trustfulness, naivety and, especially in younger people, inexperience, protection against social engineering can be implemented only with the users' personal knowledge, attention and care.

Parents can select appropriate software to improve the security on the child's computer or mobile phone. However, unfortunately many parents do not have sufficient knowledge in order to ensure child's safe participation in the virtual environment.

When it comes to information security, we primarily consider PCs and often forget the mobile devices, especially smartphones and tablets. According to Gartner Inc. (Gartner Inc., 2013) the proliferation of lower-priced tablets and their growing capability is accelerating the shift from PCs to tablets. The number of smart phones is also growing rapidly. In January 2013 Center for Safer Internet Safe.si (Safe.si, 2013) published the results of the research among internet users, which suggests that parents consider the appropriate age when a child gets a mobile phone to be 11 years. Almost every teenager has a smartphone. The number of applications for mobile devices cannot be counted. Each user has installed many of them. However, in these devices, we do not pay enough attention to the issue of information security.

Regardless of the platform, the main sources of threats are the interactive functionalities of the modern World Wide Web, especially in relation to social networks. Creating a profile is a prerequisite for joining the social networks. The profile includes information about the user along with pictorial material. When a user creates a profile, he/she can search for other users, different links, and can collect and share contacts list. The use of social network systems is increasingly popular. Interest groups attempt to realize their interests by using such a medium. The common tendency that an individual collects a multitude of "friends" is not derived from the human need for companionship, but from the need for status. For many users it could be said that the whole point of these networks is in the accumulation of as many friends as possible (Rosen, 2007).

In addition to the positive characteristics and trends, such as integration of users with common interests and keeping in touch with real friends worldwide, the users can be quickly exposed to abuse, inconvenience, and invasion of privacy. After creating his/her own profile, the user often forgets that the web is like a "bulletin board" and that the information published on the internet stays there forever. It is practically impossible to trust all online friends as much as friends in the real world, though via online social networks the users often behave in the same way. The consequence of this is the fact that the increased use of online social networks excessively reduces the level of self-protection, while at the same time also decreasing the level of attention, thereby unduly increasing the level of trust (Gregoric, 2010).

Users of the internet should be aware of the risks and pitfalls, as they can ensure their own safety with caution and taking appropriate action. The set of traps and risks may include: poor passwords, spam, fake websites, false internet phone calls, identity theft.

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 social networks. They are exposed to the same threats as seniors, some of which can be devastating. Due to its serious consequences, we have focused on the following forms of crime as it relates to young people:

- Cyberbullying - bullying of children and teenagers (threats, harassment, humiliation, embarrassment, etc.) carried out by children and teenagers with the use of internet, digital technologies or mobile phones.
- Online sexual harassment and grooming – includes all actions with the goal of 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 context.

Child development can be harmfully affected by improper internet content. Inappropriate content constitutes contents that foster violence, spread hate speech and racial intolerance, enable online harassment, humiliation and insults, mockery of bodily defects, distribution of pornographic material to children, encourage dangerous activities, show examples of extreme violence and last but not least allow playing video games with violent and other problematic content. Furthermore, websites such as Pro-Ana promote anorexia, publish photos of boney models and celebrities as an incentive for extreme weight loss called "thinspiration". They promote anorexia and bulimia as a lifestyle rather than as a disease or food disorder. This is a dangerous message to young boys and girls who are in a vulnerable period of adolescence and receptive to environmental influences.

Online pornography has become a global problem. UNICEF estimates that more than 4 million websites, which show juvenile victims and even children younger than two years, can be found on the internet (Cehovin, 2010). Such an experience causes long-term effects on the child's later life both in terms of psychological effects, such as feelings of guilt, responsibility for the abuse, low self-esteem, feelings of inferiority and depression, as well as in the light of the fact that a child is victimized every time anybody watches material depicting his/her sexual abuse. Moreover, due to the simplicity of spreading the materials with the use of web technology, it is very difficult to stop the abuse. It is impossible to completely remove the materials, once published on the Web (Dimc & Dobovsek, 2012).

2.3 Digital Identity

Digital identity is made up of the following four categories of information (Maurel, 2009):

- Authentication elements: email address, user name, password, last name, first name, alias, IP address, etc.
- Data: personal, administrative, occupational, banking, social data, etc.
- Identifiers: photograph, logo, image, avatar, etc.
- Digital traces: contributions to public content management systems such as Twitter, YouTube, Facebook, Wikipedia, etc.

Digital tracks are practically indelible. Internet users, especially children, are unaware that their digital identity may affect their lives. Furthermore, inappropriate comments and posts, inappropriate pictures and videos can lead to abuse and can negatively affect their everyday life.

Active participation on the Internet should be seen as something positive; of course, if a person creates a positive online identity.

2.4 How to Prevent Cybercrime among Youth

Nowadays, parents cannot and should not prohibit the use of online environment and activities on social networks. However, they can increase the awareness of the risks and teach the children how to protect themselves.

Children and teenagers, due to their avid use coupled with naivety, are in much greater danger of publishing too much personal information and creating too open-public profile in social software applications.

Due to the widespread use of social networking sites by children and adolescents, it is important for parents to play an important educative role. Their task is not prohibiting the use, but rather raising the awareness about the consequences of actions performed in the virtual environment. Complete control by parents is practically impossible, since children and adolescents can monitor and change their profiles at school, with friends, via mobile devices. Therefore, the main task of the parents is to communicate the awareness of the potential hazards and teach their children how to appropriately react when faced with troubles online. Adults should supervise children and teach adolescents to recognize the bad in the virtual environment.

Parents and teachers should talk to the children in order to warn them of the risks posed by irresponsible behavior on the internet, and children should have a sense that they can always turn to them. Therefore, the parents should constantly improve their knowledge on the subject.

Parents and children ought to spend some time online together. Children should inform their parents about their favorite websites. Parents should also have control over the time a child spends on the Internet. Child's computer should be in a room accessible by all family members. It must be protected by a filter, which blocks inappropriate content. Parents should also emphasize the value of personal data. They must tell their children that personal data, photos, name, address, school or data regarding their family members should not be given without their permission. Parents ought to alert the children to be careful when faced with any proposal for a meeting from people they met online. Without the knowledge and permission of the parent or responsible adult, a child should know that he/she should not meet anyone, despite the promising potential of the meeting. Children need to be aware that the people they are talking to on the internet may not be who they present themselves to be (Spletno oko, 2013).

3 PRELIMINARY RESEARCH

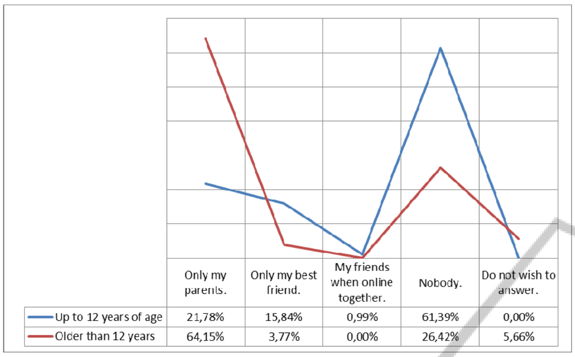
In order to appropriately adjust the learning content included in the project to the current issues and existing knowledge of target groups, we performed a preliminary research dealing with the level of awareness regarding cybercrime and information safety. In addition to the performed analysis on a group of children, teenagers and adults, we also reviewed the existing research in the field of cybercrime and information safety in Slovenia, as well as EU in general. The findings of existing research, combined with the findings of our preliminary analysis, were consequently used for the selection of the key areas to be included in our educational modules.

The analysis was performed with the use of two questionnaires intended for children and teenagers. The first questionnaire was prepared for children up to 12 years of age the second questionnaire was prepared for teenagers (older than 12 years). The first questionnaire contained fewer questions than the second questionnaire, since we assumed that the children in the first group are only beginning to use the internet, while the teenagers are already using a wider variety of internet functionalities. The third questionnaire was prepared for adults (parents and teachers), since we believe it is crucial for parents and teachers to be included in the educational process regarding cybercrime and information safety. Parents and teachers perform a crucial role in the child’s entrance to the virtual world; namely, they should educate the child regarding the positive and negative effects and not merely rely on restriction and control. For the distribution of the questionnaire, the chain-referral sampling method was used; the questionnaire was given to a selected group of participants, which then recruited future subjects among their acquaintances. The total number of participants included 205 adults, 132 children under the age of 12 and 128 children older than 12 years of age.

The children and teenagers included in the analysis all use the internet and only 0.1 percent of the participants stated that they do not have home internet access; however, they use the internet in school. Their answers were compared to the rest of the participants and we found no differences in the level of use and awareness.

The comparison of the answers between children and teenagers displayed differences primarily in their relation toward parents, namely, older children are less likely to turn to their parents when in doubt of when in trouble, which is a reason for concern, especially due to the fact that teenagers spend large amount of time on the internet. The latter can be attributed also to the increasingly wider use of smartphones.

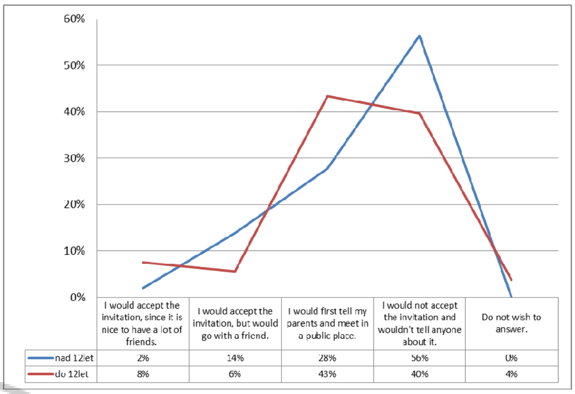
One of the first steps toward securing your information online is undoubtedly the use of passwords. Therefore, we were interested if the children and teenagers are aware of the importance of safekeeping their passwords. The results were encouraging, since 60 percent of the children stated they do not share their passwords with anyone. However, concerning is the fact that the percentage of children who would entrust their friends with their password increases with the age of the child, namely the percentage is very low in case of the children under the age of 12 (approx. 4 percent) and raises sharply with older children (approx. 16 percent). Similar were the findings related to the question of safeguarding privacy on the internet, personal data in particular. We found that younger children are much more likely to consult with their parents (90 percent) before posting personal information, while this percentage drops with the increasing age of the child (58 percent in the group of teenagers).



Graph 1: Who would you entrust with your passwords?

In addition to their attitude toward safeguarding their privacy while online, we were also interested in how the children and teenagers establish new contacts and create friendships online, and how they would react when faced with an invitation from an online acquaintance to meet in real life. The amount of friendships created and maintained online undoubtedly increased greatly with the wide popularity of social networks. The research results displayed that children in general do not discuss the difficulties they encounter online. More than half of teenagers included in the research stated that they would not meet in real life with a person they meet online; however, they would not tell anybody about the invitation to meet. The fact that almost 8 percent of children would accept the invitation to meet should raise concern. Furthermore, almost half of teenagers stated that in case their online "friend" would ask them to keep a secret, they would do so without additional questions.

Overall, the research displayed a concerning lack of awareness regarding the dangers of cybercrime, cyber-bullying in particular, since 46 percent of teenagers stated they are not particularly concerned regarding this issue and would simply ignore it if encountered with a case of cyber-bullying. The results of the analysis thus pointed out certain areas of concern where additional education of children and teenagers is needed in order to avoid further problems. Children and teenagers should be aware of the positive and negative points of the use of internet, and should be taught how to continue their self-education regarding cybercrime and internet safety.



Graph 2: What would you do if a person you met online would ask you to meet in person?

4 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 blended learning approach to approximately 10 percent of Slovenian primary schools.

LMS system is a web application designed for all platforms and devices, including tablets and smartphones.

The primary objective of the project is the development and implementation of educational modules for the field of cybercrime related to children and teenagers, which are designed for specific target groups, namely children, teenagers, parents and teachers.

The educational modules include the field of information system security, cybercrime victim protection and support, online safety, online activities and communication via mobile technology, etc. and strive to reach active involvement of all participants. Special attention is paid to the youngest target group (3rd and 4th grade) by designing learning content specifically for their level of understanding and even providing different cases 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,
- 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 blended learning modules in selected schools, and
- evaluation of results.

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

A project management methodology is used in all phases of the project to ensure the control over all project activities and ensure stable use of resources. Furthermore, the inclusion of relevant parties in the project team or as external evaluators aids the implementation, as well as continuance, of the project objectives after the formal end of the project.

The target group includes selected groups from different primary schools - their pupils, parents and teachers. The effect of the performed 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 be performed also on a control group.

Since 10 percent of Slovenian primary schools participate in the project, the critical mass is reached in order to create multiplying effects and lead to the long-term goal of the project, which is to continue the educational activities culminating in the implementation of the developed modules in the obligatory educational curriculum.

Furthermore, the project includes the development and dissemination of best practices in the field of protection and support of cybercrime victims in relation with these types of cybercrime.

5 CONCLUSIONS

The presented preliminary research, coupled with research performed with parents and educators displayed a need for additional education of all target groups regarding the dangers of cybercrime and the importance of information safety. In order to successfully address the issue of cybercrime, it is important to implement successful preventive techniques in all target groups; therefore, continuous education undoubtedly plays and important role in raising the awareness of all users and encourages them to implement the preventive techniques in everyday life. In order to evaluate the effects of the educational module implementation, an evaluation of the effects will be performed following the conclusion of each educational module. Through the implementation of the educational modules that will target our youngest internet users, and consequent recommendations for further actions, we will be making the next step toward the creation of an information security culture.

REFERENCES

Čehovin, G., 2010. Otroška pornografija na internetu. FDV, Ljubljana.

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).

Gregorič, 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. Dobovšek, B., 2012. Kriminaliteta v informacijski družbi. Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana.

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. 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., 02007. The new Atlantis, A Journal of tehnology&society. Virtual Friendship and the New Narcissism. Available online: http://www.thenewatlantis.com/publications/virtual-friendship-and-the-new-narcissism (6.april.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. 3. 2013).

Shea, V., 1994. Netiquette. Albion Books, San Rafael, CA.

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/ (27.8.2013).