Violence in Cyberspace and Possible Prevention

Maida Bećirović-Alić [1], Muzafer Saračević [2]

[1] *Department of law sciences, University of Novi Pazar, Dimitrija Tucovica bb,*
Novi Pazar, Republic of Serbia
[2] *Department of computer sciences, University of Novi Pazar, Dimitrija Tucovica bb,*
Novi Pazar, Republic of Serbia

***Abstract* - This paper describes some of the forms of violence in cyberspace and possible prevention. The second part of this paper provides an analysis of students' views on possible online abuse and prevention. The research aims to highlight statistically significant opportunities for raising awareness of possible online abuse and the prevention of cyberbullying. The survey consists of a total of 20 testimonials, which are divided into 4 parts, and each part assesses different aspects. The conclusion of this research is that the Internet environment does not provide enough feedback on the reactions of the person to whom the harassing messages were sent, which in the abuser reduces the feeling of causing true emotional and psychological harm to another person, reducing the degree of self-control and insight into the level of bullying.**

***Keywords* - Violence in Cyberspace, Data protection, Prevention mechanism, Digital violence, Identity theft.**

1. Introduction

Information security is one of the most current and important topics faced by IT users and providers today.

Until recently, many users did not take security seriously enough. They believed that if their server and mainframe computers were housed inside a secure facility that could only be accessed by a limited number of authorized users, it was unlikely that they would ever face a security breach. However, the widespread use of PCs, PDAs, and wireless devices, aided by a keen interest in the use of the Internet and other computer networks, has led to the image of computers operating safely in a physically secure location today not nearly as realistic as it used to be [10]. Those are the reasons for the great concern of the executives, managers, and other users for the best possible security of the system.

Accordingly, a lot of radical changes are being made in the organization of the information security service. Information security issues and the problem of information protection have fallen from the margins to the scope of work of top management within companies. Therefore, the interest and attention paid to information security in the world is not a reflection of the fashion trend, but the reality of the upcoming information society. Along with the violation of business information, there is also the violation of private (personal) and thus the so-called cyberbullying that opens the door to various abuses, including harassment, phishing, and identity theft.

Electronic violence (or digital violence) involves any form of messaging via the Internet or mobile phones, all to injure, harass, or otherwise harm a child, young, or adult who cannot protect himself from such acts [7]. It appears in the form of text, audio or video messages, photos, or calls. The term "Cybercrime" is a broader term than cyberbullying because it covers a wide range of crimes such as cyberbullying, copyright and related offenses, content-related content, acts against confidentiality, integrity, and availability of computer data and systems, etc. [4]

Computer forensics also involves the act of producing digital data suitable for involvement in criminal investigations. Computer forensics greatly

DOI: 10.18421/SAR52-03
https://doi.org/10.18421/SAR52-03

Corresponding author: Maida Bećirović-Alić,
Department of law sciences, University of Novi Pazar, Dimitrija Tucovica bb, Novi Pazar, Republic of Serbia
Email: maida.becirovic@uninp.edu.rs

Received: *16 April 2022.*
Revised: *03 June 2022.*
Accepted: *08 June 2022.*
Published: *27 June 2022.*

helps police officers identify both parties, victims, and perpetrators of identity theft [5].

The second part of this paper provides an analysis of students' views on possible online abuse and prevention. The research aims to highlight statistically significant opportunities for raising awareness of possible online abuse and the prevention of cyberbullying. The survey consists of a total of 20 testimonials, which are divided into 4 parts, and each part assesses different aspects.

2. Possible Threats on the Internet and Identity theft

Internet privacy includes the right to protect personal information regarding the storage, use, protection from third parties, and the display of personal information online. Protection may also include personal identifying information or information relating to a visitor to a particular website.

Identity theft on the Internet is a type of fraud by which personal and financial information is learned from computer users through fraudulent emails or websites. The Internet provides new ways for thieves to steal someone else's personal information and commit fraud. Thieves can achieve their goal in several ways, such as using Internet chat and trojans to pick up passwords, usernames, and credit card numbers that a user uses on their computer when registering, logging in to a website, or performing online purchases and sending them back to the thieves. This is another way to access someone else's personal information.

In addition, there is a so-called e-mail phishing, where thieves attempt to collect someone else's personal information by sending false e-mails [8]. Identity theft on the Internet can be done in many ways, the most common are:

1. via email or phishing;
2. through malicious software (eg. Trojan horses, spyware, keylogger, and etc.);
3. via social networks (Facebook, Twitter, Linkedin, etc.).

Academic research has shown that social networks operate at multiple levels, ranging from family to national level, and play a critical role in determining how certain problems will be addressed, how organizations will function, and the degree to which an individual will succeed in reaching individual goals. Due to the great access to the personal data of users, there is often a great misuse of this information. It is not uncommon for various developers or hackers to break into network systems, where they do considerable harm to both users and administrators. Most often victims are minors, who are easy targets of these types of abuse [3]. Due to similar reasons, many of the services have protection for minors, which to some extent provides them with safer use of the service. There are also several malicious items, i.e. viruses, which, hiding in the form of marketing, or various add-ons, can invade our computer system and do great damage. Therefore, the user should always be careful with these items [6].

Email may seem like a reliable way to have a conversation between two people, safe from third-party eavesdropping. However, the message can be intercepted anywhere in the path between the sender and the recipient at any time. If one sends an email from work, his/her boss can legally have access to their email, and if one's business is prosecuted at any time, the prosecutor or the party suing her/him has the legal right to review their email and he/she has a legal obligation to give them insight. If one sends an email from home, hackers can intercept it, or if one is under investigation by the authorities, they can seize the electronic record with the appropriate account. Even their ISP can legally control his/her email.

Email is vulnerable to both types of attacks - active and passive. Passive threats are directed to the specific content of the message (Release of message contents) and analysis of traffic (Disclosure of Information), while the active ones are directed to the modification of content (Modification of message contents), responses (Replay), Masquerade and unavailability of the service. Some of the abuses by email [8] are:

1. Disclosure of Information: Most emails are currently broadcast publicly, without encryption. Using some of the tools available, a third party can read your email.
2. Traffic Analysis: It is suspected that some countries routinely monitor emails for national security purposes. They are doing this to facilitate the fight against industrial espionage and political wiretapping.
3. Modification of message contents: The message may be modified during transmission or storage.
4. Masquerade: It is possible to send a message on behalf of another organization or other person, ie. impersonate.
5. Replay reply: Already received messages can be sent to some new recipients. This can lead to loss, confusion, or damage to the reputation of the individual or organization.
6. Spoofing: False messages can be inserted into another user's system. This can be accomplished within a local network or from any other environment, using a virus known as a Trojan horse.
7. Denial of Service -DoS: Blocking of the e-mail system can be blocked by overflowing with e-

mails. It can also be sent by sending an email with a Trojan horse or some similar virus. It is also possible to block an account by entering the wrong password again.

The school can have a huge impact and role in fostering Internet etiquette and improving IT literacy. Information technology has been successfully used for both formal and non-formal learning. The role of the school, in this case, is to research and provide accurate information in various ways of using the Internet to provide students with self-affirmation, assertiveness, participation, and developing friendships [1]. Students need to show that adults, as digital newcomers, are closely following all current changes in information technology. New Forms of Communication give digital newcomers insight into the interests of digital natives. Therefore, an effort is made to define clear rules in the use of the Internet and mobile phones in the school environment. Five Key Areas for Effective Prevention of Electronic Violence [9]:

- Highlighting the positive use of technology;
- Understanding and discussing modern communication methods and the dangers of cyberbullying;
- Establishing new and refining existing rules and consequences;
- Enabling reporting of electronic violence;
- Evaluation of the impact of prevention activities.

3. Analysis of Pupils Attitudes on Possible Abuse on the Internet and Possible Mechanisms Relating to Prevention

This part of the paper provides an analysis of students' views on possible online abuse and prevention. The survey was conducted at an elementary school in Novi Pazar. The research aims to highlight statistically significant opportunities for raising awareness of possible online abuse and the prevention of cyberbullying.

The survey was conducted from 18th to 27th November 2014. A total of 36 respondents (6th to 8th-grade students) applied for the electronic survey. Students rated the testimonials 1 to 5 (1 - I disagree at all, 2 - mostly disagree, 3 - indecisive, 4 - mostly agree, 5 - strongly agree). The survey consists of a total of 20 testimonials, which are divided into 4 parts, and each part assesses different aspects (see Table 1):

- Part 1: Knowledge of possible dangers on the Internet;
- Part 2: Risky behavior on the Internet;
- Part 3: Possible prevention and counseling;
- Part 4: The effectiveness of software protection tools.

Table 1. Different assessment criteria

ASSESSMENT CRITERIA 1: KNOWLEDGE ABOUT POSSIBLE HAZARDS ON THE INTERNET	**1**	**2**	**3**	**4**	**5**
The Internet is a safe environment if appropriate anti-virus software is used	22	9	1	2	2
Email is a secure web service	21	10	1	2	2
Posting inappropriate content is not allowed on social networks	25	7	2	1	1
Posting private information or falsehood on a chat, blog or website is not part of cyberbullying	12	8	10	3	3
Forwarding someone else's photos or any content about anyone else with a request for comment is not an identity theft	18	10	6	2	0
Total 36 students	**54.44**	24.44	11.11	5.56	4.44
ASSESSMENT CRITERIA 2: RISK BEHAVIOR ON THE INTERNET	**1**	**2**	**3**	**4**	**5**
When I correspond, I do not always bear in mind the possibility of impersonation on the other hand	21	8	1	4	2
I would go to a meeting with a person I met via mobile, social network, chat, or blog	23	8	0	1	4
I always send photos of myself, my family and friends because I feel I cannot abuse them	17	7	0	9	3
I always delete mobile data and photos that someone sent me because I don't think the police will find the person threatening me faster.	29	5	0	2	0
I do not ask for help from others so that they do not think that I have done anything illicit	22	6	1	3	4
Total 36 students	**62.22**	18.89	1.11	10.56	7.22
ASSESSMENT CRITERIA 3: POSSIBLE PREVENTION	**1**	**2**	**3**	**4**	**5**
The public in Serbia is well acquainted with the term cyber-electronic violence.	18	12	3	2	1

Children are not the most vulnerable category of internet users, they are companies	24	8	3	1	0
Workshops at schools are not the best form of education in the field of prevention of electronic violence, but rather informative articles in the media and internet campaigns	17	10	5	2	2
Public institutions and non-governmental organizations cannot help enough in fighting electronic violence in Serbia	15	12	0	2	7
The big cities (Belgrade, Novi Sad, Nis, ..) are the parts of Serbia where the most necessary education is in the field of prevention of electronic violence	14	16	4	1	1
Total 36 students	**48.89**	32.22	8.33	4.44	6.11
ASSESSMENT CRITERION 4: EFFICENCY OF SOFTWARE PROTECTION TOOLS	**1**	**2**	**3**	**4**	**5**
I believe that I do not need software protection because I do not leave my information on the internet and do not act risky	14	15	1	4	2
I use more often software tools (applications) that I download for free than the commercial ones	4	5	0	12	15
I believe that I cannot be compromised via email because of included software inside the internet browser that protects me	9	7	3	11	6
Facebook is safe when it comes to identity theft because there is automated software that removes duplicates	7	5	5	8	11
I believe that the antivirus I currently have protects me completely from all forms of violence and identity theft in an online environment	5	4	3	11	13
Total 36 students	**48.89**	20.00	6.67	**25.56**	**26.1**

4. Discussion

If we analyze the individual results, for each assessment criterion, we can see that over 50% of students have sufficient knowledge about possible dangers on the Internet (Criterion 1), and over 60% of students know when they are at risky behavior on the Internet (Criterion 2). It is certainly important to emphasize raising awareness among children and their parents of all possible threats when using modern technologies in communicating with others.

Consequences and sanctions should be defined for all those who break the rules or commit violence. It is also very important that students and their parents are supported by the school, for any form of violence, even in cases when the violence occurred outside the school. However, testimonials under Criterion 3 have been correctly evaluated below 50%, i.e. most do not know how to seek help and the right advice for effective prevention of electronic violence. Based on the results obtained, we conclude that reporting violence can be a difficult step, both for those who suffer from violence and for observers.

This is why efforts are being made to get students and their parents acquainted with the different ways of reporting cyberbullying in school and among students. School workers and associates have to be aware of the application options and who needs to be addressed in such situations. Statements under Criterion 4 were correctly rated below 25%, which again indicates the students' poor awareness of the application of security software tools and their reliability and efficiency. Based on the cumulative results for all four assessments, we can see that 10.97% of students stated that they completely agree with the stated statements, while 11.53% of students partially agree with the stated statements.

Since the statements are formulated in a form that is opposite to the correct answer, we conclude that about 22% of students are not very well versed in the field of cyberbullying and that further education should be pursued.

On the other hand, as many as 46.81% of the students denied the statements given, that is, they stated that they did not completely agree with the stated statements, while 23.89% of the students partially disagreed with the stated statements.

We find that about 70% of students would know how to recognize a form of cyberbullying.

Table 2 gives details by a number of estimates selected (from 1 to 5) for all four criteria [11].

Table 2. Summarized results for all 4 estimates

Assessment criterion:	1	2	3	4	5
1: Knowledge of possible dangers on the Internet	54.44	24.44	11.11	5.56	4.44
2: Risky behavior on the Internet	62.22	18.89	1.11	10.56	7.22
3: Possible prevention and counseling	48.89	32.22	8.33	4.44	6.11
4: Effectiveness of security software tools	21.67	20	6.67	25.56	26.11
%	**46.81**	**23.89**	**6.81**	**11.53**	**10.97**

From the above survey, we conclude that further education on violence in the Internet environment is necessary. What is important is to provide accurate insight into the very definition of electronic violence, that is, it is important to emphasize how electronic violence differs from other forms of violence, what are its specificities, and what are the impacts of such violence. Clear rules need to be devised and laid down and strictly adhered to. It is strongly recommended to keep a record of students' experiences online, that is, to evaluate the impact of preventive activities (Research: Child safety on the Internet, [2]).

Regular checks are very important to determine if prevention strategies are successful and appropriate to students' needs. It is useful to share materials and share information on actions taken, results achieved, as well as current challenges and issues with the entire school community.

5. Conclusion

The values and rules that exist in a school for peer violence should also be applied to violence in the electronic media. Five years ago, UNICEF launched a public campaign against peer abuse, and for four years its program, For a Safe and Encouraging School Environment, has been implemented in schools. So far, more than 250 primary and secondary schools have enrolled in the program. An external evaluation showed that the program successfully reduced the amount of peer abuse and established a safer environment for children. Electronic abuse has not been covered by the program so far, as it is a relatively new form of abuse, both peer and general.

It is important to note that the specificities of the Internet environment make the electronic form of abuse more widespread and, in some opinions, even more, dangerous to the psychological balance of the victim than traditional peer abuse.

The conclusion is that the Internet environment does not provide enough feedback on the reactions of the person to whom the harassing messages were sent, which in the abuser reduces the feeling of causing true emotional and psychological harm to another person, reducing the degree of self-control and insight into the level of bullying.

References

[1]. Diamanduros, T., Downs, E., & Jenkins, S. J. (2008). The role of school psychologists in the assessment, prevention, and intervention of cyberbullying. *Psychology in the Schools*, *45*(8), 693-704.

[2]. Kralj, L. (2014, May). Children's safety on the Internet-development of the school curriculum. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 593-596). IEEE.

[3]. Kovačević-Lepojević, M., & Lepojević, B. (2009). Victims of cyberstalking in Serbia. *Temida*, *12*(3), 89-108.

[4]. Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research press.

[5]. Vacca, J. R. (2002). *Computer forensics: computer crime scene investigation*. Charles River Media, Inc..

[6]. Stevanović, B. (2006). Computer forensics: Incident response. *Info M*, *5*(17), 11-16.

[7]. Casey, E. (Ed.). (2001). *Handbook of computer crime investigation: forensic tools and technology*. Elsevier.

[8]. Ramzan, Z. (2010). Phishing attacks and countermeasures. *Handbook of information and communication security*, 433-448. https://doi.org/10.1007/978-3-642-04117-4_23

[9]. de Leeuw, R. N., Rozendaal, E., Kleemans, M., Anschutz, D. J., & Buijzen, M. (2014). An experimental study on prosocial television news for children and prosocial behavior. *Tijdschrift Voor Communicatiewetenschap*, *42*(4), 342.

[10]. Turban, E., McLean, E., & Wetherbe, J. (2004). *Information technology for management: Transforming organizations in the digital economy*. Wiley Text Books .

[11]. Divić, K., & Jolić, I. (2019). Rizično ponašanje djece i mladih u virtualnom okruženju–Iskustvo Centra za pružanje usluga u zajednici „Savjetovalište Luka Ritz ". *Napredak: Časopis za interdisciplinarna istraživanja u odgoju i obrazovanju*, *160*(3-4), 265-290.