# Assessing Information Security Awareness among Secondary School Teachers

Kristijan Klasan *, Ivan Dunđer *, Sanja Seljan *
* Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb, Zagreb, Croatia
kklasan@ffzg.unizg.hr, idundjer@ffzg.unizg.hr, sanja.seljan@ffzg.unizg.hr

*Abstract* — **Every year there is a continuous increase in cyber threats all over the world. Threats appear in both the private and public sectors. In Croatia, state services in the public sector are particularly affected. This is especially pronounced in schools of all levels of education. They are considered sources of confidential information, valuable to hackers, with relatively unprotected computer systems. In addition, insufficient knowledge of school employees and teachers about the dangers of cyber threats does not help either and can result in uncertainty and confusion when crisis situations occur. The level of information security-related knowledge of every computer user is not the same, therefore this paper aims to investigate the awareness of information security among teachers. The authors decided to conduct a focused study on 72 secondary school teachers from 13 secondary schools in Karlovac County, examining their knowledge on potential threats and security measures. This research is based on a survey and subsequent quantitative and qualitative analyses. The results can provide insights into information security awareness levels and the current state of knowledge of employees in the public education system. This may also reveal topics that need to be addressed during lifelong learning activities to increase understanding of potential threats and appropriate countermeasures.**

***Keywords - information security; cyber threats; computer systems; education; teachers; lifelong learning; information and communication sciences***

## I. Introduction

Protecting personal computers from cyber threats is a substantial problem that dates to the era of the first computers. No matter how much one invests in the security and protection of computer systems, absolute security cannot be guaranteed.

Schools are often faced with a lack of financial resources for the maintenance and purchase of new computer equipment, which can consequently cause difficulties in ensuring the necessary level of protection. In the United States, schools spend about 8% their IT budgets on cyber security [1].

Student behavior while working on a school's computer can be problematic as well. According to the results of a research conducted in the Netherlands, students do not develop knowledge about information security in primary and secondary schools, but mostly acquire their knowledge through personal experiences [2].

Sometimes students run various programs, including computer viruses they find on the internet, all under the guise of having fun and proving their abilities to classmates and teachers. Less computer protection may also come from teachers. A disabled firewall is common, since it can block the seamless operation of certain programs that are used for teaching, so teachers turn them off as not to disrupt the course of a lesson. This becomes especially problematic if a computer is available and used by all teachers, e.g. for the preparation of lessons.

The results of a previous research show that numerous teachers seem to be uninformed about information security. Most were unaware of what makes a strong password, how to protect personal information, and how to securely store and access data. Furthermore, some teachers have negative attitudes towards technology, which consequently reduces their desire to learn or increase their awareness of information security issues [3].

This paper aims to investigate how knowledgeable teachers are about information security, and how much they know about protecting their computers. The remainder of the paper is structured as follows: computer security threats and protection methods are presented in Section II. Related work is presented in Section III. Research methods and results are presented and discussed in Section IV. Limitations and recommendations are presented in Section V, whereas conclusions are drawn in Section VI.

## II. Computer Security Threats and Protection Methods

The main source of threats to any computer are malicious programs. They can be defined as malicious software that exists on a computer without the knowledge and consent of the computer user [4]. They take advantage of human inattention and various weaknesses of the computer system, which can lead to computer damage and loss of valuable data.

The basic group of malicious programs includes computer viruses, worms, logic bombs, Trojan horses, rootkits, ransomware, spyware and adware programs. In addition to the ones mentioned, there are many others.

A **computer virus** is a program that independently replicates and spreads through computers with the goal of disrupting the normal use of computers [5]. **Computer worms** are programs that spread their functional copies to other computers via the network [6]. A **logic bomb** is a

malicious code that lies dormant and hidden inside legitimate software, until a condition (e.g. an event or a date) is met to trigger a payload [7]. A **Trojan horse** is a type of malicious program that tries to allow a remote user to gain control over the computer, steal data or compromise the computer's security [8]. A **rootkit** is a type of malware that is activated every time the system is booted. The program is difficult to detect because it is activated before the operating system is fully booted, and it allows the installation of hidden files and running processes in the operating system [4]. **Ransomware** is malicious software that infects a victim's device and suddenly demands the payment of a ransom for the data encrypted by the ransomware [9].

With the development of technology, spy components are becoming increasingly prominent as an integral part of today's standard programs that users have on their computers. Companies invest heavily to collect valuable data that is of interest to them. In order to access sensitive data, they rely on the use of spyware and adware programs. **Spyware** programs can be defined as programs for monitoring activities on a computer without the user's knowledge [4]. The goal of such programs is to steal valuable data, passwords, to monitor user searches etc. [8]. **Adware** can be defined as a program that automatically displays or downloads advertising material from the internet [10]. Its main task is to display advertising content as similar as possible to a user's search [8].

In addition to malicious programs, major problems in information security are generated by unsolicited e-mails, such as **spam** and **phishing** messages [11-13], and weakly protected passwords. Moreover, phishing has become a standard for trying to trick users into revealing and sharing sensitive data.

There are many different computer protection tools and techniques. However, the problem arises of how to recognize and choose an adequate solution with regard to needs and costs. Technology, such as **antivirus programs** and **firewalls**, significantly increase the security of a computer. For instance, an antivirus program works in order to protect a computer from malware by scanning files and comparing signatures to a database of known file signatures [14]. In addition to antivirus programs, it is recommended that the user has a firewall turned on, which will additionally protect the computer from unwanted network traffic, such as incoming network packets from suspicious IP addresses [4].

## III. Related Work

The following subsections provide an overview of data on cyber-attacks in Croatia, and related research on the topic of information security from around the world, with a focus on educational institutions.

### *A. Cyber-attacks in Croatia*

When it comes to cyber-attacks in Croatia, according to the National CERT, during the year 2022, 1296 reports were classified as computer security incidents and were processed accordingly. The attacks occurred in all sectors, including educational institutions such as schools. Among the leading types of incidents were phishing, scam, password guessing, and ransomware attacks [15].

### *B. Recent Studies from Europe*

To increase awareness of information security, a survey was conducted in Italy as part of a national project. The aim was to determine the perception of Italian teachers about digital awareness. More than two thousand primary and secondary school teachers participated in the research. The results confirm the need for special training on digital awareness [17].

In order to determine the level of knowledge of teachers, a survey was carried out to examine the extent to which Dutch students acquire knowledge about information security in primary and secondary schools. A questionnaire was used for self-assessment of cyber security behavior. The results of this particular research show that students mostly acquire their knowledge through personal experience, instructions on the internet, from their parents, but least of all, at school [2].

### *C. Recent Studies from the Rest of the World*

In 2020, an online survey was conducted with the aim of studying the level of awareness of teachers about cyber security in which 92 teachers from secondary schools in Karnataka, India participated. The results show that teachers have a medium level of awareness of cyber security, and that there is no significant difference in awareness among teachers regarding their gender and education [18].

A similar research was conducted in Kenya in 2020, where a total of 172 teachers from 86 Kenyan secondary schools participated. The results indicate that teachers did not have access to information security education, and had little or no knowledge of basic practices, and risks of attacks [3].

Another research was conducted in Taiwan, where the main goal was to investigate the level of cyber security awareness among 250 schoolteachers. The results showed that teachers were not familiar with many activities in the domain of cyber security [19].

In the period between June 2022 and May 2023, as many as 107 incidents related to attacks on educational institutions were recorded in the USA. Then comes the United Kingdom with 28 reported attacks, followed by Australia with 7 and Canada with 6 reported attacks [16]. In 2021, more than 670000 students are believed to have been affected by malicious attacks, and the damage was so severe that schools had to close their doors or suspend services until further notice. The victims of the attack were mostly K-12 schools [1].

## IV. Research

This section consists of three subsections: research method, sociodemographic data, and research results. The first subsection deals with the process of acquiring necessary data from respondents by using an online questionnaire, whereas the second subsection presents respondents' sociodemographic data, such as gender and age, graduate field, teaching experience, and career advancement. The third subsection discusses the results of this research in a quantitative and qualitative way.

The main goal of this research was to investigate the level of awareness of information security among secondary school teachers in one Croatian county. This was done by examining the self-assessment of teachers' i) habits and former cybercrime experiences, and ii) knowledge and techniques for protecting computers from cyber threats and crime in the educational system. The research was conducted online through a survey that was focused on:

- **habits and experiences**: information related to the general computer protection habits, and the respondents' experience as a victim of cybercrime (presented in Table III),
- **knowledge and techniques**: information related to specific computer protection knowledge and techniques (presented in Table IV).

The following two research questions were raised:

- Q1: What are the habits and experiences of secondary school teachers in the selected county?
- Q2: What security measures do secondary school teachers use to protect their computers in the selected county?

### *A. Research Method*

The research in the form of a survey was conducted from December 2023 to January 2024, with the aim of examining the self-assessment of teachers' knowledge and awareness of information security, and techniques and ways of protecting computers from cyber threats and crime in the educational system.

The research was conducted on a sample of 13 secondary schools in Karlovac County. Vocational schools and gymnasiums were taken into account, thus covering both forms of secondary education in Croatia. The list of included schools is shown in Table I along with the number of respondents from each school and the relative proportions.

The research was conducted using a questionnaire that was designed by the authors (with statements and questions defined by the authors), completely anonymous and which targeted secondary school teachers without an age limit.

It gathered sociodemographic data about the respondents, general familiarity with the presented topic, as well as type of methods used to protect against computer security threats. Statements from the questionnaire were formulated in such a way that they were based on the experience of teachers and their daily practice and routines.

For the questionnaire to reach all teachers at a school, the authors of this paper contacted every school's principal. Therefore, in the first phase of this research, all e-mail addresses of school principals had to be collected. The addresses were found on the official websites of schools. Principals were sent an e-mail, in which they were asked to participate in the research, and the possibility of delivering the questionnaire to teachers through their internal media communication channels. In order to be able to participate in the research, each teacher was obliged to accept the conditions of the research and to give consent for their answers to be used for the purposes of this study.

All schools in Karlovac County participated in the research, and the exact number of participants was recorded for each.

TABLE I. SCHOOLS INCLUDED IN THE RESEARCH

| School | Number of respondents | Percentage |
|---|---|---|
| Science School Karlovac | 23 | 31.9% |
| Medical School Karlovac | 9 | 12.5% |
| Gymnasium Karlovac | 7 | 9.7% |
| Vocational and Technical School Ogulin | 7 | 9.7% |
| High School Slunj | 6 | 8.3% |
| Forestry and Carpentry School Karlovac | 5 | 6.9% |
| Technical School Karlovac | 3 | 4.2% |
| Economic and Tourism School in Karlovac | 3 | 4.2% |
| High School Duga Resa | 3 | 4.2% |
| Trade and catering school Karlovac | 2 | 2.8% |
| Industry and Trade Vocational School Karlovac | 2 | 2.8% |
| Music School Karlovac | 1 | 1.4% |
| High and Vocational School Bernardin Frankopan Ogulin | 1 | 1.4% |
| ***Total*** | **72** | **100%** |

The majority of respondents were from the Science School Karlovac, and the least from the High and Vocational School Bernardin Frankopan Ogulin (Table I).

The questionnaire was divided into 5 parts, and there were no correct or incorrect. The structure of the questionnaire was as follows.

The first part contained instructions and guidelines for completing the survey. Each respondent had to confirm familiarity with the conditions of the research and give consent for their responses to be stored and used for this research.

The main content of the survey started from the second part, which dealt with the respondent's sociodemographic data, such as gender, age, school of employment, teaching experience, field of graduation, and promotion status (career advancement).

In the third part of the questionnaire, there were 5 short statements (presented in Table III) that checked the habits of computer protection methods and cybercrime-related experiences of the respondents. The answers to the statements were given in the form of "yes", "no", "I don't know". Each respondent had to mark one of the offered short answers, and could not proceed with further solving the questionnaire until all answers were given.

In the fourth part, there were 13 statements aimed at examining knowledge about computer protection methods, and available computer protection tools (presented in Table IV). Respondents had to express their degree of agreement with the statements on a scale from 1 to 5, where the numbers indicated: (1) completely disagree, (2) mostly

disagree, (3) neither agree nor disagree, (4) mostly agree, (5) completely agree.

In the fifth part of the questionnaire, questions were asked about password setting strategies, and about the respondents' interest in participating in information security education. These questions were optional, and therefore not relevant for answering the two research questions (Q1 and Q2).

### *B. Sociodemographic Data*

A total of 72 respondents from 13 secondary schools participated in this research. Table II lists the respondents' basic sociodemographic data, including their gender, age, years of teaching experience, graduate field, and career advancement. Column *n* indicates the number of respondents, whereas the last column represents their relative proportion.

TABLE II. SOCIODEMOGRAPHIC DATA ON RESPONDENTS

| Basic characteristics | n | % of respondents |
|---|---|---|
| *Gender* | | |
| Male | 15 | 20.8 |
| Female | 57 | 79.2 |
| *Age ranges (in years)* | | |
| up to 30 | 11 | 15.3 |
| 31 - 40 | 16 | 22.2 |
| 41 - 50 | 20 | 27.8 |
| 51 - 60 | 19 | 26.4 |
| more than 60 | 6 | 8.3 |
| *Teaching experience (in years)* | | |
| less than 2 | 11 | 15.3 |
| 2 - 5 | 7 | 9.7 |
| 6 - 10 | 11 | 15.3 |
| 11 - 20 | 18 | 25 |
| more than 20 | 25 | 34.7 |
| *Graduate field* | | |
| Social Sciences | 19 | 26.39 |
| Humanities | 14 | 19.44 |
| Natural Sciences | 13 | 18.06 |
| Technical Sciences | 9 | 12.5 |
| Biomedicine and Health Sciences | 8 | 11.1 |
| Biotechnology | 5 | 6.9 |
| Art | 2 | 2.8 |
| Other | 2 | 2.8 |
| *Career advancement* | | |
| Teacher | 58 | 80.6 |
| Mentor | 9 | 12.5 |
| Advisor | 4 | 5.6 |
| Excellent advisor | 0 | 0 |
| Other | 1 | 1.3 |

According to Table II, the majority of respondents were between the ages of 41 and 50. Most of the respondents graduated in the field of social sciences, and currently work as regular teachers without promotion. Most respondents answered that they have over 20 years of teaching experience.

### *C. Research Results*

The research results were obtained by analyzing the responses on the i) habits and experiences (with possible responses being "yes", "no", "I don't know") , and ii) knowledge and techniques (responses on a 1-5 Likert scale). The collected data was processed in Excel using pivot tables. The analysis covers basic measures of descriptive statistics, which includes the arithmetic mean, confidence intervals and standard deviation.

First, the data related to the respondents' habits and experiences were processed (Table III).

TABLE III. RESULTS ON THE RESPONDENTS' HABITS AND EXPERIENCES (POSSIBLE RESPONSES: "YES", "NO", "I DON'T KNOW)

| Statement | yes | no | I don't know |
|---|---|---|---|
| *S1: I use an antivirus program to protect my computer.* | 61 | 7 | 4 |
| *S2: I use a firewall on my computer.* | 28 | 17 | 27 |
| *S3: I have an anti-spyware program installed on my computer.* | 22 | 18 | 32 |
| *S4: I use the same password to log in in to multiple different applications.* | 33 | 39 | 0 |
| *S5: I have been a victim of cybercrime at least once.* | 8 | 56 | 7 |

Statements related to the habits and experiences show that almost 85% of respondents (61 out of 72 respondents) use an antivirus program to protect their computer, which is the highest positive score. Other positive scores range between 30%-39%, meaning that only one third or less of respondents use a firewall or an anti-spyware program. 54% of respondents (39) do not use the same password for different applications, i.e. 46% or almost half of the respondents use the same password for different applications. A large number of respondents (from 37.5% to 44.5%) have answered "I don't know" on statements related to the use of firewalls and anti-spyware programs.

In conclusion, most teachers stated that they use an antivirus program to protect their computers (S1). When asked about the use of firewalls, it is a worrying fact that a third of the teachers answered that they do not know if they use a firewall, which can be interpreted as teachers not having enough knowledge about it and how to configure it (S2). To the statement regarding anti-spyware software (S3), respondents mostly answered that they do not know if they have it installed on their computer. When it comes to using a single password for different applications (S4), more than a half of the respondents do not use the same password, which indicates that teachers are to some extent familiar with security measures for identity protection on the internet. Also, most respondents answered that they had never been a victim of cybercrime (S5).

When examining Q1, the results show that, on average, secondary school teachers in the selected county use antivirus protection the most (85%). However, when it comes to other habits and experiences, only one third or less of respondents use a firewall or anti-spyware program. Almost half of respondents use the same password for different applications. As more than one third (from 37.5% to 44.5%) answered "I don't know" on the statements related to the use of anti-spyware programs and firewalls, it is possible that the respondents are not familiar with these computer protection tools, while almost 10% of respondents stated that they were not familiar with the concept of cybercrime, and 5.5% with antivirus protection. These findings also reasonably highlight the need for education on the basics of computer security.

TABLE IV. RESULTS ON THE RESPONDENTS' KNOWLEDGE AND TECHNIQUES (RESPONSES ON A 1-5 LIKERT SCALE)

| Statement | AM | U | L | S |
|---|---|---|---|---|
| AM=arithmetic mean, U=95% CI Mean Upper, L=95% CI Mean Lower, S=standard deviation | | | | |
| *S1: I am familiar with the concept of information security and methods of protection.* | 3.611 | 3.853 | 3.369 | 1.029 |
| *S2: I write on paper the passwords that I can't easily remember and leave it near the computer.* | 1.611 | 1.865 | 1.357 | 1.082 |
| *S3: When I set/update a password, I always pay attention to its length and the combination of letters, numbers and characters.* | 4.083 | 4.367 | 3.8 | 1.207 |
| *S4: I delete suspicious e-mails without opening them.* | 4.528 | 4.758 | 4.298 | 0.978 |
| *S5: I never open links and attachments from unknown e-mail senders.* | 4.486 | 4.716 | 4.256 | 0.979 |
| *S6: I always carefully look at the web address before opening a website that interests me.* | 3.611 | 3.913 | 3.309 | 1.284 |
| *S7: I regularly update my antivirus program.* | 3.417 | 3.739 | 3.094 | 1.371 |
| *S8: An antivirus program is installed on all the electronic devices I use.* | 3.458 | 3.774 | 3.143 | 1.342 |
| *S9: I am ready to pay for an antivirus program that would fully protect my computer.* | 3.264 | 3.567 | 2.961 | 1.289 |
| *S10: I know what a firewall is and how to configure it.* | 2.417 | 2.724 | 2.109 | 1.308 |
| *S11: I know what cookies are and how they work.* | 3.556 | 3.853 | 3.258 | 1.266 |
| *S12: I always save my password within the web browser.* | 2.528 | 2.874 | 2.182 | 1.472 |
| *S13: I often use programs for safekeeping of passwords (e.g. RoboForm, Keeper).* | 1.875 | 2.185 | 1.565 | 1.321 |

Table IV presents results on the analysis of statements related to respondents' specific computer protection knowledge and techniques (confidence interval of 95%). Highest average scores were achieved for S4 (4.53), S5 (4.49) and S3 (4.08) related to deletion of suspicious mails, opening links and attachments from unknown senders and setting up passwords, respectively. The lowest score was achieved for S13 (1.88), which is related to the use of programs for safekeeping passwords. Statements S2 (1.61) and S12 (2.53) are reverse scored, where a lower score indicates better results (i.e. rarely writing passwords on paper and leaving it next to the computer, and saving passwords within the web browser). Statement S10 shows below average scores with 2.42 regarding the use of firewalls. Other statements scored average values ranging from 3.46 to 3.61.

The results point to the weak points of computer protection – they refer to firewall protection, followed by the use of programs for safekeeping of passwords.

The largest standard deviations were recorded for statements S7-S13, which are related to antivirus protection, use of firewalls, cookies, saving and protecting passwords. The smallest standard deviation was recorded for statements related to deleting suspicious messages and opening suspicious attachments.

When examining Q2, the results show that secondary school teachers regularly delete suspicious emails, take care when opening links and attachments from unknown senders, and when setting passwords. However, the lowest protection measures are taken to save passwords, followed by the use of firewalls and antivirus protection.

As for the fifth part of the questionnaire, when asked what they base their passwords on, a total of 26 (36.1%) respondents stated that their password is based on random words, numbers and characters that together have no meaningful meaning. 21 of them (29.2%) claim that it is based on their personal data. 27.8% claim that their password is based on information about the previous one. 3 of them admit that it is based on phrases, and 1 teacher claims that it is based on words from the dictionary.

When asked about their interest in participating in information security education and training, the results are as follows. A total of 47 (65.2%) teachers wants a workshop on information security to be held. 12 (16.67%) of them think that they do not need a workshop to improve their knowledge, whereas the remaining 13 respondents chose not to answer this question at all. Based on the obtained results, it can be concluded that the respondents have an interest in attending information security education and training.

## V. LIMITATIONS AND RECOMMENDATIONS

As this research was conducted in the area of only one county, it would certainly be useful to repeat the research at the national level with a larger sample of schools and respondents, in order to gain deeper insights.

Based on the conducted research, the authors advise regular holding of educational workshops and courses on relevant topics in the field of information security. The workshops would be intended for teachers of all levels of education. Attending workshops requires constant measurement of the progress of the participants, which would determine the current level of knowledge on the defined topic. Collected data could also help improve the quality of workshop content.

## VI. Conclusion

The aim of this research was to investigate the level of awareness of information security among secondary school teachers in one Croatian county – Karlovac County. The research was conducted among 72 secondary school teachers, with the help of an online questionnaire. However, the results of this research should only be taken as preliminary, due to the small number of respondents and the need for a more detailed statistical analysis.

The findings of the analysis of Q1 (habits and experiences) indicate that, on average, 85% of secondary school teachers use antivirus software. Fewer than one-third make use of an anti-spyware or firewall. Nearly 50% of those surveyed say they use the same password across several apps. When asked whether they use a firewall or an anti-spyware program, more than one-third of the respondents said, "I don't know", which may mean that they are not familiar with these computer security technologies. Five percent of respondents said they were unfamiliar with antivirus software, and nearly ten percent said they were unfamiliar with the idea of cybercrime.

Results on Q2 (knowledge and techniques) show that secondary school teachers take care on deletion of suspicious mails, opening links and attachments from unknown senders and setting up passwords. However, knowledge and techniques are of low level for safekeeping passwords and firewall protection.

Finally, it can be concluded that secondary school teachers, given their existing knowledge, are not sufficiently familiar with computer protection and the use of protective methods and security tools. Teachers are less familiar with the use of firewalls and password managers. Knowledge on the use of antivirus programs or access to various forms of suspicious e-mail messages is an important advantage. Nevertheless, the respondents state that with regular training they can raise the level of knowledge and thus contribute to the stability of information security in education.

The results of this research are mostly in line with previous research that shows the need for education on information security knowledge and skills, and thus for raising awareness of computer protection measures. For future work, the authors plan to conduct research on a larger sample of respondents and expand it to all counties in Croatia.

## References


[1] F. Hess, "The Top Target For Ransomware? It's Now K-12 Schools", Accessed: 31.12.2023 [Online]. Available: https://www.forbes.com/sites/frederickhess/2023/09/20/the-top-target-for-ransomware-its-now-k-12-schools/

[2] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele, "Measuring cyber secure behavior of elementary and high school students in the Netherlands", *Computers & Education*, vol. 186, 104536, 2022.

[3] G. A. Odiaga, S. Abeka, and S. Liyala, "An Information Security Awareness Framework For Secondary School Teachers In Kenya", *International Journal Of Innovative Research and Advanced Studies (IJIRAS)*, vol. 7, no. 5, pp. 88-98, 2020.

[4] A. Conry Murray, and V. Weafer, *The Symantec Guide to Home Internet Security*, Boston, USA: Addison-Wesley Educational Publishers Inc.; 1st edition, 2005.

[5] P. Bhargava, R. Choudhary, and A. Gupta, "A Review Study on Computer Virus", *World Journal of Research and Review (WJRR)*, vol. 14, no. 5, pp. 39-44, 2022.

[6] I. Saeed, A. Selamats, and A. Abuagoub, "A Survey on Malware and Malware Detection Systems", *International Journal of Computer Applications* , vol. 67, no. 16, pp. 25-31. 2013.

[7] P. Dusane, and Y. Pavithra, "Logic Bomb: An Insider Attack", *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 3662-3665, 2020.

[8] M. Agrawal, H. Singh, N. Gour, and M. Kumar, "Evaluation on Malware Analysis", *International Journal of Computer Science & Information Technologies*, vol. 5, no. 3, pp. 3381-3383, 2014.

[9] S. Aurangzeb, M. Aleem, M. A. Iqbal, and M. A. Islam, "Ransomware: A Survey and Trends", *Journal of Information Assurance & Security*, vol. 12, pp. 48-58, 2017.

[10] J. Gao, L. Li, P. Kong, T. F. Bissyandé, and J. Klein, "Should You Consider Adware as Malware in Your Study?", *Proceedings of the IEEE 26th International Conference on Software Analysis Evolution and Reengineering (SANER)*, pp. 604-608, 2019.

[11] I. Dunđer, S. Seljan, and M. Odak, "Data Acquisition and Corpus Creation for Phishing Detection", *Proceedings of the 46th International ICT and Electronics Convention (MIPRO)*, pp. 533-538, 2023.

[12] A. Kovač, I. Dunđer, and S. Seljan, "An overview of machine learning algorithms for detecting phishing attacks on electronic messaging services", *Proceedings of the 45th Jubilee International ICT and Electronics Convention (MIPRO)*, pp. 954-961, 2022.

[13] S. Seljan, N. Tolj, and I. Dunđer, "Information Extraction from Security-Related Datasets", *Proceedings of the 46th International ICT and Electronics Convention (MIPRO)*, pp. 539-544, 2023.

[14] S. A. Aminu, Z. Sufyanu, T. Sani, and A. Idris, "Evaluating the effectiveness of antivirus evasion tools against Windows platform", *FUDMA Journal of Sciences (FJS)*, vol. 4, no. 1, pp. 89-92, 2020.

[15] *CERT.hr, Godišnji izvještaj, CARNET, 2022*. Accessed: 31.12.2023 [Online]. Available: https://www.cert.hr/wp-content/uploads/2023/02/CERT-G.I.-2022..pdf

[16] M. Rivero, "The 2023 State of Ransomware in Education", Malwarebytes LABS. Accessed: 31.12.2023 [Online]. Available: https://www.malwarebytes.com/blog/threat-intelligence/2023/06/the-2023-state-of-ransomware-in-education-84-increase-in-known-attacks-over-6-month-period

[17] I. Corradini, and E. Nardelli, "Developing Digital Awareness at School: A Fundamental Step for Cybersecurity Education", in *Advances in Human Factors in Cybersecurity, AHFE 2020. Advances in Intelligent Systems and Computing*, vol. 1219, I. Corradini, E. Nardelli, T. Ahram, Eds. Springer, Cham, 2020, pp 102-110.

[18] K. V. Sridevi, "Cyber security Awareness among In-service secondary school teachers of Karnataka", *Indian Journal of Educational Technology*, vol. 2, no. 2, pp. 82-94, 2020.

[19] W.-Y. Chiu, and H.-F. Ho, "Time to Educate the Educators: An Evaluation of Cyber Security Knowledge Awareness and Implementation for School Teachers in Taiwan", *Proceedings of the International Conference on Technology and Social Science 2019 (ICTSS 2019)*, p. 4, 2019.

[20] C. Beaman, A. Barkworth, T. Akande, S. Hakak, and M. Khan, "Ransomware: Recent advances analysis, challenges and future research directions", *Computers & Security*, vol. 111, issue C, 2021.