



# THE CONNECTION BETWEEN DAILY/GENERAL STRESS EXPERIENCE AND RISKY INTERNET BEHAVIOR AMONG STUDENTS OF HEALTH AND NON-HEALTH STUDIES

Dubravka Matijašić-Bodalec<sup>1,2,3</sup>, Antun Bajan<sup>1,2,4</sup>, Krešimir Šolić<sup>1</sup>, Petra Mamić<sup>5</sup>, Tena Velki<sup>6</sup>, Nikola Bajan<sup>4</sup>, Andrea Milostić-Srb<sup>2</sup>, Nika Srb<sup>1</sup>, Igor Fosić<sup>7</sup>, Snježana Čukljek<sup>8</sup> and Slavica Đorđević<sup>9,10</sup>

<sup>1</sup>Osijek Faculty of Medicine, Josip Juraj Strossmayer University in Osijek, Osijek, Croatia;

<sup>2</sup>Faculty of Dental Medicine and Health, Josip Juraj Strossmayer University in Osijek, Osijek, Croatia;

<sup>3</sup>Mlinarska School of Nursing, Zagreb, Croatia;

<sup>4</sup>Institute of Emergency Medicine of Osijek-Baranja County, Osijek, Croatia;

<sup>5</sup>Division of Anti-Doping, Croatian Institute of Public Health, Zagreb, Croatia;

<sup>6</sup>Faculty of Education, Josip Juraj Strossmayer University in Osijek, Osijek, Croatia;

<sup>7</sup>HEP – Telecommunications, Osijek, Croatia;

<sup>8</sup>Department of Nursing, University of Applied Health Sciences, Zagreb, Croatia;

<sup>9</sup>Faculty of Medical Sciences, University of Kragujevac, Kragujevac, Serbia;

<sup>10</sup>Belgrade Academy of Applied Studies, Department of School of Applied Health Science, Belgrade, Serbia

**SUMMARY** – At the time of intensive development of information technologies and their penetration into every pore of human functioning, it is extremely important to understand the ways of safe Internet browsing. Data theft is most often aimed at the human factor through so-called ‘phishing’ attacks, mainly *via* e-mail. The aim of this research was to examine the potential correlation between stress and risky behavior on the Internet and indirectly with the level of knowledge about information security among students of different fields of study. For this purpose, we conducted research among students of health studies, rehabilitation studies, and students of pedagogical and psychological studies at the Josip Juraj Strossmayer University of Osijek. The research instrument consisted of two questionnaires and personal characteristics of the respondents. Perceived stress correlated slightly negatively with age, and a slight positive correlation was obtained with the assessment of the importance of safe use, and a slightly higher one with the level of awareness of online risks. In the case of self-assessment of risky behavior, students of health studies showed better results, whereas in risky behavior with simulation, no significant difference was obtained. Students of health studies with previously completed online safety education courses had a higher level of awareness of the importance of online protection and were also better in

---

Correspondence to: *Assist. Prof. Andrea Milostić-Srb, MD, PhD*, Faculty of Dental Medicine and Health, Josip Juraj Strossmayer University in Osijek, Crkvena 21, HR-31000 Osijek, Croatia  
E-mail: amsrb@fdmz.hr

Received May 31, 2023, accepted June 30, 2023

terms of awareness of online risks. No difference was found regarding the riskiness of online behavior. In conclusion, we did not find connection between stress and risky behavior, or between risky behavior and the level of knowledge about online risks. Despite all that, specific education about online security is necessary because it raises the level of awareness, and with its continuous implementation, we can expect better results of online security.

Keywords: *Cyber security; Students; Health studies; Risky online behavior; Stress*

## Introduction

Information technology has become an integral part of the lives of the vast majority of the world population. It includes smartphones, tablets and laptops in addition to personal desktop computers<sup>1,2</sup>.

Cyber security refers to technologies, but also to the people who use them. Many studies have identified users as the main causes of cybernetic attacks. This is one of the reasons why people are considered the weakest link in cybersecurity<sup>3-6</sup>. Cyber-attacks typically steal money, intellectual property or data, but increasingly they are seen to actually be aimed at causing panic or for political purposes<sup>7</sup>. Social engineering is the name for exploiting human weaknesses to achieve a malicious goal<sup>8,9</sup>. Most often, e-mail is used by the so-called 'phishing' method, where they try to get usernames, passwords, personal data, etc. from users<sup>1,10,11</sup>.

In order to improve cyber security, cyber hygiene is often mentioned<sup>4,12</sup>. The European Network and Information Security Agency explained that cyber hygiene should be viewed in the same way as personal hygiene, and once it is properly integrated into organization, it will be part of daily routine, and just as health control requires responsible behavior and periodic check-ups, so does online health<sup>12</sup>. This actually explains that the average user of information technology does not necessarily need to understand the mechanisms of why something is done because they can be too complex and complicated. Just as, for example, an individual does not necessarily need to understand transmission of a disease through droplets in order to know how to put their hand in front of their mouth when they cough. Although it is common knowledge, and research results show that the privacy of Internet users' personal data is important,

most users rarely try actively to protect it. They even give them voluntarily, in exchange for what we would say is a less important return, often just to attract attention of colleagues in an online social network. This phenomenon is commonly called the 'privacy paradox'<sup>13-15</sup>. Awareness of cyber security is extremely important. It is achieved, among other things, by motivating people to use security measures to lessen cyber threats<sup>3</sup>. Cyber security awareness is achieved in various ways, but one of the most important is education, which should primarily relate to safe handling of information, incident reporting, software updates, behavior on social networks, and secure passwords<sup>1,4,8,10,11</sup>. One of the problems we encounter is education that is unique for everyone. This proved to be less effective than, for example, specific education aimed at certain groups of users<sup>2,16</sup>. Recently, malicious attacks on health and educational institutions have become more frequent. Attacks increased during the period of the COVID-19 pandemic, which is not surprising since these two sectors were most exposed during the pandemic. Health systems have opened up and functioned largely online, and security policies have not been able to keep up<sup>6</sup>. On the other hand, these systems have very sensitive data that have a high price on the information market<sup>1</sup>. Healthcare systems have important data on the health status of patients, which can be extremely compromising for an individual if the information becomes available to someone outside the healthcare system. On the other hand, educational institutions have a lot of information related to personal data of students and employees, their financial data, data on all types of academic research, student evaluations, and similar data. However, the academic environment, unlike others, is not based on secrecy, but quite the opposite. The academic environment is based on openness, tradition of trust, exchange

of information and discussions. These activities take place in a public environment. However, as much as data security could be ensured, it is primarily exposed to constant change that characterizes the academic environment. Educational institutions annually enroll new students, hire temporary staff, guest lecturers and researchers<sup>17</sup>. This constant turnover of people makes it even more difficult to take care of cyber security<sup>18</sup>.

Numerous student surveys show mixed results regarding cyber security. Some of them show that students in higher years of study show worse results, even though they have more knowledge about cyber security, whereas some other studies have completely opposite results<sup>17</sup>. Furthermore, some studies show that a large number of students think that antivirus protection is sufficient, that they do not consider messages and e-mail received from friends to be dangerous, and that they rarely change their passwords. The passwords are most often very simple (like names or dates of birth) because more complicated ones are harder to remember<sup>11,16</sup>. The work environment, but also the private one, is full of stressful situations that affect people in different ways. Some studies examined the effect of resilience and stress at work on the three components that make up awareness of information security, namely knowledge, attitude and behavior. A large study in Australia came to the result that participants with greater resilience had a higher awareness of information security and declared in favor of lower levels of stress at work<sup>19</sup>.

Despite the fact that there is a lot of research on cyber security, the existing literature shows that there is a lack of research within higher systems of education<sup>17,20</sup>.

This research was conducted on the population of students of several different study programs in the Republic of Croatia with the purpose of gaining insight into their behavior regarding cyber security. The aim of this research was to examine the potential correlation between stress and risky behavior on the Internet and indirectly with the level of knowledge about information security among students of three different types of studies, i.e., health studies, health associate studies, and teacher studies.

## Methods

### *Examinees*

The respondents were students of lower years of health studies (medicine, nursing, physiotherapy, dental medicine, and laboratory diagnostics), rehabilitation studies (health collaborative orientation), and students of pedagogical and psychological studies (three groups of teachers) at the Josip Juraj Strossmayer University of Osijek.

### *Instruments*

For research purposes, both questionnaires, along with demographic questions and questions on prior knowledge, were programmed into an online version. The research was conducted at the end of 2022, and the students filled out the questionnaires online in the university premises, immediately before or after the lecture where the lecturer asked them to participate in the research.

The Behavioral-Cognitive Internet Security Questionnaire (BCISQ)<sup>21</sup> is an instrument for measuring Internet security, that is, the risky behavior of computer users and their level of awareness of potential online risks. The questionnaire was developed and validated primarily in English<sup>22</sup>, and the Croatian version was developed in 2020<sup>23</sup>. It consists of 4 subscales, 2 behavioral and 2 cognitive. Behavioral scales measure the level of risky behavior of computer users, and cognitive scales measure the level of awareness regarding information security.

The Perceived Stress Scale<sup>24,25</sup> measures the degree of the examinee stress through assessments of the lack of control, feeling overwhelmed and unpredictability of life, during the last few months. The scale contains 10 items, and respondents give their answers on a 5-point Likert scale.

Demographic questions collected personal data (age, gender, type of college, personal assessment of information security and privacy) and previous participation in education about security and privacy on the Internet.

### *Statistical analysis*

Standard statistical methods were used on data analysis. For categorical data analysis, we used  $\chi^2$ -test, while for numerical data correlations we used

nonparametric Spearman's rank test and Kendall's Tau test. Differences between two independent groups were tested with nonparametric Mann-Whitney test, whereas differences among more than two groups were tested with either parametric one-way ANOVA (with Scheffe post-hoc test) or nonparametric Kruskal-Wallis test (with Conover post-hoc test).

The level of significance was set at 0.05, while all p values were two-tailed. Statistical analysis was done with MedCalc statistical tool (version 20.218, MedCalc Software Ltd).

## Results

In this research, 255 students of lower years of college at the Josip Juraj Strossmayer University in Osijek, mean age  $19.8 \pm 2.8$  years, were included. There were significantly more female students, and half of the respondents were from health studies. Less than half of the respondents had received some kind of education related to Internet security, and most of them considered themselves to have good or excellent knowledge about Internet security (Table 1).

The general level of stress measured by the Perceived Stress Scale was  $3.23 \pm 0.47$  (mean  $\pm$  standard deviation) with a total range of one to five, where five is the maximum level of stress.

Perceived stress was slightly negatively correlated with age ( $\rho = -0.121$ ). A slight positive correlation of perceived stress was obtained with assessment of the importance of safe use ( $\rho = 0.134$ ;  $p = 0.033$ ) and a slightly higher one with the level of awareness of online risks ( $\rho = 0.255$ ;  $p < 0.001$ ). The obtained results coincided when only students of health studies were selected for analysis. No correlation was found between the respondent age and Internet security subscales (Table 2).

The students of health studies were slightly older ( $p = 0.007$ ) with an average difference of less than two years. Observing the subscale of self-assessment of risky behavior, students of health studies showed better results (Kruskal-Wallis test,  $p = 0.068$ ). In the subscale of cognitive awareness of the importance of safe use, students of rehabilitation studies showed worse results. In the subscale of awareness of the existence of online risks, students of teacher studies had significantly better results (Kruskal-Wallis test, 0.008). There was no significant difference in the subscale of risky behavior with simulation. All three groups of students behaved equally risky, regardless of self-assessment (Table 3).

When students of health studies were observed separately, the vast majority of them marked their self-assessment of online safety as "good", but the results regarding safe use were worse than of students

Table 1. Demographic characteristics of students

Characteristic	Category	n (%)	p*
Gender of examinees	Male	49 (19.2)	<0.001
	Female	206 (80.8)	
Type of college	Health students	129 (50.6)	<0.001
	Associates	30 (11.8)	
	Teachers	96 (37.6)	
Knowledge self-assessment regarding online security and privacy	Poor	39 (15.3)	<0.001
	Good	191 (74.9)	
	Excellent	25 (9.8)	
Education regarding online security	Yes	105 (41.2)	0.046
	No	150 (58.8)	
Total		255 (100.0)	

\* $\chi^2$ -test

Table 2. Correlations between stress level and each subscale regarding Internet security

Each variable pair		Rho/tau	95% CI	p	
Correlation between PSS and BCISQ_or age	Perceived stress level	Age	-0.121	-0.240 to 0.002	0.054*
		Risky behavior with simulation	0.007	-0.085 to 0.098	0.087†
		Risky behavior self-assessment	0.001	-0.122 to 0.124	0.987*
		Importance of safe usage	0.134	0.011 to 0.253	<b>0.033*</b>
		Awareness of online risk	0.255	0.137 to 0.367	<b>&lt;0.001*</b>
Additional correlations with age	Age	Risky behavior with simulation	0.063	-0.053 to 0.178	0.133†
		Risky behavior self-assessment	-0.017	-0.140 to 0.106	0.787*
		Importance of safe usage	0.094	-0.029 to 0.214	0.135*
		Awareness of online risk	-0.040	-0.162 to 0.083	0.527*
Correlation between BCISQ subscales	Risky behavior with simulation	Risky behavior self-assessment	0.081	-0.025 to 0.206	0.054†
		Importance of safe usage	-0.016	-0.114 to 0.091	0.706†
		Awareness of online risk	-0.028	-0.130 to 0.068	0.503†
	Risky behavior self-assessment	Importance of safe usage	-0.095	-0.215 to 0.029	0.132*
		Awareness of online risk	-0.002	-0.125 to 0.121	0.977*
	Importance of safe usage	Awareness of online risk	0.145	0.023 to 0.264	<b>0.020*</b>
Correlation between PSS and BCISQ only with health care studies students (n=129)	Perceived stress level	Risky behavior with simulation	0.004	-0.128 to 0.166	0.950†
		Risky behavior self-assessment	-0.007	-0.180 to 0.166	0.934*
		Importance of safe usage	0.134	-0.040 to 0.300	<b>0.130*</b>
		Awareness of online risk	0.221	0.050 to 0.380	<b>0.012*</b>

CI = confidence interval; PSS = Perceived Stress Scale; BCISQ = Behavioral-Cognitive Internet Security Questionnaire; \*Spearman's rank correlation test; †Kendall's Tau correlation test

Table 3. Differences among students according to their study or previous knowledge

Examined variable	Health studies /n=129	Associates /n=30	Teachers /n=96	P
<b>According to type of college</b>				
Age / mean (SD)	20.6 (3.4)	18.4 (1.0)	19.2 (1.7)	<b>0.007*</b>
Perceived stress level / median (q1-q3)	3.2 (2.9-3.5)	3.2 (2.9-3.3)	3.3 (3.0-3.6)	0.145†
Risky behavior with simulation / median (q1-q3)	0.0 (0.0-2.0)	0.0 (0.0-2.0)	1.0 (0.0-2.0)	0.233†
Risky behavior self-assessment / median (q1-q3)	1.0 (1.0-1.3)	1.3 (1.0-1.3)	1.3 (1.0-1.5)	0.068†
Importance of safe usage / median (q1-q3)	4.0 (3.5-4.3)	3.8 (3.0-4.0)	4.0 (3.8-4.5)	<b>0.025†</b>
Awareness of online risk / median (q1-q3)	4.0 (2.6-4.8)	3.8 (2.0-4.2)	4.6 (3.5-4.8)	<b>0.008†</b>

Table 3. [Continued]

Examined variable	Health studies /n=129	Associates /n=30	Teachers /n=96	P
<b>According to knowledge self-assessment regarding online security and privacy-only health students (n=129)</b>				
Examined variable	Poor /n=19	Good /n=98	Excellent /n=12	P
Age/median (q1-q3)	20.0 (19.0-20.0)	20.0 (19.0-20.0)	19.5 (19.0-20.0)	0.548†
Perceived stress level / median (q1-q3)	3.4 (3.0-3.6)	3.2 (2.9-3.5)	3.2 (3.0-3.3)	0.245†
Risky behavior with simulation / median (q1-q3)	1.0 (0.0-2.0)	0.0 (0.0-1.0)	0.0 (0.0-1.0)	0.132†
Risky behavior self-assessment / median (q1-q3) /	1.0 (1.0-1.7)	1.0 (1.0-1.3)	1.0 (1.0-1.3)	0.642†
Importance of safe usage / median (q1-q3) /	4.0 (3.3-4.2)	4.0 (3.5-4.3)	4.3 (4.3-4.9)	<b>&lt;0.001†</b>
Awareness of online risk / median (q1-q3)	4.4 (2.5-4.9)	4.0 (2.6-4.8)	4.6 (3.0-4.9)	0.468†

\*One-way ANOVA (with Scheffe post-hoc test); †Kruskal-Wallis test (with Conover post-hoc test)

Table 4. Differences between students according to gender or training on security

<b>Differences according to gender – health studies students only (n=129)</b>			
Examined variable	Male /n=29	Female /n=100	P*
Age/median (q1-q3)	20.0 (19.0-20.0)	20.0 (19.0-20.0)	0.476
Perceived stress level / median (q1-q3)	3.0 (2.7-3.5)	3.2 (3.0-3.6)	<b>0.003</b>
Risky behavior with simulation / median (q1-q3)	0.0 (0.0-1.0)	0.0 (0.0-2.0)	0.150
Risky behavior self-assessment / median (q1-q3)	1.0 (1.0-1.3)	1.0 (1.0-1.3)	0.514
Importance of safe usage / median (q1-q3)	4.0 (3.4-4.3)	4.0 (3.5-4.4)	0.428
Awareness of online risk / median (q1-q3)	3.0 (2.6-4.4)	4.2 (3.0-4.8)	0.064
<b>Differences according to some kind of previous training on cybersecurity – health studies students only (n=129)</b>			
Examined variable	No training /n=80	With training /n=49	P*
Age/median (q1-q3)	20.0 (19.0-20.0)	20.0 (19.0-20.0)	0.168
Perceived Stress level / median (q1-q3)	3.2 (2.9-3.4)	3.2 (3.0-3.6)	0.203
Risky behavior with simulation / median (q1-q3)	0.0 (0.0-2.0)	0.0 (0.0-1.0)	0.140
Risky behavior self-assessment / median (q1-q3)	1.0 (1.0-1.3)	1.0 (1.0-1.3)	0.919
Importance of safe usage / median (q1-q3)	3.9 (3.3-4.3)	4.3 (4.0-4.5)	<b>&lt;0.001</b>
Awareness of online risk / median (q1-q3)	3.8 (2.6-4.6)	4.6 (3.0-4.8)	0.065

\*Mann-Whitney test

who self-assessed online safety as “excellent” ( $p < 0.001$ ) (Table 3).

Additional analysis showed that female respondents experienced significantly more stress (Mann-Whitney test,  $p = 0.003$ ) and were somewhat better (Mann-Whitney test,  $p = 0.064$ ) in terms of awareness of online risks.

Students of health studies with previously completed education on online security had a significantly higher level of awareness of the importance of online protection (Mann-Whitney test,  $p < 0.001$ ) and were somewhat better in terms of awareness of online risks (close to the significance limit, Mann-Whitney test,  $p = 0.065$ ). However, no difference was found regarding riskiness of online behavior (Table 4).

## Discussion

More women participated in the research than men, which can be explained by the fact that the study included study programs that normally enroll women more often. On the other hand, a greater representation of students in health studies is expected because within these studies, there are more different study directions and thus a larger number of students. It is interesting to note that a minority of the respondents completed some kind of education related to Internet security, but this should be taken with caution because subjects related to IT are an integral part of high school education curricula, so a certain level of familiarity with information security is expected from them, regardless of the fact that they have not listened specific courses. This speaks in favor of the result that most respondents rated their knowledge of Internet security as good or even excellent.

The age of the examinees could not be related to the Internet security subscales, which contradicts the results of the studies by An *et al.*<sup>18</sup> and Hong *et al.*<sup>20</sup>, who found the older group of students to have significantly less awareness than the younger ones, while Huang *et al.*<sup>26</sup> found in their research that upperclassmen were most sensitive to security incidents. This contradiction in the results supports the fact that adolescents, regardless of age, behave equally risky in the online environment, that is, different studies give different results that lead to this conclusion.

The mean general level of stress was  $3.23 \pm 0.47$ , and slightly negatively correlated with age, which mostly coincides with the results of previous research on student population, which show that stress levels range from moderate to high<sup>27-29</sup>.

Perceived stress correlated slightly positively with assessment of the importance of safe use and slightly more with the level of awareness of online risks, and the results did not differ from those of health students. These results are contrary to previous research conducted in Croatia, in which no connection was found among stress, awareness of information security and risky behavior on the Internet<sup>30</sup>. We can state that a certain level of stress can contribute to positive behavior in general<sup>31</sup>, and in this research, it had a positive effect on the level of information security awareness among the examinees.

Students of health studies were slightly older than other examinees, which could be related to the duration of their secondary education. Namely, more than half of the respondents were from health studies, and part of them were nursing studies enrolled by students who had previously completed high school for nurses, which in Croatia lasts one year longer (5 years) than other high school programs (4 years). However, since the average age difference was less than two years, we did not consider it significant. Regarding riskiness of behavior, there was no difference among students based on their fields of study, which speaks in favor of the fact that all students, regardless of the type of study, behaved equally risky.

Teacher study students showed better results regarding the importance or level of awareness of online risks, although there was no significant difference in absolute results. Previous studies have found positive association between awareness of information security and risky behavior on the Internet in adolescents<sup>32</sup>.

Students of health studies showed better results in terms of self-assessment of risky behavior on the Internet, which is a desirable result because after completing their studies, they are employed in health institutions where they have a lot of private data of patients to care for. Many studies support the fact that people are the weakest link<sup>3-6,9</sup> in Internet security, and by hiring young staff, better awareness of Internet security is expected, which should result in safer behavior. These results pave the way for additional research in order

to determine the accuracy of the data obtained and possibly influence the possible changes in educational curricula in the direction of online security education.

In the subscales of cognitive awareness of the importance of safe use and existence of online risks, students of teacher studies showed significantly better results (Kruskal-Wallis test 0.008), while there was no significant difference in the subscales of risky behavior with simulation. All three groups of students behaved equally risky, regardless of self-assessment.

Female examinees experienced significantly more stress<sup>27,33</sup> and had slightly better results in terms of awareness of online risks<sup>34</sup>, which coincides with the results of An *et al.* who report that women had higher scores on information knowledge, attitudes, and behavior than men<sup>17</sup>.

A significantly higher level of awareness of the importance of online protection, as well as awareness of online risks was found among health students who had previously completed some kind of online safety education, but there was no difference regarding riskiness of online behavior. These results are very significant because we found disconnection and contradiction in the results. It would be expected that a higher level of knowledge results in better and safer behavior, which turned out to be incorrect. The results obtained coincide with previous researches which confirm that the safety of online behavior is not higher among people who have a higher level of knowledge about online risks, but quite the opposite<sup>13,14,16,35</sup>. Despite this, education is very important because it increases awareness of online risks<sup>3,5,6,8-10,36-38</sup>. Some authors are inclined to think that universal equivalent education is not most effective and that a personalized approach should be developed<sup>2,16</sup>.

## Conclusion

Through this research, we obtained a slight association of perceived stress with assessment of importance and awareness regarding online security, but not with risky behavior. The results obtained apply equally to all three groups of respondents.

In general, we did not find a connection between stress and risky behavior, or between risky behavior and the level of knowledge about online risks, which

leads us to a conclusion that people know one thing, but do the other.

Although the level of knowledge is not related to safer behavior on the Internet, we can still say that specific education is necessary and that with its permanent implementation, we can expect better results of online security.

## References

1. Nifakos S, Chandramouli K, Nikolaou CK, *et al.* Influence of human factors on cyber security within healthcare organisations: a systematic review. *Sensors*. 2021;21(15):5119. doi: 10.3390/s21155119
2. Fujs D, Vrhovec S, Vavpotič D. Towards personalized user training for secure use of information systems. *Int Arab J Inf Technol*. 2022;19(3). doi: 10.34028/iajit/19/3/3
3. Chaudhary S, Gkioulos V, Katsikas S. Developing metrics to assess the effectiveness of cybersecurity awareness program. *J Cybersecur*. 2022;8(1):tyac006. doi: 10.1093/cybsec/tyac006
4. Neigel AR, Claypoole VL, Waldfogle GE, Acharya S, Hancock GM. Holistic cyber hygiene education: accounting for the human factors. *Comput Secur*. 2020;92:101731. doi: 10.1016/j.cose.2020.101731
5. Sasse MA, Brostoff S, Weirich D. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technol J*. 2001;19(3):122-31. doi: 10.1023/A:1011902718709
6. He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *J Med Internet Res*. 2021;23(4):e21747. doi: 10.2196/21747
7. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we? *BMJ*. Published online July 6, 2017;j3179. doi: 10.1136/bmj.j3179
8. Aldawood H, Skinner G. Reviewing cyber security social engineering training and awareness programs – pitfalls and ongoing issues. *Future Internet*. 2019;11(3):73. doi: 10.3390/fi11030073
9. Aldawood H, Skinner G. Educating and raising awareness on cyber security social engineering: a literature review. In: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). IEEE; 2018:62-8. doi: 10.1109/TALE.2018.8615162
10. Priestman W, Anstis T, Sebire IG, Sridharan S, Sebire NJ. Phishing in healthcare organisations: threats, mitigation and

- approaches. *BMJ Health Care Inform.* 2019;26(1):e100031. doi: 10.1136/bmjhci-2019-100031
11. Cain AA, Edwards ME, Still JD. An exploratory study of cyber hygiene behaviors and knowledge. *J Inf Secur Appl.* 2018;42:36-45. doi: 10.1016/j.jisa.2018.08.002
  12. Vishwanath A, Neo LS, Goh P, *et al.* Cyber hygiene: the concept, its measure, and its initial tests. *Decis Support Syst.* 2020;128:113160. doi: 10.1016/j.dss.2019.113160
  13. Gerber N, Gerber P, Volkamer M. Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. *Comput Secur.* 2018;77:226-61. doi: 10.1016/j.cose.2018.04.002
  14. Snyman DP, Kruger H, Kearney WD. I shall, we shall, and all others will: paradoxical information security behaviour. *Inf Comput Secur.* 2018;26(3):290-305. doi: 10.1108/ICS-03-2018-0034
  15. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Comput Secur.* 2017;64:122-34. doi: 10.1016/j.cose.2015.07.002
  16. Chandarman R, Van Niekerk B. Students' cybersecurity awareness at a private tertiary educational institution. *Afr J Inf Commun AJIC.* 2017;(20). doi: 10.23962/10539/23572
  17. An Q, Hong WCH, Xu X, Zhang Y, Kolletar-Zhu K. How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. *Int J Inf Secur.* 2023;22(2):305-17. doi: 10.1007/s10207-022-00637-z
  18. Ulven JB, Wangen G. A systematic review of cybersecurity risks in higher education. *Future Internet.* 2021;13(2):39. doi: 10.3390/fi13020039
  19. McCormac A, Calic D, Parsons K, Butavicius M, Pattinson M, Lillie M. The effect of resilience and job stress on information security awareness. *Inf Comput Secur.* 2018;26(3):277-89. doi: 10.1108/ICS-03-2018-0032
  20. Hong WCH, Chi C, Liu J, Zhang Y, Lei VNL, Xu X. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Educ Inf Technol.* 2023;28(1):439-70. doi: 10.1007/s10639-022-11121-5
  21. Velki T, Šolić K. Development and validation of a new measurement instrument: the Behavioral-Cognitive Internet Security Questionnaire (BCISQ). *Int J Electr Comput Eng Syst.* 2019;10(1):19-24. doi: 10.32985/ijeces.10.1.3
  22. Etienne E. Exploring workplace bullying in nursing. *Workplace Health Saf.* 2014;62(1):6-11. doi: 10.1177/216507991406200102
  23. Velki T, Šolić K. Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS). *Polic Sigur.* 2020;29(4):341-55. <https://hrcak.srce.hr/249659> (in Croatian)
  24. Cohen S, Kamarck T, Mermelstein R. Perceived stress scale. Published online February 10, 2014. doi: 10.1037/t02889-000
  25. Hudek-Knežević J, Kardum I, Vukmirović Ž. The structure of coping styles: a comparative study of Croatian sample. *Eur J Personal.* 1999;13(2):149-61. doi: 10.1002/(SICI)1099-0984(199903/04)13:2<149::AID-PER326>3.0.CO;2-Z
  26. Huang X, He W, Hua C, Shang Y. The statistical analysis about status and influencing factors of university students' safety accidents. *Stat Appl.* 2014;03(02):57-67. doi: 10.12677/SA.2014.32009
  27. Labrague LJ, McEnroe-Petitte DM, Gloe D, Thomas L, Papatheanasiou IV, Tsaras K. A literature review on stress and coping strategies in nursing students. *J Ment Health.* 2017;26(5):471-80. doi: 10.1080/09638237.2016.1244721
  28. McKerrow I, Carney PA, Caretta-Weyer H, Furnari M, Miller Juve A. Trends in medical students' stress, physical, and emotional health throughout training. *Med Educ Online.* 2020;25(1):1709278. doi: 10.1080/10872981.2019.1709278
  29. Smolana A, Loster Z, Loster JE. Assessment of stress burden among dental students: a systematic literature review and meta-analysis of data. *Dent Med Probl.* 2022;59(2):301-7. doi: 10.17219/dmp/133955
  30. Velki T, Milić M. Stress as a mediator between risk and protective factors and online risky behaviors in adolescents. *Primenj Psihol.* 2021;14(2):149-71. doi: 10.19090/pp.2021.2.149-171
  31. Araújo AAC, Godoy S de, Maia NMF E S, *et al.* Positive and negative aspects of psychological stress in clinical education in nursing: a scoping review. *Nurse Educ Today.* 2023;126:105821. doi: 10.1016/j.nedt.2023.105821
  32. Brstilo I, Batinić L, Grgić S. Navike djece i mladih kod objavljivanja osobnih podataka na društvenim mrežama. *Sociološka Luča.* 2014;VIII(2):105-21. (in Croatian) <http://www.socioloskaluca.ac.me/Drugi%20broj%202014.htm>
  33. Kilic R, Nasello JA, Melchior V, Triffaux JM. Academic burnout among medical students: respective importance of risk and protective factors. *Public Health.* 2021;198:187-95. doi: 10.1016/j.puhe.2021.07.025
  34. Helsper EJ. Gendered Internet use across generations and life stages. *Commun Res.* 2010;37(3):352-74. doi: 10.1177/0093650209356439

35. Velki T, Romstein K. User risky behavior and security awareness through lifespan. *Int J Electr Comput Eng Syst.* 2019;9(2):53-63. doi: 10.32985/ijeces.9.2.2
36. Sawaya Y, Sharif M, Christin N, Kubota A, Nakarai A, Yamada A. Self-confidence trumps knowledge: a cross-cultural study of security behavior. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* ACM; 2017:2202-14. doi: 10.1145/3025453.3025926
37. Nazeer Khan SB, Richards D, Formosa P, Bankins S. To breach or not? Profiling students' likelihood of breaching university ICT Codes of Conduct: student profiling of breach of ICT Codes of Conduct. In: *2023 Australasian Computer Science Week.* ACM; 2023:50-7. doi: 10.1145/3579375.3579382
38. Šolić K, Nenadić K, Galić D. Empirical study on the correlation between user awareness and information security. *Int J Electr Comput Eng Syst.* 2012;3(2):47-51. <https://hrcak.srce.hr/133175>

### Sažetak

#### POVEZANOST SVAKODNEVNOG/OPĆEG DOŽIVLJAJA STRESA I RIZIČNOG PONAŠANJA NA INTERNETU MEĐU STUDENTIMA ZDRAVSTVENIH I NEZDRAVSTVENIH STUDIJA

*D. Matijašić-Bodalec, A. Bajan, K. Šolić, P. Mamić, T. Velki, N. Bajan, A. Milostić-Srb, N. Srb, I. Fosić, S. Čukljević i S. Đorđević*

U vrijeme intenzivnog razvoja informacijskih tehnologija i njihovog prodora u sve pore ljudskog funkcioniranja neobično je važno razumjeti načine sigurnog rada. Krađa podataka usmjerena je najčešće na ljudski faktor takozvanim "fišing" napadima uglavnom e-poštom. Ovo istraživanje imalo je za cilj ispitati potencijalnu korelaciju između stresa i rizičnog ponašanja na internetu te posredno s razinom znanja o informacijskoj sigurnosti između studenata različitih studijskih usmjerenja. U tu svrhu proveli smo istraživanje kod studenata zdravstvenih studija, studija rehabilitacije te studenata pedagoško-psiholoških studija Sveučilišta u Osijeku. Instrument istraživanja se sastojao od dva upitnika te osobnih obilježja ispitanika. Percipirani stres korelirao je blago negativno s dobi, a blaga pozitivna korelacija dobivena je s procjenom važnosti sigurne uporabe te nešto veća s razinom svjesnosti o *online* rizicima. Ispitanice značajno više doživljavaju stres te su nešto bolje u pogledu svjesnosti o *online* rizicima. Kod samoprocjene rizičnog ponašanja bolje rezultate pokazuju studenti zdravstvenih studija, a kod rizičnog ponašanja sa simulacijom nije dobivena značajna razlika. Studenti zdravstvenih studija s prethodno završenom izobrazbom o *online* sigurnosti imaju višu razinu svjesnosti o važnosti *online* zaštite te su bolji i u pogledu svjesnosti o *online* rizicima. Nije nađena razlika u pogledu rizičnosti *online* ponašanja. Zaključno, nismo pronašli povezanost stresa i rizičnog ponašanja, kao niti povezanost rizičnog ponašanja s razinom znanja o *online* rizicima. Unatoč tome specifična izobrazba o *online* sigurnosti je nužna, jer podiže razinu svjesnosti, a njezinim stalnim provođenjem mogu se očekivati bolji rezultati *online* sigurnosti.

**Ključne riječi:** *Kibernetička sigurnost; Studenti; Studenti zdravstvenih studija; Rizično online ponašanje; Stres*