Comparative Study on Online Security Awareness and Behavior Among Healthcare Professionals in Croatia

K. Solic *, T. Velki **, D. Matijasic Bodalec *, I. Fosic ***,
* J.J. Strossmayer University of Osijek, Faculty of Medicine, Osijek, Croatia
** J.J. Strossmayer University of Osijek, Faculty of Education, Osijek, Croatia
*** HEP Telekomunikacije, Osijek, Croatia
Kresimir.Solic@mefos.hr

***Abstract* — Healthcare professionals predominantly operate under additional stress, leading to the assumption that they exhibit riskier online behavior. Therefore, the aim was to assess their security awareness and online behavior, comparing them with the average internet user, administrative staff, and health studies students.**

This empirical study was conducted across four hospitals, two faculties, and within the general population. The Behavioral-Cognitive Internet Security Questionnaire was utilized, supplemented by demographic inquiries and questions regarding prior knowledge, including a deceptive question concerning the acceptance of terms and conditions.

Despite two-thirds of participants assessing their information security knowledge as good, less than one-third had received specific education on internet security. Relatively low average score for risky behavior and comparatively high average score for security awareness were observed, with no significant difference between healthcare professionals and the general population. Students exhibited slightly better results. However, only 7.25% of all participants responded correctly to the deceptive question.

The findings suggest that healthcare professionals, similar to the average user, behave rather safely when online. The absence of specific education did not show a negative correlation with online behavior or security awareness. Nevertheless, a notable number of participants granted consent to terms and conditions without reading them.

Keywords - information security; online security; online behavior; healthcare professionals; BCISQ

I. INTRODUCTION

Providing healthcare nowadays is highly dependent on integrated and complex information systems. However, the growing complexity of digital systems has also led to significant security challenges [1, 2]. The healthcare industry is among prime targets for malicious attacks as it lags behind other leading industries in safeguarding critical data [3].

The COVID-19 pandemic has posed an additional challenge to the existing threat to the information security of healthcare systems [4], as attacks on healthcare institutions increased during the pandemic [5, 6]. The pandemic has been an unprecedented challenge for global healthcare systems, leading to a neglect of information system security due to immense pressure on healthcare institutions. Consequently, the entire healthcare sector has become more vulnerable to cyberattacks. Numerous cyberattacks on hospitals, pharmaceutical companies, health ministries, the World Health Organization, and its partners have been recorded [5]. Since the outbreak of the COVID-19 pandemic, cyberattacks on healthcare institutions have intensified, adding an extra burden to an already overwhelmed healthcare industry [7]. This is primarily because the healthcare industry lags behind other leading industries in implementing security measures [8].

Research indicates that human behavior is responsible for the majority of cybersecurity incidents. *People* are considered the weakest link in the triad of cybersecurity: people, processes, and technology [9]. Human errors are associated with sudden changes in work practices, such as saving lives, and prolonged exposure to stress makes employees more susceptible to malicious frauds and mistakes [5]. For instance, a higher email workload is linked to an increased likelihood of responding to phishing emails [5]. Similarly, some researchers found that heavy workload reduces tolerance thresholds, leading to poorer adherence to security policies [5, 10]. Efforts regarding security methods should undoubtedly involve characterizing human factors that significantly contribute to the vulnerability and risk of cybersecurity [11]. The lack of education and awareness of cybersecurity has exposed healthcare in general to the risk of these events, with the majority of users having only a superficial understanding of cybersecurity beyond passwords, antivirus software, and virtual private networks [2, 12].

The most common motivation for attackers is money, constituting 91% of data breaches [13]. Each patient record is valued at an average of 50 dollars on the darknet and the entire set of medical records can be worth up to 1000 dollars [14]. Additionally, the collected data is worth much more, as it can be sold and exploited for further extortion from the institution from which it was stolen [15, 16].

Despite robust legal regulations, the healthcare industry significantly lags behind other industries in terms of cybersecurity [3]. Together with the lack of digital literacy among employees, it continues to be an easy and attractive

target for cyberattacks [17, 18]. Since the mental state of employees or their exposure to stress can play a mediating role in risky online behavior [19], and healthcare professionals predominantly operate under additional stress, the assumption was that they exhibit riskier online behavior compared to the average internet user.

Therefore, the aim of this empirical study was to assess the security awareness and the degree of risky online behavior among healthcare professionals and compare them with the average internet user, administrative staff in hospitals and students of health studies.

II. Study Design, Participants and Questionnaire Utilized

The research was structured as an empirical study and was conducted across four public state hospitals, two public faculties, and among the general population. Participants were divided into four research groups: healthcare professionals, administrative staff in hospitals, students of health studies as future healthcare professionals, and average online users from the general population as the control group in this study.

Students were informed by professors about the research and were asked to fill out a questionnaire. The questionnaire for healthcare employees was primarily distributed by hospital management, utilizing their own contacts, colleagues, and collaborators. The control group consisted of personal acquaintances (family, friends, etc.), regardless of age, gender, or prior knowledge.

The online approach to completing the questionnaire was anonymous and voluntary. Before filling out the questionnaire, each participant received an explanation about the study, its purpose, and goals. The online *Behavioral-Cognitive Internet Security Questionnaire (BCISQ)* was utilized, complemented by demographic questions and inquiries about prior knowledge, including additional deceptive questions concerning the acceptance of terms and conditions. The BCISQ, previously developed and validated, consists of four subscales measuring the riskiness of online behavior (both self-assessed and simulated real behavior) and cognitive information security awareness. A detailed description of this measurement instrument can be found in the authors' earlier papers [20 – 22].

Additional deceptive question concerning the acceptance of terms and conditions is named *Statement of consent for processing personal data* and has 318 words of text explaining what is The General Data Protection Regulation (GDPR) about, the importance of privacy protections and reasons to do this research. After approximately 80% of the *boring* text there was the instruction for examinees to mark both options, to both agree and not to agree to this tricky terms and conditions. Detailed description on English of this additional deceptive question can also be found in authors' earlier paper (23).

For data analysis, common statistical methods were employed, including the Kruskal Wallis test with post hoc Conover, Chi square test, and Spearman's rank correlation test. Results are presented in tables with median and interquartile range or correlation coefficient. All p values were two tailed, with the significance level defined as 0.05. The statistical software used included MedCalc (version 22.006, MedCalc Software Ltd, Ostend, Belgium; https://www.medcalc.org; 2023) and SPSS (version 23, IBM Corp. Released 2015. Armonk, NY: IBM Corp.).

III. Results

In total, 484 participants were included in this empirical research. The median age was 36, with an interquartile range from 22 till 48 years. The majority of participants were female (78.9%), and most had only high school education (59.7%). Approximately two-thirds of the participants (70.7%) assessed their information security knowledge as good, while less than one-third (28.7%) had received some specific education related to internet security and privacy protection issues.

A significant difference among the four examined groups of online users was found only concerning the self-assessed riskiness of online behavior, where students and administrative staff rated themselves higher. However, no difference was found in the perceived riskiness of simulated real online behavior. Additionally, there was no significant difference in either of the two cognitive subscales regarding security awareness among the examined groups (Table 1).

TABLE I. Average Scores and Differences Between Groups for Each Subscale

Subscale	Median (interquartile range)				p-value
	Students N=120	*Healthcare professionals N=169*	*Administrative staff N=92*	*Average user N=103*	
Behavior scale: Simulation of risky behavior (from 0 to 3)	0 (0–1.8)	0 (0–0)	0 (0–1)	0 (0–0)	0.37
Behavior scale: Self-assessed risky behavior (from 1 to 4)	1 (1–1.3)	1.3 (1–1.5)	1 (1–1.5)	1.3 (1–1.5)	***0.03***
Cognitive scale: Importance of Protection (from 1 to 5)	4 (3.5–4.3)	4 (3.5–4.5)	4 (3.5–4.5)	4 (3.5–4.5)	0.99
Cognitive scale: Awareness of Risk (from 1 to 5)	4 (2.7–4.8)	4 (3–4.8)	4 (2.4–5)	4 (3–4.6)	0.86

a. For Behavioral Scales Lower Number is Better Score; Kruskal Wallis test (with Conover post-hoc) was utilized

In the first table, concerning median scores, there are relatively low average scores for risky online behavior and comparatively high average scores for security awareness in all four examined groups (Table 1).

The correlation between scores of pairs of subscales is negligible in every one of the six pairs, even though it is statistically significant in two cases. The most concerning result is that there is no correlation between self-assessed and simulated real riskiness in online behavior, while a strong positive correlation would ideally be expected (Table 2).

Unexpectedly, only 7.25% of all participants responded correctly to the deceptive question concerning the acceptance of terms and conditions. However, even that there was no significant difference between groups of examinees, students showed slightly better results (Table 3).

TABLE II. CORRELATIONS BETWEEN EACH SUBSCALE AMONG ALL EXAMINEES

Pair of subscales	Spearman's correlation coefficient (*p*-value)		
	Behavior scale: Simulation of risky behavior	***Behavior scale: Self-assessed risky behavior***	***Cognitive scale: Importance of Protection***
Behavior scale: Simulation of risky behavior	–		
Behavior scale: Self-assessed risky behavior	-0.035 (0.44)	–	
Cognitive scale: Importance of Protection	0.007 (0.88)	***-0.144 (0.001)***	–
Cognitive scale: Awareness of Risk	-0.016 (0.72)	-0.066 (0.15)	***0.178 (<0.001)***

a. For Behavioral Scales Lower Number is Better Score; Spearman's rank correlation test was utilized

IV. DISCUSSION

The assumption that healthcare professionals exhibit riskier behavior when handling digital data due to higher job-related stress was not confirmed. Specifically, the investigation into risky online behavior (measured by the Behavioral subscale: simulation of risky behavior) did not significantly differ among any of the four observed groups of participants. However, through a separate deceptive question concerning the acceptance of terms and conditions, assessing how well participants read instructions before responding, it was revealed that students exhibited slightly better (at the borderline of statistical significance) regarding the riskiness of online behavior compared to healthcare workers, administration staff, and the control group.

The results of this study indicated that healthcare professionals (as well as the control group) self-assessed their risky online behavior less favorably compared to administrative workers and students, as measured by the Subscale of self-assessed risky behavior. They seem to be somewhat more self-critical. The results of the analysis of awareness levels on information security issues, measured by two cognitive subscales, showed no significant differences among the four observed groups of participants. Moreover, all participants demonstrated a relatively high level of awareness regarding online risks and the importance of protection against cyber-attacks.

Overall, current and future employees in the healthcare system do not significantly deviate from the control group regarding the riskiness of online behavior or behavior when handling digital data, nor in terms of awareness of information security. Students even showed slightly better results, contrary to previous research indicating a higher inclination towards online risks during adolescence [19, 21]. The results of this study are also somewhat inconsistent with the research of Alhuwail et al. [24], whose findings suggest that professionals with more work experience demonstrate greater compliance with good cyber security practices.

TABLE III. CORRECT RESPONSE TO THE DECEPTIVE QUESTION AMONG GROUPS OF EXAMINEES

Response	Number (%) of the participants			
	Students N=120	***Healthcare professionals N=169***	***Administrative staff N=92***	***Average user N=103***
Did not read full text	105 (87.5)	159 (94.1)	87 (94.6)	98 (95.1)
Responded correctly	15 (12.5)	10 (5.9)	5 (5.4)	5 (4.9)

a. $p = 0.08$; Chi-square test

Average scores for all participants across the subscales were surprisingly very good. Online users generally act relatively safely and exhibit high awareness of information security and privacy issues. The real riskiness of online behavior, measured with simulation questions, received an average grade of zero (on a scale from 0 to 3), indicating very good results. Additionally, results on self-assessed riskiness of online behavior also presented a relatively low level of risky online behavior with an average score of 1.3 (on a scale from 1 to 4). In the self-assessed awareness level regarding the importance of secure usage of computer systems and the internet, the results show that participants consider the protection of computer equipment, laptops, and smartphones, as well as logging out from various information systems after completing work, important. The average score of 3.9 on a scale from 1 to 5 is very good, as for cognitive awareness subscales, higher scores indicate better awareness. The cognitive risk subscale measures the self-assessed level of awareness of potential risks in internet usage. It was evaluated as highly risky, encompassing the misuse of credit or debit cards, identity theft on the Internet, and hacking personal computers or smartphones. The obtained average score of 3.73 on a scale from 1 to 5 is also very good, indicating a high level of awareness of potential risks among the participants of this study.

As fewer than one-third of all participants received specific education related to internet security and privacy protection issues, it seems that the lack of specific education does not negatively influence the riskiness of online behavior or security awareness. However, it is concerning, yet consistent with previous results, that there is an absence of the expected positive correlation between self-assessment and actual behavior among online users [22]. It seems that these online users generally believe they act safely on the Internet when they actually do not, and vice versa.

Additionally, there is also no correlation between the riskiness of online behavior and the level of security awareness. This phenomenon, known as the *privacy paradox*, has been observed in previous research, where users express concerns about their privacy but take little action to protect their personal data [25, 26].

Another unexpected result was that only 7.25% of all participants answered correctly to the deceptive question concerning the acceptance of terms and conditions, which required simultaneous acceptance and rejection of consent after reading a somewhat long and *boring* text with instructions hidden within. In a previous study, results revealed that 74% skipped reading terms of service and privacy policy, selecting the *quick join* clickwrap when joining a fictitious social networking service [27]. Terms of service and privacy agreements are generally verbose and full of legal jargon, making them difficult to read and understand [28].

A similar situation arises with the acceptance of cookies, where users are presented with the option to access more information about cookies. However, upon opening, users encounter a large text, typically written in a small and visually unattractive font. Although this text naturally contains all the legal information, its extensive nature and lack of user-friendliness often deter ordinary users from reading it. Consequently, most users opt for the *I accept* option automatically [29]. Skipping the reading of certain instructions, information about services, or legal regulations is a common practice but poses potential risks in terms of information security. Uninformed acceptance of a particular service can facilitate data theft, especially since spear phishing employs sophisticated emails that are challenging to detect. Recognizing such emails requires more attention, as users must evaluate the credibility of the written text, not just the visual elements [6].

In the future research, it would be valuable to explore additional data on a broader and wider population of participants, possible on international sample. Additionally, it would be beneficial repeat this research in real time high stress environment. Further investigation could shed light on why users exhibit relatively safe behavior, especially considering that more than 90% of them did not read the deceptive question on accepting terms and conditions.

V. CONCLUSION

With this empirical research, generally surprising positive results were obtained regarding the behavior of participants concerning information security. However, an exception was found in the responses to the deceptive question regarding the acceptance of terms and conditions.

The assumption that healthcare workers exhibit riskier behavior when handling digital data was not confirmed, as the riskiness of online behavior did not significantly differ among the four observed groups of participants. Nevertheless, a separate deceptive question revealed that students exhibited slightly better in terms of the riskiness of online behavior compared to healthcare workers, administration staff, and the control group.

Most participants rated their knowledge of information security as good, but students and administrative workers significantly assessed themselves as less risky compared to healthcare workers and the control group of participants. All participants, on average, have a very high level of awareness regarding security and privacy issues. Additionally, as less than one-third of all participants received specific education related to internet security and privacy protection issues, it seems that the lack of specific education doesn't negatively influence the riskiness of online behavior or security awareness.

No correlation was found between the subscales of simulating risky online behavior and self-assessment of risky online behavior. Similarly, no correlation was observed between the subscales of riskiness in handling digital data and the level of awareness of information security.

Despite the findings suggest rather safe online behavior and rather high security awareness among internet users, a notable majority of participants in this study provided consent to the deceptive question on terms and conditions.

REFERENCES

[1] H. Belani, "Understanding privacy basics in healthcare," *Bilt Hrvat Druš Za Med Inform (Online)*, vol. 28, no. 2, pp. 4–14, Jun. 2022, [Online]. Available: https://hrcak.srce.hr/285167

[2] S. Nifakos et al. "Influence of human factors on cyber security within healthcare organisations: a systematic review," *Sensors*. vol. 28, no. 15, pp. 5119, Jul. 2021, Available: https://doi.org/10.3390/s21155119

[3] C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technol Health Care*, vol. 25, no. 1, pp. 1–10, Feb. 2017, doi: 10.3233/THC-161263,

[4] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions," *IEEE Access,* vol. 9, pp. 7152–7169, Jan. 2021, doi: 10.1109/ACCESS.2020.3048839,

[5] Y. He, A. Aliyu, M. Evans and C. Luo, "Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review," *J Med Internet Res*, vol. 23, no. 4, pp. e21747, Apr. 2021. doi: 10.2196/21747,

[6] M. S. Jalali, M. Bruckes, D. Westmattelmann and G. Schewe, "Why employees (still) click on phishing links: investigation in hospitals," *J Med Internet Res*, vol. 22, no. 1, pp. e16775, Jan. 2020, doi: 10.2196/16775,

[7] G. Lorenzini, D. M. Shaw and B. S. Elger, "It takes a pirate to know one: ethical hackers for healthcare cybersecurity," *BMC Med Ethics,* vol. 23, no. 1, pp. 131, Dec. 2022, Available: https://doi.org/10.1186/s12910-022-00872-y,

[8] D. R. Farringer, "Maybe if we turn it off and then turn it back on again? Exploring health care reform as a means to curb cyber attacks," *J Law Med Ethics*, vol. 47, no. 4, pp. 91–102, Jan. 2020, doi: 10.1177/1073110519898046,

[9] S. Chaudhary, V. Gkioulos and S. Katsikas, “Developing metrics to assess the effectiveness of cybersecurity awareness program,” *J Cybersecurity*, vol. 8, no. 1, pp. tyac006, May 2022, Available: https://doi.org/10.1093/cybsec/tyac006

[10] D. Sturman et al, “The role of cue utilization in the detection of phishing emails,” *Appl Ergon*, vol. 106, Jan. 2023, Available: https://doi.org/10.1016/j.apergo.2022.103887,

[11] Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman and C. Sample, “Characterizing and measuring maliciousness for cybersecurity risk assessment,” *Front Psychol*, vol. 9, Feb. 2018, Available: https://doi.org/10.3389/fpsyg.2018.00039

[12] A. U. Patel et al, “Cybersecurity and information assurance for the clinical laboratory,” *J Appl Lab Med*, vol. 8, no. 1, pp. 145–161, Jan. 2023, doi: 10.1093/jalm/jfac119,

[13] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, Available: https://doi.org/10.1016/j.maturitas.2018.04.008

[14] B. Stack, “Here’s how much your personal information is selling for on the dark web,” *Experian*, Dec. 2017. [Online]. Available: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[15] M. Searles, “2022 HIMSS Healthcare cybersecurity survey,” HIMSS, Chicago, USA, Jan. 2022, [Online]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

[16] H. Ghayoomi, K. Laskey, E. Miller-Hooks, C. Hooks and M. Tariverdi, “Assessing resilience of hospitals to cyberattack;” *Digit Health*, Nov. 2021, doi: 10.1177/20552076211059366,

[17] A. Sardi, A. Rizzi, E. Sorano and A. Guerrieri, “Cyber risk in health facilities: a systematic literature review,” *Sustainability*, vol. 12, no. 17, pp. 7002, Aug. 2020, Available: https://doi.org/10.3390/su12177002,

[18] Dw. Kim, Jy. Choi and Kh. Han, “Risk management-based security evaluation model for telemedicine systems,” *BMC Med Inform Decis Mak*, vol. 20, no. 1, pp. 106, Dec. 2020, Available: https://doi.org/10.1186/s12911-020-01145-7

[19] T. Velki and M. Milic, “Stress as a mediator between risk and protective factors and online risky behaviors in adolescents,” *Primenj Psihol*, vol. 14, no. 2, pp. 149–71. Jul. 2021, Available: https://doi.org/10.19090/pp.2021.2.149-171

[20] T. Velki and K. Solic, “Development and validation of a new measurement instrument: the Behavioral-Cognitive Internet Security Questionnaire (BCISQ),” *Int J Electr Comput Eng Syst*, vol. 10, no. 1, pp. 19–24, Dec. 2019, doi: 10.32985/ijeces.10.1.3,

[21] T. Velki and K. Solic, “Development of social engineering research tool on college student population: Behavioural Cognitive Internet Security Questionnaire (BCISQ),” *Polic. sigur,* vol. 29, no. 4, pp. 341–355,

[22] K. Solic, T. Velki, I. Fosic and M. Vukovic, “Study on information security awareness using the Behavioral-Cognitive Internet Security Questionnaire,” *Acta Polytech. Hungarica*, vol. 21, no. 4, 49–68, 2024, doi: 10.12700/APH.21.4.2024.4.3,

[23] K. Solic, R. Idlbek and T. Velki, “Empirical study on differences between self-assessed and measured real risk in online behavior,” *Int J Electr Comput Eng Syst*, 2024, in press,

[24] D. Alhuwail, E. Al-Jafar, Y. Abdulsalam and S. AlDuaij, “Information security awareness and behaviors of health care professionals at public health care facilities,” *Appl Clin Inform*, vol. 12, no. 4, pp. 924–932, Aug. 2021, doi: https://doi.org/10.1055/s-0041-1735527,

[25] Z. Aivazpour and V. S. (Chino) Rao, “Information disclosure and privacy paradox: the role of impulsivity,” *ACM SIGMIS Database: the DATABASE Adv Inf Syst,* vol. 51, no. 1, pp. 14–36, Jan. 2020, Available: https://doi.org/10.1145/3380799.3380803

[26] I. Khan, J. Loh, A. Hossain and J. H. Talukder, “Cynicism as strength: Privacy cynicism, satisfaction and trust among social media users,” *Comput Hum Behav*, vol. 142, pp. 107638-107638, Dec. 2022, doi: 10.1016/j.chb.2022.107638,

[27] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services," Information, Communication & Society, vol. 23, no. 1, pp. 128–147, Jul. 2018. doi: 10.1080/1369118X.2018.1486870,

[28] T. Perera and T. Perera, "Barrister-processing and summarisation of terms & conditions / privacy policies," Proceedings in 6th International Conference for Convergence in Technology (I2CT), pp. 1–7, 2021, doi: 10.1109/I2CT51068.2021.9418090,

[29] O. Kulyk, K. Renaud, S. Costica, “People want reassurance when making privacy-related decisions – not technicalities,” J Syst Softw, vol. 200, pp. 111620 Jun. 2023, Available: https://doi.org/10.1016/j.jss.2023.111620