An empirical study on differences between self-assessed and measured real risk in online behaviour

Idlbek, Robert; Velki, Tena; Šolić, Krešimir

Source / Izvornik: **International journal of electrical and computer engineering systems, 2024, 15, 297 - 304**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

https://doi.org/10.32985/ijeces.15.3.8

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:277:808295

An empirical study on differences between self-assessed and measured real risk in online behaviour

Original Scientific Paper

Krešimir Šolić
J. J. Strossmayer University of Osijek,
Faculty of Medicine, Department of Medical Statistics and Medical Informatics
Josipa Huttlera 4, Osijek, Croatia
kresimir@mefos.hr

Robert Idlbek
J. J. Strossmayer University of Osijek,
Faculty of Tourism and Rural Development, Department of Computer Science
Vukovarska 17, Požega, Croatia
ridlbek@ftrr.hr

Tena Velki
J. J. Strossmayer University of Osijek,
Faculty of Education, Department of Social Sciences
Ul. Cara Hadrijana 10, Osijek, Croatia
tvelki@foozos.hr

Abstract *– As the leading cause of security breaches is human susceptibility to hackers' deception, the riskiness of an individual's online behaviour and low awareness regarding privacy protection significantly influence the overall security of an information system. Thus, this study aimed to compare self-assessed and measured real risk in online behaviour among online users. The additional aim was to modify the questionnaire by replacing the existing trick question about password quality with the new questions on accepting the terms and conditions. An international online Behavioral Cognitive Internet Security Questionnaire (BCISQ), validated in previous studies, was used for data collection. The examinees involved in this study were 278 students from different faculties. The results showed a relatively high level of risk in online behaviour, as 22.7% of examinees revealed their passwords.*

In comparison, only 10.8% read the consent statement. Students who behave in a riskier manner self-assess themselves as being significantly safer in online behaviour, which is contradictory. They also performed worse in all other examined variables. The new version of the simulation subscale, with improved internal consistency and reliability (Cronbach's Alfa=0.810), consists of only three items, which are questions used in the previous version, without adding any of the two tested trick questions. Generally, this study concludes that, on average, information security awareness is still low among online users and that even the ones realistically acting riskier believe they are acting more safely.

Keywords: *information security, information system, security awareness, user behaviour*

Received: November 12, 2023; Received in revised form: January 21, 2024; Accepted: January 22, 2024

1. INTRODUCTION

The direct or indirect aim of the security breach on an information system is basically to gain some financial benefit. Therefore, in the beginning, the information systems of the banking sector were best protected by additional national and international regulations. Onwards, security experts, who were primarily managers of security regulations, were focused on information security policies in business companies and healthcare information systems, as loss of public reputation can indirectly cause financial loss. Nowadays, information security and privacy protection focus on any information system in the business and non-profit sectors and public and private areas. However, for many years, the information system user has been identified as the weakest link in information security protocols, as the leading cause of security breaches is human susceptibility to hacker's

deception [1]. So, the human factor still represents the central junction regarding cyber-attacks [2]. Therefore, influencing user behaviour, raising security awareness, and protecting an individual's privacy will increase the overall security of an information system.

Level of knowledge, behaviour toward following security guidelines and learning inertia can significantly influence information security awareness [3]. However, users are susceptible to social engineering despite targeted education [4]. Furthermore, even highly aware online users often give personal data away voluntarily and behave in a high-risk manner on the internet [5]. It is very worrying and confusing, but no comprehensive explanation for this privacy paradox has been found so far [6]. However, although insufficient, education still significantly impacts increasing safety in online behaviour [7].

Further cyber security training to improve digital trust is needed to raise individuals' awareness [8-11]. New concepts to solve the problem of risky behaviour and low-security awareness should combine periodic education regularly with some notification system. Some studies also suggest that future learning models should use more interactive educational methods and should be based on simulation procedures [12, 13].

Online user's text-based passwords are still the first line of defence. However, they are still weak in securing all kinds of information systems. Users' careless security behaviour, involving password reuse, writing down and sharing passwords, and creating short or low-quality passwords are the main problems related to password security issues [14]. Modelling users' risky online behaviour based on analysing millions of passwords, both the most frequent passwords and how users create new passwords, can be helpful to hackers [15, 16].

The quality of the password, e.g., how the password is constructed, differs between students, average users, and professionals [17]. Average online users like having and using usernames and passwords with similar characters - the first few digits or the last few digits in a decade system, while the most used unique character is the underscore sign [18]. Additionally, male users have significantly stronger passwords than female ones, and password complexity decreases with age [19]. Also, 72% of users based their passwords on a single word or used a simple sequence of digits. Meanwhile, 39% of examined passwords were found in word lists of previous password leaks [19]. An additional paradox regarding the quality of passwords is as follows: a simple one is easier to remember, but a complicated one is more secure from being guessed [20].

Most research studies regarding passwords are focused on their quality. However, as the most essential property of a password is its secrecy, other properties such as length and the combination of special characters are becoming irrelevant. Findings in previous studies have shown that up to three out of four average online users will, in some cases, reveal their passwords, mainly to a friend, college, or authority figure. The easiest way to find someone's password is to ask for it. However, over the last few years, a promising trend has shown specific improvements [21].

Password disclosure becomes a big problem when someone logs in and thus impersonates the system during identification. That is why advanced additional confirmation methods, such as biometrics and blockchain technology, are increasingly used during authentication [22-24]. The most secure way is to use the three-factor authentication (3FA) scheme to identify itself through three categories of authentication factors (knowledge, possession and inherence): something you know, have, and are.

Many online users, or even most, have never read the terms and conditions but accept them without reading and understanding. A probable reason is that terms and conditions are verbose and contain legal jargon [25]. Accepting something online without reading it can lead to significant information security and privacy risks, and younger online users are more careless regarding reading terms and conditions [26]. Reading terms and conditions is related to concern for privacy, positive perceptions about notice comprehension, and higher trust in the notice. Three-quarters of participants included in one study skipped reading privacy policies, as they view policies as a nuisance and ignore them [27]. The results of another study have shown that most participants will skip reading the privacy policy if it is not presented by default [28].

This study aimed to analyse users' risky online behaviour to compare self-assessed and measured actual levels of risk. It also examined the awareness and knowledge of information security and privacy protection issues. The additional aim was to modify the questionnaire by replacing the existing trick question about password quality with the new trick question on accepting terms and conditions to improve the internal consistency and reliability of the simulation subscale. The study was based on a Croatian version of the previously developed and statistically validated international online questionnaire: the Behavioral Cognitive Internet Security Questionnaire (BCISQ) [29].

The BCISQ was chosen as it measures real risky online behaviour with its simulation subscale compared to similar solutions. Many empirical studies on this subject have been made. However, only several statistically validated questionnaires are developed as the basis for empirical studies dealing with information system users' risky behaviour. One of the most used is the SeBIS (Security Behavior Intentions Scale), which was developed in the USA and published in 2016 [30]. Then, in the same year, the FMS (Four Measurements Scales) was designed and validated in Turkey [31]. Then, the HAIS Q (Human Aspects of Information Security) was developed in Australia, with a validated version published in 2017 [32].

2. MATERIALS & METHODS

An internationally validated Behavioral Cognitive Internet Security Questionnaire (BCISQ) was used for data collection. This questionnaire has only an online version currently available in four languages at http://security.o-i.hr. The BCISQ consists of four subscales and measures: simulated risky online behaviour, self-assessed risk of online behaviour, cognitive awareness of online risks, and the importance of safe online usage. The questionnaire uses 17 items divided into subscales and has additional demographic questions [29]. In this research, a Croatian version of a questionnaire was used.

This study primarily focuses on measuring a real online risk by analysing the data gathered with the first subscale that simulates real online risky situations, emphasising the trick question about password quality and, with additional, new trick question examining how much online users read terms and conditions. However, all collected data are correlated with the other three subscales and demographic questions in further analysis.

The simulation subscale consists of four questions, with the first two asking if the examinee would like to receive notifications from third-party partners about similar studies and free antivirus software from third-party partners via email. The third question asks the examinee to leave an email address, and the fourth question, positioned at the end of the BCISQ questionnaire, is a trick question asking the examinee to reveal their most used password. A trick question is constructed so that the examinee is deceived by scientific and anonymous research to write down a password to help researchers examine the quality of the password's security (Fig. 1).

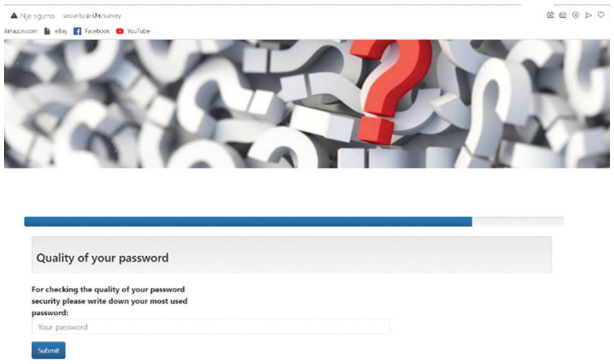

Fig. 1. Visual of the trick question regarding password quality

As participants in this study were Croatian students, an additional question was constructed for this research only in the Croatian version of the BCISQ questionnaire. This additional, new trick question was named Statement of Consent for processing personal data and has 318 words of text explaining what the GDPR is and why this research is essential. After approximately 80% of a text, there is an instruction for the examinee to mark both squares: to both agree and disagree (Fig. 2).

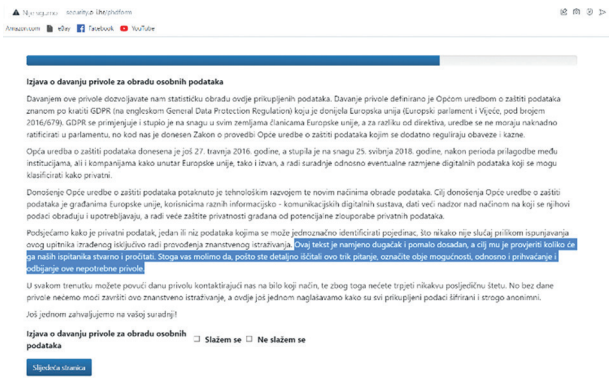

Fig. 2. Position of explanation in the trick question regarding (not) reading terms and conditions

Here is the text of the new question, translated to English under the title: Statement of consent for processing personal data

By giving this consent, you allow us to statistically process the data collected here. Consent is defined by the General Data Protection Regulation, known by the abbreviation GDPR (in English General Data Protection Regulation), adopted by the European Union (European Parliament and Council, under number 2016/679). The GDPR is applied and enforced in all European Union member states. Unlike directives, regulations do not have to be subsequently ratified in parliament. However, we have adopted the Law on Implementing the General Data Protection Regulation, which regulates obligations and penalties.

The General Data Protection Regulation was adopted on April 27, 2016. It came into force on May 25, 2018, after a period of adjustment among institutions and companies both within and outside the European Union and for cooperation, i.e., the eventual exchange of digital data that can be classified as private.

The adoption of the General Data Protection Regulation was prompted by technological development and new ways of data processing. The goal of adopting the General Regulation on Data Protection is to give citizens of the European Union, users of various information and communication digital systems, greater control over how their data is processed and used and for more excellent protection of citizens' privacy from potential misuse of private data.

We remind you that private data is one or a series of data that can uniquely identify an individual, which is by no means the case when filling out this questionnaire created solely to conduct scientific research. This text is deliberately lengthy and somewhat dull, and its goal is to check how many of our respondents will read it. Therefore, after reading this trick question in detail, we instruct you to mark both options to accept and decline this unnecessary consent.

You can withdraw your consent at any time by contacting us in any way, and you will not suffer any consequential damages. However, without consent, we cannot complete this scientific research, and here, we emphasise that all collected data is encrypted and strictly anonymous.

Thank you once again for your cooperation!

□ *I agree* □ *I do not agree*

This new trick question has been planned to examine how many examinees read the Statement of consent. So, the text itself is of no importance. It is not very informative but deliberately long. At the same time, the crucial sentence with instructions for examinees is underlined only here in the translation text.

The authors attempted to replace the existing trick question asking for a password with the new trick question by examining the reading of the Statement of consent, as previous research had shown that the question on a password decreased the stability (internal consistency and reliability) of the simulation subscale of risky online behaviour [33]. It was also unclear if the revealed password was real and still actual for this particular examinee, as even the examinee could leave this field blank. Many of them wrote down something in a way that they did not want to write down their password. Before analysis, all passwords were inspected and removed if they did not look like actual passwords.

Standard statistical methods were applied to the collected data, where each used statistical model is pointed out at the bottom of each table. Categorical data are presented with absolute and relative frequencies. At the same time, the Chi-square Test was used to compare categorical data between independent groups. A normality test was applied to each distribution of numerical data to choose a parametric or nonparametric test and how to present the average value (median or arithmetic mean). Because distributions of examined numerical data did not follow Gaussian normal distribution, data were presented with median, interquartile and total range. They were tested with a nonparametric Mann-Whitney Test for independent samples. When modifying the examined subscale, Cronbach's alpha coefficient was calculated to estimate each version's internal consistency and reliability. Analysis was done in the statistical tool MedCalc (version 20.218, 64-bit, MedCalc Software Ltd), with statistical significance set at $\alpha=0.05$, where all P values were two-tailed.

The examinees were 278 students from different J. J. Strossmayer University of Osijek faculties. There were 48 students from the Faculty of Education, including 28 studying rehabilitation; 73 from the Faculty of Medicine, including 33 studying to be laboratory technicians; 49 from the Faculty of Dental Medicine, including nursing and physiotherapy; 19 from the Faculty of Tourism and Rural Development, and 11 from the Faculty of Economics, while the rest were from other faculties and gathered mainly on the university campus. As future engineers have already proven, in a previous study, to be a specific sample, because they are not average Internet users, they were deliberately left out of this research. Another reason for excluding them was that the quality of the password, e.g., how the password is constructed, differs between students, professionals (future engineers), and average users [17].

Data were collected mainly in classrooms, as students were asked by professors, often before their lectures, to fill out online questionnaires. The link was shared through the official communication channels for teaching materials.

The students had a median age of 19, an interquartile range of 18 to 20, and a total range of 17 to 38 years old. There were 21.4% male students, 42.1% had some training regarding information security awareness, and 85.4% had self-assessed their knowledge of information security and privacy as good or excellent.

3. RESULTS AND DISCUSSION

Two main results, password revealing and not reading a statement of consent, present a relatively high level of risk in average users' online behaviour. Thus, out of 278 students, even 158 (56.8%) had written down and revealed their passwords in replying to the trick question on password quality. Because there were obvious false passwords among them (e.g., No, I will not, 123456, and similar), after the personal assessment of each answer, the number of "presumably real and discovered" passwords was reduced to 63 (22.7%). The assessment of each answer, the false password evaluation, was done as a consensus of experts, the authors of this research. However, on the new trick question regarding giving consent for data processing for research purposes, only 30 (10.8%) indicated how it was in question and requested (both to accept and decline) and, in that way, confirmed that they had read the consent. Among others, 38 (13.7%) students declined consent but continued to answer other questions and finished the whole questionnaire, while most examinees (210, 75.5%) gave their consent obviously without carefully reading it first. Here, it can be assumed that examinees may feel the false security of authority, just like when giving out the password - at the university under the supervision of the professor.

Revealing passwords and giving consent without reading the terms and conditions are two actions that can be considered hazardous online behaviour. As the P value is close to the significance level, there could be a potential correlation between these two risky actions among average online users, meaning that online users who reveal passwords usually do not read the Statement (Table 1). In total, 60 (21.6%) examinees did both risky actions. In further analyses, they were compared to the other examinees regarding all examined variables (Table 2).

Table 1. Comparison between revealing password and not reading statement

	Read statement	Didn't read statement	Total	*P**
Didn't reveal password	27 (90.0)	188 (75.8)	215 (77.3)	0.079
Revealed password	3 (10.0)	60 (24.2)	63 (22.7)	
Total	**30 (100.0)**	**248 (100.0)**	**278 (100.0)**	

*Chi-square Test

Table 2. Differences between most risky examinees and the others

Examined variable with categories		Didn't read statement and revealed password /*n*=60	Others /*n*=218	*P*
Gender/*n*(%)	male	8 (13.3)	52 (23.9)	0.079*
	female	52 (86.7)	166 (76.1)	
Age/median (25%-75%)		19 (19.0 - 21.0)	19 (18.0 - 20.0)	***0.016***
Self-assessed knowledge on security and privacy/*n*(%)	poor	13 (21.7)	28 (12.8)	0.119*
	good	43 (71.7)	161 (73.9)	
	excellent	4 (6.7)	29 (13.3)	
Previous training on security/*n*(%)	Yes	26 (43.3)	90 (41.3)	0.776
	No	34 (56.7)	128 (58.7)	
Notifications from third-party partners about similar studies/*n*(%)	Yes	12 (20.0)	25 (11.5)	0.085
	No	48 (80.0)	193 (88.5)	
Receiving free anti-virus software from third-party partners/*n*(%)	Yes	22 (36.7)	60 (27.5)	0.169
	No	38 (63.3)	158 (72.5)	
Personal email address left /*n*(%)	Yes	20 (33.3)	51 (23.4)	0.118
	No	40 (66.7)	167 (76.6)	
Self-assessed risky of online behavior***/median (25%-75%)		1.0 (1.0 - 1.3)	1.3 (1.0 - 1.5)	***0.030***
Cognitive importance of safe online usage/median (25%-75%)		4 (3.5 - 4.5)	4 (3.5 - 4.4)	0.595**
Cognitive awareness of online risks/median (25%-75%)		4.2 (2.8 - 4.8)	4.4 (3.2 - 4.8)	0.189**

*Chi-square Test | **Mann-Whitney Test | ***Higher score means riskier behavior

On the other three questions from the Simulation subscale, 37 (13.3%) examinees answered positively regarding receiving notifications from third-party partners about similar studies, and 82 (29.5%) answered positively regarding receiving free antivirus software from third-party partners via email. Personal email addresses were left by 71 (25.5%) of all examinees in order to receive notifications and free promotional materials.

Students who did not read the Statement and revealed the password, which is a risky action, are significantly older (Mann-Whitney test, P=0.016) than other students. However, as the absolute value of the difference is not high, maybe this result is not that important. A significant result is a significant difference in self-assessed risk of online behaviour (Mann-Whitney test, P=0.030), meaning that contradictory students that behave riskier self-assess themselves as significantly safer in online behaviour. Generally, students who behave riskier are worse in all other examined variables, except in evaluating the importance of safe online usage, even though this finding lacks statistical significance (Table 2).

The additional aim of this study was to upgrade the first subscale of the BCISQ questionnaire that measures the risk of actual online behaviour by simulating some risky online situations. The plan was to change the existing trick question on password disclosure with the new trick question on giving consent without reading the terms and conditions. Here are the results concerning Cronbach's alpha coefficient, which measures the internal consistency and reliability of a set of survey items, in this case, questions constructing a simulation subscale (Table 3).

Table 3. Differences in internal consistency regarding items of simulation subscale

Steps in statistical analysis	Number of items constructing subscale	Cronbach's alpha coefficient*	Effect of dropping variable
Step one	Four items (initial version from previous studies)	0.6812	revealing password causes change of +0.1288
Step two	Five items (added trick question on giving consent)	0.6192	giving consent, change of +0.06199 revealing password, change of +0.05677
Step three	Four items (with trick question on giving consent instead of revealing password question)**	0.6760	giving consent causes change of +0.1340
Finale step	Three items (excluded both trick questions)	0.8100	(best result)

*coefficient needs to be > 0.7 | **aim was to switch two trick questions

Even though this analysis aims to switch the existing trick question on revealing a password with the new trick question on accepting consent without reading it, the first step analysed the simulation subscale's version from the previously validated and used version of the BCISQ questionnaire. The result in step one in the table confirms that this subscale needs to be corrected and upgraded, as shown in the previous study [33] - Cronbach's alpha coefficient is lower than 0.7. The effect of dropping the trick question will increase the value of the coefficient (Table 3).

Adding a new trick question further reduces the value of Cronbach's alpha coefficient. In contrast,

dropping each trick question will positively affect the internal consistency and reliability of the simulation subscale. The analysis result in step three additionally confirms that the new trick question on accepting conditions without reading them does not contribute to the internal consistency and reliability of the simulation subscale and thus needs to be dropped. However, the final step of Cronbach's alpha coefficient analysis shows an outstanding result, meaning that the internal consistency and reliability of the simulation scale are best if only three items are included. So, the result is to exclude both trick questions and construct a simulation scale with only three previously existing questions regarding receiving notifications, free antivirus, and revealing a personal email address.

4. CONCLUSIONS

The revealing of passwords and the giving of consent without reading applicable terms and conditions are two actions that could be considered extremely risky online behaviour, according to the primary results (22.7% of users revealing their passwords and even 89.2% not reading the terms and conditions), it can be concluded that behaviour is still quite risky among online users. The main result, showing a contradiction between the self-assessed and measured real risk of online behaviour, further highlights this problem. The result shows that users who behave riskier self-assess themselves as performing significantly better in risky online behaviour than they do. Users who engage in risky behaviour think they are acting safely online.

This unexpected result draws a conclusion that can be very important to information security managers and cyber security trainers. It shows that special care needs to be directed towards self-confident users, as they behave in a riskier manner when dealing with digital online data.

It seems that this particular, statistically significant result is new and not comparable but is additional information to the other empirical studies on this subject, mentioned previously in the Introduction section.

Results concerning the additional aim of this study have shown that authors were unsuccessful in replacing the old trick question asking for a password with the new trick question regarding giving consent when not reading terms and conditions. However, concerning internal consistency and reliability, the result of the simulation subscale is to reduce the subscale on three existing items presenting questions.

That is another unexpected result, but it implies a new and better simulation subscale than the previous version. So, the additional result of this empirical study is a new, improved version of the Behavioral Cognitive Internet Security Questionnaire.

Even though students were from different university faculties, excluding engineers as untypical online users, it is incorrect to conclude that these results can apply to the average online user. Another drawback of this study is the relatively small sample size, constructed only of students and only from students in their lower years of study.

Potential future research should examine all kinds of users to evaluate the average user's level of risk in online behaviour, as information security awareness is still low. Another highly beneficial research would be a review article of all the existing empirical studies on information security and privacy protection, focusing on users' awareness, knowledge and behaviour.

5. REFERENCES

[1] S. Goel, K. Williams, E. Dincelli, "Got Phished? Internet Security and Human Vulnerability", Journal of the Association for Information Systems, Vol. 18, No. 1, 2017, pp. 22-44.

[2] D. R. Vuţă, E. Nichifor, O.M. Tierean, "Extending the Frontiers of Electronic Commerce Knowledge through Cybersecurity", Electronics, Vol. 11, No. 14, 2022, p. 2223.

[3] J. Zhen, K. Dong, Z. Xie, L. Chen, "Factors Influencing Employees' Information Security Awareness in the Telework Environment", Electronics, Vol. 11, No. 21, 2022, p. 3458.

[4] H. Aldawood, G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs - Pitfalls and Ongoing Issues", Future Internet, Vol. 11, No. 3, 2019, p. 73.

[5] T. Velki, "Psychologists as information-communication system users: Is this bridge between information-communication and behavioural science enough to prevent risky online behaviours?", Proceedings of the 45th Jubilee International Convention on Information, Communication and Electronic Technology, Opatija, Croatia, 23-27 May 2022, pp. 1048-1052.

[6] N. Gerber, P. Gerber, M. Volkamer, "Explaining the privacy paradox: A systematic review of the literature investigating privacy attitude and behaviour", Computers & Security, Vol. 77, 2018, pp. 226-261.

[7] A. Bostan, I. Akman, "Impact of education on security practices in ICT", Tehnički Vjesnik - Technical Gazette, Vol. 22, No. 1, 2015, pp. 161-168.

[8] I. Borić-Letica, "Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary

School Students", International Journal of Electrical and Computer Engineering Systems, Vol. 10, No. 2, 2019, pp. 85-89.

[9] A. Tick, D. J. Cranfield, I. M. Venter, "Comparing Three Countries' Higher Education Students' Cyber Related Perceptions and Behaviours during COVID-19", Electronics, Vol. 10, No. 22, 2021, p. 2865.

[10] A. R. Gillam, W. T. Foster, "Factors affecting risky cybersecurity behaviours by U.S. workers: An exploratory study", Computers in Human Behavior, Vol. 108, 2020.

[11] L. Hadlington, "Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom", International Journal of Cyber Criminology, Vol. 12, No. 1, 2018, pp. 269-281.

[12] I. Ortiz-Garces, R. Gutierrez, D. Guerra, "Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions", Electronics, Vol. 12, No. 7, 2023, p. 1753.

[13] M. Amanowicz, M. Kamola, "Building Security Awareness of Interdependent Services, Business Processes, and Systems in Cyberspace", Electronics, Vol. 11, No. 22, 2022, p. 3835.

[14] V. Taneski, M. Heričko, B. Brumen, "Systematic Overview of Password Security Problems", Acta Polytechnica Hungarica, Vol. 16, No. 3, 2019, pp. 143-165.

[15] E. Y. Güven, A. Boyaci, M. A. Aydin, "A Novel Password Policy Focusing on Altering User Password Selection Habits: A Statistical Analysis on Breached Data", Computers & Security, Vol. 113, 2022, p. 102560.

[16] M. Curry, B. Marshall, J. Correia, R. E. Crossler, "InfoSec Process Action Model (IPAM): Targeting Insiders' Weak Password Behavior", Journal of Information Systems, Vol. 33, No. 3, 2019, pp. 201-225.

[17] R. Alomari, J. Thorpe, "On password behaviours and attitudes in different populations", Journal of Information Security and Applications, Vol. 45, 2019, pp. 79-89.

[18] W. Albattah, "Analysis of passwords: Towards an understanding of strengths and weaknesses", International Journal of Advanced And Applied Sciences, Vol. 5, No. 11, 2018, pp. 51-60.

[19] A. Juozapavičius, A. Brilingaitė, L. Bukauskas, R. G. Lugo, "Age and Gender Impact on Password Hygiene", Applied Sciences, Vol. 12, No. 2, 2022, p. 894.

[20] J. P. Kaleta, J. S. Lee, S. Yoo, "Nudging with construal level theory to improve online password use and intended password choice", Information Technology & People, Vol. 32, No. 4, 2019, pp. 993-1020.

[21] T. Velki, K. Romstein, "User Risky Behavior and Security Awareness through Lifespan", International Journal of Electrical and Computer Engineering Systems, Vol. 9, No. 2, 2018, pp. 53-60.

[22] M. A. El-Sayed, M. A. Abdel-Latif, "Achieving Information Security by multi-Modal Iris-Retina Biometric Approach Using Improved Mask R-CNN", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 6, 2023, pp. 657-665.

[23] N. Balan, V. Ila, "A Novel Biometric Key Security System with Clustering and Convolutional Neural Network for WSN", Tehnicki Vjesnik - Technical Gazette, Vol. 29, No. 5, 2022, pp. 1483-1490.

[24] V. Thakkar, V. Shah, "A Privacy-Preserving Framework Using Hyperledger Fabric for EHR Sharing Applications", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 6, 2023, pp. 667-676.

[25] T. Perera, T. Perera, "Barrister-Processing and Summarisation of Terms & Conditions / Privacy Policies", Proceedings of the 6th International Conference for Convergence in Technology, Maharashtra, India, 2-4 April 2021, pp. 1-7.

[26] P. Martiskova, R. Svec, M. Slaba, "Online Shopping and Reading E-Shops' Terms and Conditions", Education Excellence and Innovation Management through Vision 2020, Proceedings of the 33rd International Business Information Management Association Conference, Granada, Spain, 10-11 April 2019, pp. 682-690.

[27] J. A. Obar, 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, 2020, pp. 128-147.

[28] N. Steinfeld, "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment", Computers in Human Behavior, Vol. 55, Part B, 2016, pp. 992-1000.

[29] T. Velki, K. Šolić, "Development and Validation of a New Measurement Instrument: The Behavioral-Cognitive Internet Security Questionnaire (BCISQ)" International Journal of Electrical and Computer Engineering Systems, Vol. 10, No. 1, 2019, pp. 19-24.

[30] S. Egelman, M. Harbach, E. Peer, "Behavior ever follows intention? A validation of the security behaviour intentions scale (SeBIS)", Proceedings of the CHI Conference on Human Factors in Computing Systems, New York, NY, USA, May 2016.

[31] G. Öğütçü, Ö. M. Testik, O. Chouseinoglou, "Analysis of personal information security behaviour and awareness", Computer Security, Vol. 56, 2016, pp. 83-93.

[32] K. Parsons, D. Calic, M. Pattinson, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", Computer Security, Vol. 66, 2017, pp. 40-51.

[33] T. Velki, K. Šolić, B. Žvanut, "Cross-cultural validation and psychometric testing of the Slovenian version of the Croatian Behavioral-Cognitive Internet Security Questionnaire", Elektrotehniški Vestnik, Vol. 89, No. 3, 2022, pp. 103-108