Cross-cultural validation and psychometric testing of the Slovenian version of the Croatian Behavioral-Cognitive Internet Security Questionnaire

Velki, Tena; Šolić, Krešimir; Žvanut, Boštjan

Source / Izvornik: **Elektrotehniški vestnik, 2022, 89, 103 - 108**

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:141:709718

ELEKTROTEHNIŠKI VESTNIK 89(3): 103-108, 2022
ORIGINAL SCIENTIFIC PAPER

Cross-cultural validation and psychometric testing of the Slovenian version of the Croatian Behavioral-Cognitive Internet Security Questionnaire

Tena Velki[1], Krešimir Šolić[2], Boštjan Žvanut[3]

[1] J.J. Strossmayer University of Osijek, Faculty of Education, Croatia
[2] J.J. Strossmayer University of Osijek, Faculty of Medicine, Croatia
[3] University of Primorska, Faculty of Health Sciences, Slovenia
E-mail: bostjan.zvanut@fvz.upr.si

Abstract. The Behavioral-Cognitive Internet Security Questionnaire (BCISQ) is a reliable and validated measurement instrument that examines risky online behavior and security awareness of information-communication system users. It consists of four short subscales that measure the behavioral and cognitive aspects of a risky online behavior, including a simulation scale that measures an actual risky online behavior. Previous research on a Croatian sample of students shows a satisfactory construct validity and reliability of the English and Croatian BCISQ versions. The aim of our research is to cross-validate the BCISQ Slovenian version and to test the questionnaire for psychometric properties among Slovenian students. The research is conducted on Slovenian students (N = 151; Mage = 21.68; SD = 3.12). During their regular class, they fill in online BCISQ in the Slovenian language. The results show a good construct validity of BCISQ (CFI = 0.99, TLI = 0.99, RMSEA = 0.01) and a relatively satisfactory internal consistency (Cronbach α = 0.42 – 0.88) as well as test-retest reliability (ICC = 0.415 – 0.878). Future research about the information security can use BCISQ as a basic tool for reliable evaluation of a risky online behavior and security awareness among internet users.

Keywords: information security, questionnaire, students, Slovenian language, validation

Medkulturna validacija in psihometrično testiranje slovenske različice Behavioral-Cognitive Internet Security Questionnaire (BCISQ)

Behavioral-Cognitive Internet Security Questionnaire (BCISQ) je zanesljiv in validiran merski instrument, ki preučuje tvegano spletno vedenje in varnostno ozaveščenost uporabnikov informacijsko-komunikacijskega sistema. Sestoji iz 4 kratkih podlestvic, ki merijo vedenjske in kognitivne vidike tveganega spletnega vedenja, vključno s simulacijsko lestvico, ki meri dejansko tvegano spletno vedenje. Prejšnje raziskave na vzorcu hrvaških študentov so pokazale zadovoljivo konstruktno veljavnost in zanesljivost angleške in hrvaške različice BCISQ. Cilj pričujoče raziskave je navzkrižno validirati slovensko različico BCISQ in preizkusiti vprašalnik za psihometrične lastnosti na slovenskih študentih (N = 151; Mstarost = 21.68; SD = 3.12), ki so slovensko različico BCISQ izpolnili med predavanju. Rezultati so pokazali dobro konstruktno veljavnost BCISQ (CFI = 0.99, TLI = 0.99, RMSEA = 0.01), zadovoljivo notranjo sklandost (Cronbach α = 0.42 – 0.88) in test-retest zanesljivost (ICC = 0.415 – 0.878). Prihodnje raziskave na področju informacijske varnosti lahko uporabijo BCISQ kot osnovno orodje za zanesljivo ocenjevanje tveganega spletnega vedenja in varnostne ozaveščenosti med uporabniki interneta.

1 INTRODUCTION

The information security and data privacy have been a problem for a long time, and only ten years ago, interdisciplinary cooperation between information security engineers and behavioral experts took an effort to solve this problem [1].

Although well documented that users are the weakest link in the information and communication security system [2,3], a recent systematic literature review shows that there is still most of the research in the field of engineering with a predominately technical focus which doesn't take into consideration the human factor i.e. the impact of person's behavior when solving cybersecurity issues [4].

Numerous studies clearly show that users are unaware of potential online risks and behave risky in their online activities, even though they have some degree of knowledge about cybersecurity [5-8]. They rarely protect their online privacy although they know that the threat is high [9]. Users often consider themselves immune to tailored advertisements, and lack understanding of how automated approaches and algorithms work in relation to their network personal data [10]. A recent study shows

Received 6 June 2022
Accepted 27 June 2022

the importance of raising the awareness of the situational information security, where only the users past experience with phishing shows as relevant in increasing the security awareness, while the phishing e-mail's contextual relevance and misplaced salience have an opposite effect of reducing the users information security awareness [11].

It is particularly important that experts in both fields, i.e. behavioral science and ICT, emphasize the high risk online behavior. The study that examines the information security awareness and behavior on a sample of psychologists who are also experts in the ICT shows devastating results [5]. Although most of the participants in the online survey on conference with the central topic "Psychology and the Digital World" report about their good general technical knowledge of computers (80%) and some of them have previous education about the data privacy and internet security (38.2%), 40% of them gave their e-mail address and 45.5% their passwords, in 29% of the cases they give both data.

An additional problem is the users' self-assessment, which in fact is not aligned with their actual online behavior. One field study [12] shows that self-reported online behavior has non-zero correlations with the actually observed online behavior, and another one [5] finds there is no statistically significant association between self-assessed and simulated online risk behavior even in experts. Obviously, self-reported measurement of one's risky online behavior is questionable for certain behaviors, thus urging the need to develop accurate and comprehensive tools to accurately measure one's online behavior.

1.1 Questionnaires that measure the users Internet security

One of the first validated scientific instrument to measure the online risky behavior and information security awareness is the Users' Information Security Awareness Questionnaire (its Croatian abbreviation is UZRPKIS) developed and published in Croatia [13]. Thereupon, Security Behavior Intentions Scale (SeBIS) was developed in the USA [14] and a questionnaire called the Four Measurements Scales in Turkey [15]. A more comprehensive and very long questionnaire consisting of 21 subscales, entitled Human Aspects of Information Security (HAIS-Q), was developed in Australia [16]. However, the numerous shortcomings of these questionnaires were fullness criticized, mostly for being too long or containing too many questions, does not measure the users' actual behavior and being available only in Croatian language [17].

The first English versions of BCISQ were tested on German and Croatian students (in English) as shortened versions of previous long paper-pencil internet security questionnaires [18]. Based on this work, the same authors developed a short version of the questionnaire to measure the risky online behavior of information-communication system users in order to correct the shortcomings. A today's questionnaire consists of a 17 items and basic demographic data. BCISQ is the first to measure the level of the user online behavior. As it consists of an additional behavioral simulation scale, it can only be applied online [17,19]. The first version was validated on the English on Croatian students to generalize and compare data between the different countries [17]. The second BCISQ version was translated in Croatian and validated on a sample of Croatian students participating in a national research [19].

1.2 Slovenian BCISQ version

Slovenia and Croatia have a similar historical, cultural, educational, linguistic and economic background. According to the Eurostat data from 2019 [20], comparing the gross domestic product (GDP) per inhabitant in PPS (purchasing power standard), Croatia (GDP=66) is ranked ten places below Slovenia (GDP=87). However, according to the International Monetary Fund (IMF) [21] and the World Bank [22] who use the PPP (purchasing power parity) method for comparing living standards between countries (it takes into account the cost of living and the inflation rate, rather than a simpler comparison of nominal amounts that may not show real income differences), the data for 2020 show that Croatia (rank=83) is ranked 14 places above Slovenia (rank=97). Furthermore, both Croatia and Slovenia have the same average number of foreign languages learned per pupil in Upper Secondary Education (International Standard Classification of Education level 3), and about the same number of foreign students coming to host their institutions (through Erasmus programs) (Eurostat data for 2020 [20]).

Because of these similarities, it is assumed that a similar pattern of a risky online behavior and internet security awareness would be found among the Croatian and Slovenian students. The first translation of BCISQ in the Slovenian language and preliminary testing were done in 2019 [23]. To check for some basic psychometric characteristics of the Slovenian version of BCISQ two independent information security experts validated the translation. A Slovenian language lecturer checked the translation for grammatical errors. Preliminary results show a moderate internal consistency of the four subscales. However, validation in the Slovenian language has not yet been completed.

2 AIM OF OUR STUDY

The aim of our study is to cross-validate the translation of BCISQ into Slovenian language, and to test the questionnaire for psychometric properties among Slovenian students.

Because of the very similar historical, educational and economic situation in Croatia and Slovenia, it is assumed that the behavior of information-communication systems users will be similar and can thus be assessed in the same way. BCISQ was translated into the Slovenian language. It is therefore expected that testing the translated BCISQ

on Slovenian students will show equally good psychometric characteristics, i.e. similar construct validity and reliability as when testing the English and Croatian version on Croatian students.

3 METHOD

3.1 Participants

The participants in our study were students of the University of Primorska. 151 students filled-in BCISQ, 23.2 % of them were male and 76.8 % female. Their average age was M = 21.68 (SD = 3.12), with an age span from 18 to 42 years. Most of the students had an average technical knowledge about computers and Internet (76.8 %) and about the information security and data privacy (68.2 %) and some of them had previous training related to the security and privacy issues of Internet (35.8 %). The students were from different faculties and study programs: Biomedicine and health (55 %), Social Sciences (20.5 %), Interdisciplinary fields of science (4 %), Natural Sciences (7.3 %), Technical Sciences (12.6 %) and Arts (0.7 %).

3.2 Instrument

The Slovenian BCISQ version, containing also some general and demographical data was used (Figure 1). Its first part consists of two behavior scales to measure the information security, i.e., a potentially risky behavior of the computer user (risky behavior self-assessment (k =4; e.g. How often do you reveal the password of your e-mail account to others?) and risky behavior simulation (k=4; e.g. If you would like to receive notifications and our free promotion material, please leave your e-mail:_____)). Participants were asked to self-assess their online behavior on a 5-point Likert scale (from 0-never to 4-always). On behavior simulation scale, the participants were asked to leave some private data (0 – didn't leave any data, 4 – left the data on all four items).

The BSCISQ second part consists of two cognitive scales to measure the level of the user information security awareness (risk scale (k=5), e.g. How would you rate the risk of someone hacking your personal computer, laptop or smart phone?, and importance scale (k=4), e.g. How would you rate the importance of periodical changing of your passwords with new ones?). The participants were asked to self-assess their information security awareness on a 5-point Likert scale (from 0 - not important/no risk to 4 – extremely important/high risk).

For each scale the result represents an arithmetic mean of a specific items. The theoretical span result is the same for all four scales, ranging from 0 to 4. On the behavioral scales, higher results indicate a riskier behavior, but higher results indicate a higher level of the Internet security awareness on the cognitive scales.

3.3 Procedure

The data were collected during a students' regular class. Professors shared link for online BCISQ via e-mail, and the students were asked to fill-in BCISQ during their class. It took them some ten minutes.

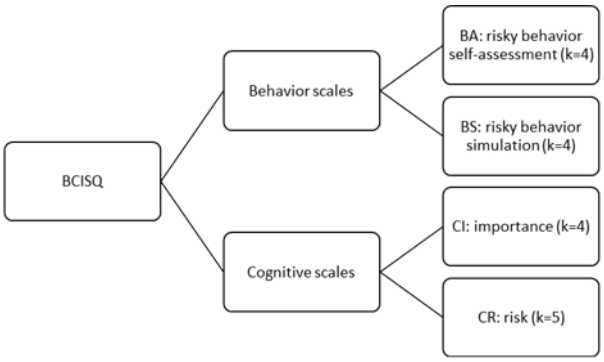

Figure 1. BCISQ scales with the number of items per scale

4 RESULTS & DISCUSSION

4.1 Data description

Descriptive statistics for each of the four BCISQ subscales are presented in Table 1. With the exception of the Risky behavior self-assessment subscale (BA), each of the subscales was within a satisfactory response range. The data for all four subscales were approximately normally distributed (the asymmetry index was less than +/- 4, and for the three subscales it was less than +/-1). A parametric statistics was therefore used to check the BCISQ construct validity and internal reliability. The average means of the Behavioral subscales indicate that all participants self-assessed themselves and show a low level of risky behavior while they were online, and the average means of the Cognitive subscales show that they had quite a high level of security awareness

Table 1. Descriptive statistics for the four BCISQ subscales.

Subscales of BCISQ	N	Min	Max	M	SD	S	K
BA: risky behavior self-assessment	151	0.00	2.00	0.33	0.39	1.55	2.52
BS: risky behavior simulation	151	0.00	4.00	1.31	1.17	0.48	-0.93
CI: importance	151	0.50	4.00	2.86	0.78	-0.67	0.23
CR: risk	151	0.40	4.00	2.60	0.99	-0.33	-0.87

Legend: Min – minimal value
Max – maximal value
M – mean
SD – standard deviation
S – Skewness asymmetry indices
K – Kurtosis asymmetry indices

4.2 Construct validity

Confirmatory factor analysis (CFA) was checked by using SEM. Results show excellent model fit indices (Table 2), even the chi square is non-significant [24]. Comparing to the English and Croatian language version

[17, 19], the Slovenian version shows a better model fit, i.e. construct validity.

Table 2. Model fit indices for the three language versions (Slovenian, English and Croatian) of BCISQ.

Model fit indices	Slovenian version (Slovenian students; N= 151)	English version (Croatian students; N=165) [17]	Croatian version (Croatian students; N=287) [19]
	Final Model (df=113)	Final Model (df=111)	Final Model (df=111)
$\chi 2$	113.868/113=1.01 n.s. (p=0.46)	159.707/111 = 1.43	198.691/111= 1.79
CFI	0.99	0.96	0.96
TLI	0.99	0.96	0.95
RMSEA	0.01	0.05	0.05

Legend: CFI - Comparative Fit Index, compares the fit of a target model to the fit of an independent, or null, model
TLI - Tucker Lewis Index, a relative reduction in misfit per degree of freedom
RMSEA - Root Mean Square Error of Approximation, an absolute measure of model fit based on the non-centrality parameter

All items prove to be good indicators for the assumed subscales (Figure 2). The construct validity is confirmed in accordance with our assumption about the similar historical, cultural, educational, linguistic and economic background of Croatia and Slovenia [20-22], showing that the Croatian and Slovenian students imply similar constructs in terms of the user online risky behavior and information security awareness.

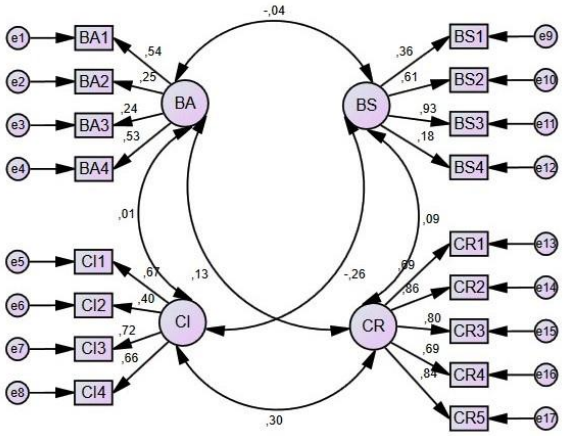

Figure 2. CFA model of BCISQ for the Slovenian version.

4.3 Reliability analysis

In order to check the internal consistency of each of the four BCISQ subscales, Cronbach's alpha is calculated (Table 3). Results show a rather poor reliability for the Behavioral subscales, especially for the Risky behavior self-assessment subscale. This is common in an early stage of a research, i.e. when new measurement instruments are tested [25]. Both Cognitive subscales show a good internal consistency.

Table 3. Reliability analysis of the three language versions (Slovenian, English and Croatian) of BCISQ.

Cronbach α / Subscales of BCISQ	Slovenian version (Slovenian students; N=151)	English version [17] (Croatian students; N=165)	Croatian version [19] (Croatian students; N=287)
BA: risky behavior self-assessment (k=4)	0.42	0.81	0.68
BS: risky behavior simulation (k=4)	0.53	0.68	0.66
CI: importance (k=4)	0.72	0.78	0.71
CR: risk (k=5)	0.88	0.93	0.93

An additional analysis was done to check for the possible reasons of the poor reliability of the Behavioral subscales (Table 4). For the Risky behavior self-assessment subscale (BA) there was no full range of responses obtained for any of the items. Over 90% of the participants indicated they had never or rarely behave a risky while online. The sensitivity of the subscale was violated.

Table 4. Analysis of the answers distribution for the Risky behavior self-assessment scale.

Items	% of answer 0 (never)	% of answer 1 (rarely)	Total %
BA1	64.9 %	29.1 %	94 %
BA2	72.2 %	23.8 %	96 %
BA3	78.1 %	16.6 %	94.7 %
BA4	81.5 %	11.9 %	93.4 %

For the Risky behavior simulation subscale (BS) one item shows an extremely poor reliability compromising the reliability of the whole scale. This is the item where participants were asked to leave their personal password for the e-mail. A possible reason for such poor reliability is that the students finally became aware of the need of saving the data privacy and did not leave their real password. Actually, some answers where "I won't", "I bet you would know", "No", although they stated that they did not leave their real password such answers were treated in the same way as the ones where participants left the question unanswered. However, we cannot say which passwords were real and which were fake.

Moreover, although the BS arithmetic mean (Table 1) shows a low level of the risky simulated online behavior, quite a high number of participant left their personal data. They wanted to be notified about a similar research (17.9 %) and about a free antivirus program by third party on e-mail (48.3%). Some left their personal e-mail (26.5 %) and password for e-mail (38.4%, after the obviously false ones were excluded). In 12.6 % cases they left both data, i.e. e-mail and password.

Comparing the Slovenian version with the English and Croatian version [17,19], shows a decrease in reliability in the Slovenian version. Between the English and Croatian version a slight decrease in the reliability,

especially for the Behavioral subscales is also noticed. One of the possible reasons is that the data for the English version collected in 2018 and for the Croatian version in 2019, both before the covid-19 pandemic and digitalization of educational process, especially for the college students. The data for the Slovenian version were collected in spring 2022, after the students had been spending last two years mostly online. This specific period of their lives is likely to have significantly affected their online activities. The huge increase in the time spent online, because their whole life had become mostly virtual, is believed to have raised their security awareness due to the process of learning through trial and error, with a direct consequence on their life [26].

Table 5. Test-retest reliability on Slovenian students (N=151).

Subscales of BCISQ	**ICC (95% Confidence Interval)**	**$F_{(df1,df2)}$**
BA: risky behavior self-assessment	0.415 (0.247–0.553)	$1.714_{(150,450)}$ *
BS: risky behavior simulation	0.501 (0.359–0.618)	$2.108_{(150,450)}$ *
CI: importance	0.669 (0.541–0.762)	$3.551_{(150,450)}$ *
CR: risk	0.878 (0.844–0.906)	$8.384_{(150,600)}$ *

*p<0.001

To check the intra-rater reliability (test-retest), the ICC is calculated for the four subscales. The test-retest reliability shows almost the same results as for the Cronbach's alpha. The Risky behavior self-assessment subscale shows a poor reliability, the Risky behavior simulation and Cognitive importance subscales show a moderate reliability, while the Cognitive risk subscale shows a good reliability [27].

4.4 Intercorrelation of the BCISQ subscales

Table 6. Pearson correlation coefficients between the BCISQ subscales (Slovenian version).

Subscales of BCISQ	BA	BS	CI	CR
BA: risky behavior self-assessment	1	0.006	-0.070	0.062
BS: risky behavior simulation	0.006	1	-0.155	0.048
CI: importance	-0.070	-0.155	1	0.198*
CR: risk	0.062	0.048	0.198*	1

*p<0.01

Our correlation analysis shows the same results as in the previous research [5,12,19]. First, a statistically positive and relatively low correlation is obtained between the two Cognitive subscales, i.e., between the assessment of the online risk awareness and the assessment of the importance of a safe use of the computers and Internet. As both subscales measure the same construct, i.e. the information awareness, the obtained results were expected. Second, for the Behavioral subscales, the results show a non-significant correlation between the self-assessment of the online risky behavior and the simulation of the actual online risky behavior. Again, results confirm that internet users do not reliably self-asses their online behavior and that it is necessary to measure their actual online behavior using different types of simulation [28].

5 CONCLUSION

Our conclusion is that the Slovenian version of BCISQ shows a good psychometric characteristic, i.e. excellent construct validity and relatively good reliability.

The main guidelines for future research are:

- the development of an additional simulation scale, including some other significant but not so obvious items about a person's private data, as this type of the simulation measures shows to be more reliable than self-assessment;
- in the BS subscale, the item about leaving the e-mail password should be replaced with a more suitable one;
- some significant item changes should be made in the BA subscales, e.g. the items about Facebook and Twitter or bank PIN should be replaced with the items about TikTok and Instagram;
- and, future study should use both measures of risky online behavior, i.e. self-assessed and simulated; as they neither correlate nor measure same construct.

REFERENCES

[1] T. Islam, I. Becker, R. Posner, M. Ekblom, M. McGuire, H. Borrion, S. Li, "A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems", in G. Wang, M.Z.A. Bhuiyan, S. De Capitani di Vimercati, Y. Ren (Eds.), Dependability in Sensor, Cloud, and Big Data Systems and Applications, *Communications in Computer and Information Science, 1123*, str. 277-293, 2019.

[2] S.J. Lukasik, "Protecting Users of the Cyber Commons", *Communications of the ACM, 54*, str. 54-61, September, 2011.

[3] H. Thompson, "The Human Element of Information Security", *IEEE Security&Privacy, 11*, str. 32-35, January-February 2013.

[4] J. Jeong, J. Mihelcic, G. Oliver, C. Rudolph, "Towards an improved understanding of human factors in cybersecurity", *Proceedings of the IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, str. 338-345, 2019.

[5] T. Velki, "Psychologists as information-communication system users: Is this bridge between information-communication and behavioral science enough to prevent risky online behaviors?", *Proceedings of the 45th International Convention on Information and Communication Technology, Electronics and Microelectronics*, str. 1196-2000, May 2022.

[6] K. Šolić, V. Ilakovac, A. Marušić and M. Marušić, "Trends in using insecure e-mail services in communication with journal editors", *6th Peer Review and Biomedical Publication, 33*(2), str. 50, 2009.

[7] A. N. Joinson, U. D. Reips, T. Buchanan and C. B. Paine Schofield, "Privacy, trust, and self-disclosure online", *Human–Computer Interaction, 25*, str. 1-24, 2010.

[8] S. Pötzsch, "Privacy awareness: a means to solve the privacy paradox?", in M. Vashek, S. Fischer-Hübner, D. Cvrček and P. Švenda, (Eds.), *The Future of Identity in the Information Society*, Berlin Heidelberg: Springer-Verlag, str. 226-236, 2009.

[9] S.C. Boerman, S. Kruikemeier, F.J. Zuiderveen Borgesius, "Exploring motivations for online privacy protection behaviour: insights from panel data", *Communication Research, 8*(7), str. 953-977, 2021.

[10] J. Hinds, E.J. Williams, A.N. Joinson, "It would not happen to me: privacy concerns and perspectives following the Cambridge analytica scandal", *International Journal of Human-Computer Studies, 143*, article 102498, 2020.

[11] L. Jaeger, A. Eckhardt, "Eyes wide open: the role of situational information security awareness for security-related behavior", *Information System Journal, 31*(3), str. 429-472, 2021.

[12] R. Wash, E. Rader, C. Fennell, "Can people self-report security accurately? Agreement between self-report and behavioural measures. Association for computing machinery", *Proceedings of the CHI Conference on Human Factors in Computing System*s, str. 2228-2232, 2017.

[13] T. Velki, K. Šolić and H. Očevčić, "Development of Users' Information Security Awareness Questionaire (UISAQ) - Ongoing Work", *Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics*, str. 1417-1421, May 2014.

[14] S. Egelman, M. Harbach, E. Péer, "Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)", *Proceedings of Annual ACM Conference on Human Factors in Computing Systems,* San Jose, California, USA, str. 7-12, May 2016.

[15] G. Öğütçü, Ö.M. Testik, O. Chouseinoglou, "Analysis of personal information security behavior and awareness", *Computers & Security, 56*, str. 83-93, 2016.

[16] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac and T. Zwaans., "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", Computers & Security, 66, str. 40-51, 2017.

[17] T. Velki and 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, 10*(1), str. 19-24, 2019.

[18] T. Velki, A. Mayer and J. Norget, "Development of a New International Behavioral-Cognitive Internet Security Questionnaire: Preliminary Results from Croatian and German samples", *Proceedings of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics*, str. 1410-1413, May 2019.

[19] T. Velki and K. Šolić "Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS)", *Policija i sigurnost, 29*(4), str. 341-355, 2020.

[20] Eurostat, online, https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en (24.4.2022).

[21] Monetary Fund (IMF), online, https://www.imf.org/en/Publications/WEO/weo-database/2022/April (27.4.2022).

[22] The World Bank, online, https://data.worldbank.org (19.4.2022).

[23] K. Šolić, T. Velki, P. Pucer and B. Žvanut "Translation and validation of the BCISQ onto Slovenian language - preliminary results", *Medicinska informatika*(14), str. 37, 2019.

[24] D. Hooper, J. Coughlan and M. Mullen, "Structural Equation Modelling: Guidelines for Determining Model Fit", *Journal of Business Research Methods, 6*(1), str. 53-60, 2008.

[25] J.C. Nunnally and I. H. Bernstein, I. H., Psychometric theory (3rd ed.), New York, NY: McGraw-Hill, 1994.

[26] M. J. A. Howe, Psihologija učenja, Jastrebarsko: Naklada Slap,2002.

[27] T. K. Koo and M. Y. LiA "Guideline of Selecting and Reporting Intraclass Correlation Coefficients for Reliability Research". *Journal of chiropractic medicine, 15*(2), str. 155–163, 2016.

[28] T. Velki and K. Šolić, Izazovi digitalnog svijeta, Osijek: Fakultet za odgojne i obrazovne znanosti Sveučilšta J.J. Strossmayera u Osijeku, 2019.

Tena Velki, PhD, works as an Associate Professor in the field of developmental psychology at the Faculty of Education in Osijek. She has received several rewards for her scientific work and promotion of applied psychology in Croatia. In the last 15 years, she has published over 60 scientific papers and nine books. She also hosts the Assistant Training Program for Children with Developmental Disabilities and a postgraduate specialist study in Inclusive Education. In the last ten years, her focus has also been on the area of information security, awareness, data privacy and risk behavior of computer users.

Krešimir Šolić, PhD works as an Assistant Professor at the Faculty of Medicine lecturing courses in biostatistics and medical informatics. His research interest is in information and communication security systems with a focus on the ICT systems' users behavior. He obtained his PhD degree in 2013 from the Faculty of Electrical Engineering of Osijek. The title of his thesis was "Model for Computer System Security Level Assessment Based On Ontology and Evidential Reasoning Algorithm". He is a member of the Croatian Biometric Society, Croatian Society for Medical Informatics (HBMD) and IEEE.

Boštjan Žvanut, PhD, is an Associate Professor at the Faculty of Health Science, University of Primorska, Izola, Slovenia, and a guest professor at the Josip Juraj Strossmayer University of Osijek, Medical Faculty, Croatia. He received his PhD degree from the Faculty of Computer and Information Sciences, University of Ljubljana, in 2009. His research interest is in healthcare information security, nursing informatics, business processes, e-learning and research methods. Currently, he is a national representative in the International Medical Informatics Association, Nursing Informatics interest group.