Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire

Šolić, Krešimir; Velki, Tena; Fosić, Igor; Vuković, Marin

Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire

Kresimir Solic

Josip Juraj Strossmayer University of Osijek, Faculty of Medicine Osijek, Josipa Huttlera 4, 31000 Osijek, Croatia, Kresimir@mefos.hr

Tena Velki

Josip Juraj Strossmayer University of Osijek, Faculty of Education Osijek, Cara Hadrijana 10, pp 330, 31000 Osijek, Croatia, tvelki@foozos.hr

Igor Fosic

HEP-Telekomunikacije, Martina Divalta 199, 31000 Osijek, Croatia, Igor.Fosic@hep.hr

Marin Vukovic

University of Zagreb, Faculty of Electrical Engineering and Computing, Unska 3, 10000 Zagreb, Croatia, Marin.Vukovic@fer.hr

Abstract: As technical security solutions are far from being enough to protect different kinds of information and communication systems, due to the human element, it was necessary to involve psychologists and define this problem as an interdisciplinary one. A validated questionnaire can be a good instrument for measuring users' information security awareness, knowledge on privacy issues and risk involved in online behavior, so conclusions gathered through empirical studies based on those kinds of questionnaires should be helpful in designing educative training programs. The aim of this paper was both to present the validated Behavioral-Cognitive Internet Security Questionnaire and prove its suitability for international usage as well as to present general conclusions regarding information and communication system users gathered through its development process. In this study, were included participants from 41 different countries, while English, Croatian, Slovenian and Hungarian language versions of questionnaire were used. Results have shown that developed questionnaire can be used internationally and the sum of the

conclusions is that users believe themselves to act more safely than they actually do; awareness has been rising over the years, but risk in online behavior has not been mitigated. Consequently, many users will still reveal their password, mostly under the influence of friendship or authority. Therefore, seeing as existing solutions are not good enough to resolve this global problem further studies should focus on developing some kind of an interactive platform that will be based on the results of empirical studies. It should not be based on restrictions, but rather on educational training, preferably personalized, and expanded with real-time warning solutions in order to keep up with constant changes in this field.

Keywords: ICT users; information security; security awareness; BCISQ questionnaire

1 Introduction

Nowadays there is finally a consensus among engineers and information security managers that technical security solutions are far from being enough to protect various ICT systems, due to the human element. This is because however good security procedures and hardware and software are, the impact of the user on the overall system security remains significant [1-4]. Once this problem was identified, it was necessary to include psychologists and define the problem as an interdisciplinary one [5], focusing on (miss) behavior and cross-cultural research with data collection and measurement issues [6].

Authors of this paper began their research into the users' impact back in 2009 [7, 8] and published their first validated questionnaire in 2014. The first published questionnaire was the UISAQ (Users' Information Security Awareness Questionnaire), which was validated in the Croatian language [9] and then translated into English [10] in order to reach a broader audience. After that first questionnaire, other scientifically validated security awareness (and risky online behavior, knowledge) questionnaires followed. The SeBIS (Security Behavior Intentions Scale) was developed in the USA and published in 2016 [11]. In the same year, the FMS (Four Measurements Scales) was designed and validated in Turkey [12]. The HAIS Q (Human Aspects of Information Security) was developed in Australia, with a validated version published in 2017 [13] and some preliminary results published earlier, in 2014 [14]. Further development of the UISAQ questionnaire ensued, based on an international, short and efficient version of the questionnaire. To the best of our knowledge, there are currently those four scientifically validated questionnaires for users' knowledge, (information security) awareness and online behavior examination. In scientific literature there have been many other attempts to test and partly measure online users' behavior regarding security and privacy issues, but through statistical process of validation, a questionnaire becomes a measurement instrument with defined reliability [15, 16]. So, it is of great importance to first undergo the

scientific validation process or to use other already validated questionnaires. Today's version of the Behavior Cognitive Information Security Questionnaire (BCISQ) presented in this paper has been validated in several languages, but primarily in English, and has been used internationally [17, 18].

The aim of this paper is both to present the validated BCISQ questionnaire and prove its suitability for international usage as well as to present general conclusions regarding online ICT system users' information security awareness, knowledge on privacy issues and risk of online behavior based on data gathered through its development process. The rest of the paper is organized as follows: next section describes the questionnaire, examinees and some properties of the statistical data analysis, then the following section presents a detailed theoretical background and history of the BCISQ's development. After results combined with discussion, the paper ends with the most important conclusions of this paper.

2 Overview of the Development of Constructs, Participants and Applied Data Analyses

The validated part of the BCISQ questionnaire comprises 17 items grouped into four scales, where two scales make a subgroup of the Behavioral Elements and two other scales make a subgroup of the Cognitive Elements. Under the Additional Questions there are two subgroups: Demographic Questions and Questions about Experience (Figure 1).

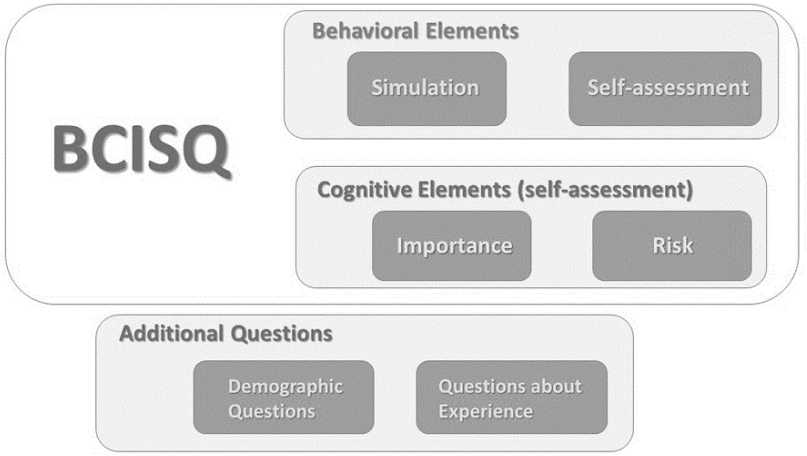

Figure 1
Schema of the BCISQ questionnaire

Demographic questions examine age, gender, level of education, field of expertise and current country of residence. Three questions examine the level of knowledge and experience regarding security and privacy on the Internet and two questions examine time spent online (Table 1).

Table 1
Questions regarding security, privacy and time spent online

Questions	Possible answers
Level of knowledge and experience regarding security and privacy	
How would you rate your knowledge about information security and privacy?	Poor/ Good/ Excellent
How would you rate your general technical knowledge about computers and the Internet?	Poor/ Good/ Excellent
Have you ever had some training or other experience(s) regarding security and privacy on the Internet?	Yes/ No
Consumption of time on the Internet	
How long have you been using the Internet?	A couple of years/ Half of life/ As long as I remember
On a daily basis, how often do you use Internet?	Less than 1 hour/ 2 to 3 hours daily/ 4 to 5 hours daily/ between 6 to 10 hours daily/ more than 10 hours daily

The 17 questions of the validated section referring to BS, BA, CI and CR are explained in the table (Table 2). Answers to the questions in the Behavioral Simulation scale are actually participant's action or lack of action in giving particular information, while answers to the questions in other three scales that are based on the self-assessment process represent scoring answers on the Likert scale from zero to four (Table 2).

In the Behavior Simulation scale participants can score up to 4 points (either based on answering Yes or filling in e-mail address or password), where a higher score means riskier behavior. In the Behavior Self-assessment scale each of the four questions has answers scored up to 4 points (answer Not very important gives zero, and answer Very important gives 4 points) and the arithmetic mean of those four answers gives the total score of the scale, where a higher score also means riskier behavior.

In the Cognitive Elements scale, subscale of Importance, each of the four questions has answers scored up to 4 points (answer Never gives zero, and answer Always gives 4 points) and the arithmetic mean of those four answers gives the total score of the scale, where a higher score means a higher level of awareness. While in the Cognitive Elements scale, subscale of Risk.

Table 2
List of items constructing each of the four scales of the BCISQ questionnaire

Items (questions)	Proposed answers
Behavior scale (BS): risky behavior Simulation	
Would you like to receive notifications from third-party partners about studies that investigate human behaviors, marketing, Internet security or other related topics?	Yes/ No
Would you like to receive free anti-virus software from third-party partners on your e-mail?	
If you would like to receive notifications and our free promotion material, please leave your e-mail:	*empty space for writing in (can be left empty)*
For checking the quality of your password security please write down your most used password:	
Behavior scale (BA): risky behavior Self-assessment (Frequency of your behavior:)	
How often do you lend your e-mail login and password to your friends or relatives?	Never/ Rarely/ Sometimes/ Often/ Always
How often do you lend your private debit or credit card(s) and associated PIN(s) to anyone?	
How often do you reveal your PIN (by non-concealment or saying it out loud) when you pay by card?	
How often do you reveal the password of your e-mail account to others?	
Cognitive scale (CI): Importance	
How would you rate the importance of maintaining protection of your computer equipment, laptop, smartphone (e.g. periodic updates of antispyware and antivirus software)?	Not very important/ Rather important/ Not sure/ Important/ Very important/
How would you rate the importance of logging off from different information systems when you finish your work (e.g. from social network, e-mail system, your laptop, etc.)?	
How would you rate the importance of checking removable media for viruses before usage?	
How would you rate the importance of periodical changing of your passwords with new ones, at least for frequently used services?	
Cognitive scale (CR): Risk	
How would you rate the risk of someone stealing your identity on the Internet (e-banking, Facebook, e-mail)?	Not very risky/ Somewhat risky/ Not sure/ Risky/ Very risky/
How would you rate the risk of someone stealing the money from your bank account when using mobile or Internet banking?	
How would you rate the risk of someone hacking your personal computer, laptop or smart phone?	
How would you rate the risk of losing your private photos and videos?	
How would you rate the risk of someone misusing your debit or credit card?	

Each of the five questions has answers scored up to 4 points (answer Not very risky gives zero, and answer Very risky gives 4 points) and the arithmetic mean of those five answers gives the total score of the scale, where a higher score means also a higher level of awareness. After submitting their answers, participants get a short explanation with some recommendations for more secure behavior on the Internet.

There were in total 960 examinees included in the study, with median age of 22 years (with interquartile range from 20 to 28, and total range from 18 to 72 years of age). More than two-thirds (71.2%) were female examinees and most were examined during year 2000 (42.6%). Most examinees were from Croatia (614, 64.0%) and Slovenia (192, 20.0%), then from Hungary (18, 1.9%), Czech Republic (15, 1.6%), Germany (12, 1.3%), Portugal (10, 1.0%) and USA (8, 0.8%). In total, the examinees were from 41 different countries around the globe.

Model fit has been analyzed during validation of different versions of the questionnaire, and it did turn out to be good, including the previous version in German [17]. As a result, in this analysis, answers to all translated versions were included [19, 20], in which context the English language version was considered the original version [21]. Moreover, participant groups overlapped because many examinees filled in the English version even though they had a version in their own language available.

Standard statistical methods were used for data analysis, specifically nonparametric Mann-Whitney U test for two and Kruskal-Wallis H test for three or more independent samples of numerical data. The significance level was set at 0.05 and all P values were two-tailed, while the snowball sampling method was used for data collection [16]. The online version that was used in this research is available on the following url: http://security.o-i.hr/.

3 Theoretical Background and History of Development

Earlier studies on the subject of ICT system users' awareness, online behavior and knowledge regarding information security issues mostly examined password quality and frequency of revealing passwords among users. Results showed that around 50% of the examined users reveal their passwords in some way [10, 11] while the proportion among children and adolescents is much higher, reaching approximately 77% [22]. With some simpler technical methods (e.g. dictionary attack) it is possible to break around 25% of used passwords [23-25] and more than 50% of the ICT system users prefer to use the same password for different systems [26]. On the other hand, 78% of ICT system users assess their information security skills as good [27].

When determining ICT system users' significant influence on the information security as an interdisciplinary problem, scientists integrated knowledge from behavioral and computer science fields. Maybe most important solutions existing nowadays for measuring that significant influence are statistically/scientifically validated questionnaires as measurement instruments. A validated questionnaire is a much more serious measurement instrument than a simple list of questions in a poll, because validity implies the degree to which a questionnaire actually measures what it is supposed to measure. A valid questionnaire, as any measurement instrument, involves a specific development procedure. The first step is establishing content validity, i.e. choosing items adequate for the problem intended for measurement. In other words, content validity reflects the experts' view of whether the questionnaire contains items which cover all aspects of the construct being measured. The second step is conducting a pilot study using a sample questionnaire, which is at least 5 to 8 times bigger than the initial questionnaire. The third step is a test of construct validity, done by using principal component analysis on underlying components that are being measured by questionnaire items. This way it is possible to identify items that have low factor loadings and should be removed. In step four, the goal is to analyze reliability using the Cronbach's Alpha test for internal consistency and remove items that violate overall reliability. In step five, a new study is conducted in order to check again for construct validity and reliability, confirm overall construct validity of the new questionnaire and additionally check for external validity. External validity shows the extent to which the results of a study can be generalized to and across other situations and people, i.e. age and gender differences [15, 28]. In order to test the BCISQ questionnaire internationally, the snowball sampling method for recruiting participants has been used. Existing subjects from different countries, authors' acquaintances and colleagues, provided referrals to recruit samples required for this research study [16].

To the best of the authors' knowledge, there are four validated questionnaires that have been developed for this purpose so far, even though there are many empirical studies trying to examine and measure ICT users' online behavior and their information security awareness and knowledge.

The Users' Information Security Awareness Questionnaire (UISAQ) was first developed and validated in the Croatian language and later translated into English language [10]. Validation was published in year 2015, with the final version consisting of 33 items grouped into two scales: Scale of Computer users' potentially risky behavior (k=17) and Scale of Information security knowledge (k=16). Both of the two scales are divided into three subscales, which makes six scales in total. The questionnaire has demographic questions and two control questions [9].

A year later, scientists from the USA developed and validated a questionnaire titled Security Behavior Intentions Scale (SeBIS) [11]. The SeBIS comprises 24

items and measures the computer security attitudes of end-users. It has four scales measuring awareness and relevant computer security behaviors.

The same year, scientists from Turkey developed a more elaborate questionnaire called the Four Measurements Scales (FMS). It has a total of 89 items measuring risky and conservative behavior, exposure to violation and risk perception of ICT system's users [12].

The Human Aspects of Information Security (HAIS Q) is the most recently validated questionnaire [13]. It was developed by Australian scientists and the final version comprises a total of 63 items. Those questions are grouped into seven large domains (password management, email use, Internet use, social media use, use of mobile devices, information management and reporting about incidents). Each of the seven domains is divided into 3 smaller domains (knowledge, attitudes and behavior), which in the end means that the questionnaire consists of 21 subscales.

Other related work is a study presenting development of an instrument that measures the security and privacy habits/practices of end users, specifically students. It seems that it is still in the development phase [29].

Some drawbacks of the existing questionnaires are as follows: the UISAQ has not been validated in the English language, all questionnaires have too many items/questions (except the SeBIS), they are based only on the self-assessment process and do not measure the level of actual behavior. All of those questionnaires were used only in their countries of origin, but not abroad or internationally.

All those drawbacks are confronted with the proposed new international questionnaire presented in this paper. The BCISQ has been developed and validated primarily in the English language, it has only 17 items/questions grouped into four scales, measures actual behavior with simulation and has very good statistical parameters [21]. In the development phases, the BCISQ questionnaire even had a version in German, while now it has validated versions in Croatian and Slovenian and an additional version in the Hungarian language. The BCISQ questionnaire was used abroad with intention to be used globally [17, 18].

Some general conclusions gathered so far measuring ICT users' knowledge, awareness and risk of their behavior are:

- Children with the average age of less than 8 are starting to use Internet in EU countries. They are the most vulnerable group of the Internet users [30, 31]
- Female users are slightly more cautious on the Internet [22, 32]
- In developing countries with both a large sample size and large age span, gender differences were not significant [9, 22, 33]

- Older and less experienced users are also more cautious and more careful when using Internet [31, 34]
- Electrical engineers (generally more technically experienced users) are unexpectedly less cautious and their behavior is riskier [22, 31, 35].
- Some users tend to note that privacy protection is important, but are behaving risky. This is also known as the privacy paradox [36-38].
- Over the last decade, users have generally shown higher knowledge (i.e. higher level of risk awareness), but behaved in a way that was riskier [35]
- We did not get any correlation between real and self-assessed risk behavior among ICT users [21].

Those conclusions listed above have been confirmed, but also expanded, by the results gained in this study. Results that are gained in this study are explained and discussed in the next section.

4 Questionnaire's Reliability and Current Results by Countries and Total Results

Perhaps the most interesting and most intriguing result was connected with revealing one's password. Almost half of the participants (439, 45.7%) seemed to have provided their real password. Although this field, which represented a trick question about the supposed examination of quality of the password could have been left unfilled, some participants provided passwords that were clearly fake, or wrote "I will not" or "I do not give my password," and those passwords were left out. But, if only half were the real passwords, they are still too many. From experience, it has been observed that in workshops or presentations dealing with this topic, students, but also colleagues, give away their passwords out of a sense of collegiality, trust or authority. Interestingly, in workshops where they received post-its and were asked to reveal their password, purportedly to check their strength, more than 70% of the participants revealed it. Also, during conferences, when the online version of the questionnaire was used and participants answered by mobile phones, again almost 70% provided their password [39]. As already indicated, these proportions are very high. However, it is not possible to verify with great certainty whether the answers are correct, because it is possible that the password provided could be false, outdated or changed immediately after the filling in of the questionnaire because the participants got some cautionary information and additional advice at the end of the questionnaire.

Also, this question regarding the password affects the reliability of the scale in the last validated version, the one in Slovenian. When this question is excluded, Cronbach's alpha improves significantly ($\alpha = 0.706$; Table 3). Consequently,

owing to the inability to verify the accuracy of the answers to this question, the plan is to substitute it by a new question in the next version of the questionnaire.

A part of this study applied in Slovenia has shown that users from that country exhibit somewhat worse behavior compared to other users (Kruskal-Wallis H test, $p = 0.002$), but they also give themselves worse scores in the self-assessment regarding the risk of their behavior (Kruskal-Wallis H test, $p < 0.001$). Nevertheless, the overall results of this study give no correlation between real and self-assessed risk behavior among ICT users (Table 6). There was no correlation between real and self-assessed risk behavior among ICT users in the previous study either [21]. This group of users (the Slovenian sample) is somewhat unusual, as they also reduce the Cronbach's alpha for those two scales, but the authors have not managed to identify the reason.

Overall mean values of scoring answers are not (yet) reference values for the BCISQ questionnaire, but in the future, once an upgraded version is made, with the unstable question regarding password eliminated, the authors plan to define normed reference values, as it was done for the earlier UISAQ questionnaire. However, those mean values can be used for comparison between some specific group of users and the sample of users analyzed in this study (Table 3).

It seems that ICT users using Unix OS, which represents mostly Android on mobile phones, give themselves better scores regarding risk in their behavior (Kruskal-Wallis H test, $p = 0.003$). However, they are not better in real behavior, so this may mean that they have an unjustified higher opinion of their online behavior (Table 3). Better self-assessment of risk in ICT users' online behavior does not have any correlation with any of the other three scales (Table 6).

When examining scores over the four-year period it is possible to conclude that ICT users were significantly more careful (Kruskal-Wallis H test, $p < 0.001$) during the period of the Covid-19 pandemic. Examinees self-assessed their online behavior better and better identified risky behavior presented in some risky online situations (Table 3). However, results collected during the first six months of 2022 are showing that there is no promising trend, especially not in ICT users' real online behavior (Table 3). One previous study did show increased knowledge and security awareness among middle aged ICT users, but also a tendency toward risky online behavior that increases with age [35].

Female users are significantly more cautious (Mann-Whitney U test, $p < 0.007$) than male ICT users (Table 4). This result is in line with previous studies [22, 31] However, in developing countries with both a large sample size and large age span, gender differences were not significant [33].

Table 3
Comparisons by versions and years

	BS‡	**p***	**BA‡**	**p***	**CI**	**p***	**CR**	**p***
Cronbach's Alpha per version for each scale								
English /n=159	0.615		0.725		0.791		0.901	
Croatian /n=594	0.685		0.640		0.729		0.925	
Slovenian /n=173	0.582†		0.396		0.727		0.880	
Hungarian /n=34	0.717		0.677		0.836		0.929	
Overall	**0.654**		**0.620**		**0.750**		**0.917**	
Mean (SD) values of scoring answers per version for each scale								
English /n=159	0.90 (1.11)	***0.002***	0.27 (0.42)	***<0.001***	2.81 (0.93)	**0.17**	2.16 (1.21)	***<0.001***
Croatian /n=594	1.12 (1.23)		0.22 (0.40)		2.99 (0.74)		2.81 (1.11)	
Slovenian /n=173	1.36 (1.23)		0.31 (0.37)		2.94 (0.77)		2.61 (0.99)	
Hngarian /n=34	0.88 (1.23)		0.26 (0.40)		2.71 (0.97)		2.64 (1.18)	
Overall /n=960	1.12 (1.22)		0.25 (0.40)		2.94 (0.79)		2.66 (1.13)	
Mean (SD) values of scoring answers regarding used OS when accessing questionnaire								
Unix /n=482	1.17 (1.25)	0.08	0.22 (0.37)	***0.003***	2.99 (0.76)	0.07	2.72 (1.08)	0.44
Windows /n=317	0.98 (1.14)		0.27 (0.46)		2.94 (0.78)		2.62 (1.14)	
Macintosh /n=161	1.21 (1.25)		0.29 (0.37)		2.81 (0.86)		2.57 (1.25)	
Differences in mean (SD) values of scoring answers regarding years								
2019 /n=202	1.18 (1.31)	0.54	0.27 (0.40)	***<0.001***	2.89 (0.85)	0.39	2.35 (1.11)	***<0.001***
2020 /n=409	1.03 (1.17)		0.22 (0.42)		3.00 (0.74)		2.80 (1.13)	
2021 /n=222	1.18 (1.21)		0.24 (0.39)		2.94 (0.79)		2.76 (1.13)	
2022 /n=127	1.18 (1.25)		0.32 (0.37)		2.86 (0.83)		2.54 (1.06)	

*Kruskal-Wallis H test; †after removing the question regarding the password, Cronbach's Alpha becomes much better (α=0.71); ‡lower mean values represent less risky behavior
Used abbreviations are BS: Behavior scale of Simulation, BA: Behavior scale of Self-assessment, CI: Cognitive scale of Importance, CR: Cognitive scale of Risk

Table 4
Comparison by demographic elements

	BS‡	**p***	**BA‡**	**p***	**CI**	**p***	**CR**	**p***
Differences in mean (SD) values of scoring answers regarding gender								
Male /n=276	1.01 (1.15)	0.11	0.23 (0.37)	0.69	2.84 (0.81)	***0.007***	2.35 (1.19)	***<0.001***
Female /n=684	1.16 (1.24)		0.25 (0.41)		2.98 (0.78)		2.79 (1.08)	
Differences in mean (SD) values of scoring answers regarding education								
Secondary school only /n=179	1.29 (1.27)	0.07	0.28 (0.47)	0.12	2.88 (0.79)	***0.003***	2.87 (1.07)	***<0.001***
High school /n=426	1.00 (1.12)		0.22 (0.39)		2.91 (0.77)		2.74 (1.16)	
Bachelor's degree (BSc) /n=136	1.23 (1.22)		0.27 (0.41)		3.08 (0.80)		2.52 (1.12)	
Master's degree (MSc) /n=164	1.16 (1.37)		0.25 (0.35)		3.07 (0.70)		2.46 (1.11)	
Postgraduate (PhD) /n=55	1.09 (1.25)		0.28 (0.35)		2.63 (1.02)		2.36 (0.98)	
Differences in mean (SD) values of scoring answers regarding participants' profile								
Students /n=670	1.10 (1.18)	0.84	0.24 (0.40)	0.11	2.95 (0.74)	0.51	2.75 (1.13)	***<0.001***
Others /n=290	1.14 (1.30)		0.27 (0.40)		2.92 (0.89)		2.46 (1.10)	
Differences in mean (SD) values of scoring answers regarding area of expertise								
Natural sciences /n=51	1.20 (1.22)	0.43	0.25 (0.43)	0.43	2.81 (0.87)	0.13	2.55 (1.13)	***0.03***
Technical /n=87	0.98 (1.16)		0.30 (0.41)		2.83 (0.86)		2.31 (1.17)	
Biomedicine and Health /n=407	1.14 (1.17)		0.22 (0.36)		2.98 (0.74)		2.75 (1.09)	
Biotechnical /n=7	0.57 (0.79)		0.14 (0.24)		3.18 (0.51)		2.86 (0.93)	
Social sciences /n=270	1.17 (1.28)		0.27 (0,43)		2.91 (0.77)		2.68 (1.14)	
Humanities /n=75	1.13 (1.36)		0.24 (0.41)		3.05 (0.78)		2.74 (1.18)	
Art /n=14	0.57 (0.76)		0.38 (0.56)		2.34 (1.20)		1.99 (1.21)	

Interdisciplinary /n=49	1.02 (1.25)		0.22 (0.38)		3.03 (0.90)		2.64 (1.15)	

*Mann-Whitney U test for two, and Kruskal-Wallis H test for more than two groups; ‡lower mean values represent less risky behavior
Used abbreviations are BS: Behavior scale of Simulation, BA: Behavior scale of Self-assessment, CI: Cognitive scale of Importance, CR: Cognitive scale of Risk

Regarding results there is a certain connection between education and awareness, but not between the level of education and risk involved in online behavior (Table 4). This result is in line with the results of a previous study which showed that more knowledgeable users behave more casually, with a higher level of risk when online. For example, electrical engineers, who are generally more technically experienced users, are unexpectedly less cautious and behave in a way that is riskier [22, 31, 35]. Generally, some users tend to note that privacy protection is important, but are behaving riskily, in line with the so-called privacy paradox phenomenon [36-38].

It also seems that students are more aware (Mann-Whitney U test, $p < 0.001$) of online risks (Table 4), but there is also low but significant negative correlation of awareness with age of the ICT user (Table 6), implying the reason for this result. Also, in some previous studies, older and less experienced users were also more cautious and more careful when online [31, 34].

Generally, ICT system users with higher level of knowledge about information security and privacy are significantly better in both real and self- assessed online behavior and have significantly higher awareness regarding the importance of behaving carefully while online (Kruskal-Wallis H test, $p < 0.007$). However, users that had some kind of training regarding security and privacy on the Internet are significantly better (Mann-Whitney U test, $p < 0.001$) only in terms of the awareness regarding the importance to behave carefully while online (Table 5). It seems that existing training programs only effect awareness of importance and are not enough to correct user behavior. Existing training programs require evaluation of their effectiveness and adaptation in order to transform new knowledge into practical behavior [41, 42]. Also, personalized user training programs can be one possible solution [43, 44]. Training programs are only part of the education process which should start as early as possible in a person's life [45], because children of no more than eight years of age are starting to use the Internet in EU countries. And the young are the most vulnerable group of ICT users [30].

Users that have excellent general technical knowledge about computers and Internet score their own behavior as better compared to others, to a statistically significant extent (Kruskal-Wallis H test, $p < 0.001$) (Table 5). They also have somewhat better scores regarding real behavior, which is in line with another empirical study on self-assessing information security skills [27].

Again, a more experienced ICT user is more nonchalant in the assessment of risky online situations, probably thinking that such a situation cannot happen to them (Table 5).

Table 5

Questions regarding security, privacy and f time spent online

	BS‡	**p***	**BA‡**	**p***	**CI**	**p***	**CR**	**p***
Differences in mean (SD) values of scoring answers regarding knowledge about information security and privacy issues								
Poor 154	1.33 (1.30)	***0.004***	0.33 (0.45)	***0.003***	2.73 (0.85)	***<0.001***	2.63 (1.09)	0.48
Good 667	1.12 (1.21)		0.24 (0.39)		2.94 (0.77)		2.70 (1.09)	
Excellent 139	0.88 (1.12)		0.19 (0.37)		3.19 (0.77)		2.52 (1.32)	
Differences in mean (SD) values of scoring answers regarding general technical knowledge about computers and the Internet								
Poor	1.19 (1.26)	0.52	0.36 (0.49)	***<0.001***	2.87 (0.89)	0.20	2.72 (1.09)	0.23
Good	1.12 (1.22)		0.24 (0.39)		2.94 (0.76)		2.69 (1.11)	
Excellent	1.04 (1.18)		0.19 (0.31)		3.01 (0.82)		2.50 (1.23)	
Differences in mean (SD) values of scoring answers regarding some training in security								
No 587	1.13 (1.19)	0.26	0.25 (0.40)	0.87	2.87 (0.80)	***<0.001***	2.67 (1.12)	0.99
Yes 373	1.10 (1.27)		0.24 (0.40)		3.05 (0.76)		2.65 (1.14)	
Differences in mean (SD) values of scoring answers regarding period of using Internet								
A couple of years /n=120	1.26 (1.29)	0.20	0.31 (0.55)	0.79	2.91 (0.88)	0.93	2.94 (1.01)	***<0.001***
Half of my life /n=655	1.13 (1.23)		0.24 (0.39)		2.95 (0.77)		2.68 (1.11)	
As long as I remember /n=185	0.97 (1.12)		0.21 (0.30)		2.92 (0.82)		2.41 (1.22)	
Differences in mean (SD) values of scoring answers regarding frequency of Internet usage								
Less than 1 hour /n=29	1.24 (1.41)	0.48	0.34 (0.55)	0.32	2.94 (0.92)	0.96	2.66 (1.19)	0.44
1 to 3 hours daily /n=243	1.18 (1.25)		0.25 (0.40)		2.97 (0.76)		2.72 (1.06)	
4 to 5 hours daily /n=370	1.15 (1.23)		0.26 (0.39)		2.94 (0.78)		2.70 (1.13)	
Between 6 and 10 /n=253	1.04 (1.18)		0.23 (0.42)		2.95 (0.78)		2.60 (1.18)	
More than	0.94		0.19		2.84		2.48	

10 hours /n=65	(1.10)		(0.33)		(0.92)		(1.14)	

*Mann-Whitney U test for two, and Kruskal-Wallis H test for more than two groups; ‡lower mean values represent less risky behavior
Used abbreviations are BS: Behavior scale of Simulation, BA: Behavior scale of Self-assessment, CI: Cognitive scale of Importance, CR: Cognitive scale of Risk

As already discussed earlier in this chapter, the main result of correlation analysis between each scale is that there is no correlation (rho = 0.036) between real and self-assessed risk involved in online behavior (between BS and BA, Table 6), as users think they behave more securely than they do (e.g. means of overall scoring values in Table 3). Even though there is statistically significant correlation for some pairs of the examined variables, the coefficient of correlation is very low and close to value zero (one is the highest correlation coefficient). There is low positive correlation (rho = 0.244) between the importance of online security and back up, including the rating of risky online situations (CI and CR scales), as these two scales basically measure two related elements of user' awareness (Table 6). There is also significant negative, but very small correlation (rho = -0.118) between users' age and users' rating of risky situations, possibly connected to knowledge about security issues, as older users have somewhat less experience in these situations (Table 6).

Table 6
Correlations between age and individual scale

Correlation between variables		**coefficient of correlation: rho**	**95% Confidence interval of rho**	**p***
Age	BS‡	-0.013	-0.076 to 0.050	0.68
	BA‡	0.044	-0.020 to 0.107	0.18
	CI	0.070	0.006 to 0.132	***0.03***
	CR	-0.118	-0.180 to -0.055	***<0.001***
BS‡	BA‡	0.036	-0.028 to 0.099	0.27
	CI	-0.018	-0.081 to 0.046	0.59
	CR	0.086	0.023 to 0.148	***0.008***
BA‡	CI	-0.135	-0.197 to -0.073	***<0.001***
	CR	-0.084	-0.146 to -0.021	***0.009***
CI	CR	0.244	0.184 to 0.303	***<0.001***

*Spearman's correlation test; ‡lower mean values represent less risky behavior
Used abbreviations are BS: Behavior scale of Simulation, BA: Behavior scale of Self-assessment, CI: Cognitive scale of Importance, CR: Cognitive scale of Risk

Conclusions

Results presented here show that previously validated BCISQ is a good measurement instrument and can be used worldwide to examine any particular group of users or to make comparisons among different groups in order to test differences between, for example, countries and cultures or to analyze employees

of a company or some government institution [21]. Previous research has shown how important it is to analyze ICT user behavior and their impact on overall security [6].

There have been several key conclusions so far. Specifically, there is no correlation between real and self-assessed behavior [21]. There is also significant, but surprisingly negative correlation between the level of knowledge and safe behavior [31, 35]. Moreover, risky behavior in real life is mirrored in the digital world, with women, for example, behaving more cautiously compared to men, both in digital and real world [22, 32]. Also, a higher level of knowledge and awareness does not imply less risky online behavior, and even though it seems that awareness has been rising over the years, riskiness of online behavior has not been improved [35]. More than two thirds of users will reveal their password, mostly under the influence of friendship or authority, and at the same time a similar percentage assess their information security skills as good.

Therefore, future studies should answer the question of how to educate the users, how to make them more cautious and how to increase their awareness of these highly important issues [36, 37]. Restrictions and controls over ICT system users should not be among the solutions for this major problem, on the other hand, education alone is clearly not enough. The scientific community, in cooperation with professionals from the real sector, the practitioners, should find models that could lead to some new solutions that will succeed in influencing risky user behavior by raising their awareness of this problem [39, 40].

Changes in the field of information security, in particular protection of privacy, are happening constantly and daily ("Change is the only constant in life"). Because of that, solutions regarding security awareness need to be adjusted frequently through time in order to improve usability and sustainability [41]. In this sense, by the time the process of validation of the questionnaire is completed, the final version becomes outdated very soon, requiring corrections.

The authors' main goal was to develop a global and short questionnaire that will measure both real and self-assessed behavior and the level of knowledge and awareness among all kinds of ICT users. But, much more challenging is to develop a model or a platform that will be of help to ICT users in terms of teaching them about online threats, to raise their awareness, and to inform about risky behavior in real-time, but not to restrict the users' use of Internet services.

One of the limitations of our study is that proposed BCISQ questionaire focuses on the general worldwide population, but does not include specific ICT users. Also, we had majority of examinees from Croatia and only several examinees from some of the 41 included country. In that way, although the sample size is relatively large (n = 960), it should be significantly larger in the future studies.

So regarding pointed limitations, potential future work could involve the use of the proposed BCISQ in different countries in order to examine differences

between cultures. Furthermore, some more detailed comparison between existing and new questionnaires could result in a new, better and more universal international questionnaire. Additionaly, focusing on specific groups of users would be a great benefit to development of new versions of this questionnaire. As the ICT field is rapidly growing and evolving, encompassing the rapid development of new technologies and applications, new research will require the inclusion of additional items in the questionnaire to cover the entire scope of applications. Certainly some self-educational solutions should be developed based on the mentioned questionnaires, like the one developed based on the UISAQ [46]. All future scientific efforts and educational attempts should focus on increasing information security awareness among ICT system users in order to reduce risky online activities.

Acknowledgement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] R Diesch, M Pfaff, H Krcmar. Prerequisite to Measure Information Security - A State of the Art Literature Review. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy. SCITEPRESS, 2018

[2] R von Solms, J van Niekerk. From information security to cyber security. Comput Secur, 38:97-102, 2013

[3] MA Sasse, S Brostoff, D Weirich. Transforming the “Weakest Link” - a Human/Computer Interaction Approach to Usable and Effective Security. BT Technol J, 19(3):122-131, 2001

[4] SJ Lukasik. Protecting users of the cyber commons. Commun ACM, 54(9):54-61, 2011

[5] K Solic, K Nenadic, D Galic. Empirical Study on the Correlation between User Awareness and Information Security. International Journal of Electrical and Computer Engineering, 3(2):47-51, 2012

[6] RE Crossler, et. al. Future directions for behavioral information security research. Comput Secur, 2013;32:90-101. 2013

[7] K Solic, K Grgic. Usage of Unsecured Free Web-based E-mail Services among Biomedical Researchers. In: Proceedings of the 31st International Conference on Information Technology Interfaces (ITI). Cavtat/Dubrovnik, Croatia: IEEE; 2009

[8] K Solic, V Ilakovac. Security Perception of a Portable PC User (The Difference Between Medical Doctors and Engineers): A Pilot Study. Med Glas, 6(2):261-264, 2009

[9] T Velki, K Solic, K Nenadic. Development and Validation of Users' Information Security Awareness Questionnaire (UISAQ) Psihologijske teme, 24(3):401-424, 2015

[10] T Velki, K Solic, H Ocevcic. Development of users' information security awareness questionnaire (UISAQ) - Ongoing work. In: Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija, Croatia: IEEE; 2014

[11] S Egelman, M Harbach, E Peer. Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS) In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM; 2016

[12] G Öğütçü, ÖM Testik, O Chouseinoglou. Analysis of personal information security behavior and awareness. Comput Secur, 56:83-93, 2016

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

[14] K Parsons, A McCormac, M Butavicius, M Pattinson, C Jerram. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) Comput Secur, 42:165-176, 2014

[15] MJG Yébenes Prous, FR Salvanés, LC Ortells. Validation of questionnaires. Reumatol Clín (Engl Ed), 5(4):171-177, 2009

[16] A Field. Discovering statistics using IBM SPSS statistics. 4th ed. London, England: SAGE Publications; 2013

[17] T Velki, A Mayer, J Norget. Development of a new international behavioral-cognitive internet security questionnaire: Preliminary results from Croatian and German samples. In: Proceedings of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija, Croatia: IEEE; 2019

[18] K Solic, T Velki, P Pucer, B Zvanut. Translation and validation of the BCISQ onto Slovenian language - preliminary results. In: Proceedings of the 14th Croatian Society for Medical Informatics Symposium (HDMI) Zagreb, Croatia; 2019

[19] T Velki, K Solic. Development of Social Engineering Research Tool on College Student Population: Behavioural Cognitive Internet Security Questionnaire (BCISQ) Polic. sigur, 29(4/2020):341-355, 2020

[20] T Velki, K Solic, B Zvanu. Cross-cultural validation and psychometric testing of the Slovenian version of the Behavioral-Cognitive Internet Security Questionnaire (BCISQ) Elektrotehniški Vestnik, 89(3):103-108, 2022

[21] T Velki, K Solic. Development and validation of a new measurement instrument: The Behavioral-Cognitive Internet Security Questionnaire (BCISQ). Int j electr comput eng syst, 10(1):19-24, 2019

[22] T Velki, K Solic, V Gorjanac, K Nenadic. Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. In: Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Opatija, Croatia: IEEE; 2017

[23] AG Voyiatzis, CA Fidas, DN Serpanos, NM Avouris. An empirical study on the web password strength in Greece. In: Proceedings of the 15th Panhellenic Conference on Informatics. USA: IEEE; 2011

[24] M Dell' Amico, P Michiardi, Y Roudier. Password strength: An empirical analysis. In: Proceedings of the IEEE INFOCOM. San Diego, California, USA: IEEE; 2010

[25] PG Kelley, et al. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In: Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, California, USA: IEEE, 2012

[26] K Solic, H Ocevcic, D Blazevic. Survey on password quality and confidentiality. Automatika, 56(1):69-75, 2015

[27] M Kyytsönen, J Ikonen, A-M Aalto, T Vehko. The self-assessed information security skills of the Finnish population: A regression analysis. Comput Secur, 118(102732), 2022

[28] H Taherdoost. Validity and reliability of the research instrument; How to test the validation of a questionnaire/survey in a research. SSRN Electron J, 5(3):28-36, 2016

[29] NF Khan, N Ikram. Development of students' security and privacy habits scale. In: Lecture Notes in Networks and Systems. Cham: Springer International Publishing, 951-963, 2020

[30] S Livingstone, L Haddon, A Görzig, K Ólafsson. Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. EU Kids Online Network, Lse.ac.uk. 2012

[31] K Solic, T Velki, T Galba. Empirical study on ICT system's users' risky behavior and security awareness. In: Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija, Croatia: IEEE; 2015

[32] M Sharples, R Graber, C Harrison, K Logan. E-safety and Web 2.0 for children aged 11-16. J Comput Assist Learn, 25(1):70-84, 2009

[33] EJ Helsper. Gendered Internet use across generations and life stages. Communic Res, 37(3):352-374, 2010

[34] K Solic, M Plesa, T Velki, K Nenadic. Awareness About Information Security and Privacy Among Healthcare Employees. SEEMEDJ, 3(1):21-28, 2019

[35] T Velki, K Romstein. User risky behavior and security awareness through lifespan. Int j electr comput eng syst, 9(2):53-63, 2019

[36] N Gerber, P Gerber, M Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Comput Secur, 77:226-261, 2018

[37] S Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput Secur, 64:122-134, 2017

[38] DP Snyman, H Kruger, WD Kearney. I shall, we shall, and all others will: paradoxical information security behaviour. Inf Comput Secur, 26(3):290-305, 2018

[39] T Velki. Psychologists as information-communication system users: Is this bridge between information-communication and behavioral science enough to prevent risky online behaviors? In: Proceedings of the 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO) Opatija, Croatia: IEEE; 2022

[40] T Velki, K Solic. Handbook for Information Security and Privacy. Faculty of Education, Josip Juraj Strossmayer University of Osijek, 2018

[41] S Chaudhary, V Gkioulos, S Katsikas, Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity, 8(1):1-19, 2022

[42] W He, Z Zhang. Enterprise cybersecurity training and awareness programs: Recommendations for success. J Organ Comput, 29(4):249-257, 2019

[43] D Fujs, S Vrhovec, D Vavpotic. Towards personalized user training for secure use of information Systems. int Arab j inf technol, 19(3):307-313, 2022

[44] H Aldawood, G Skinner. Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future internet, 11(3):73, 2019

[45] AA Al Shamsi. Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. International Journal of Information Technology and Language Studies, 3(2):8-29, 2019

[46] T Galba, K Solic, I Lukic. An information security and privacy self-assessment (ISPSA) tool for internet users. Acta Polytechnica Hungarica, 12(7):149-162, 2015