# Development and Validation of a New Measurement Instrument: The Behavioral Cognitive Internet Security Questionnaire (BCISQ)

**Velki, Tena; Šolić, Krešimir**

# Development and Validation of a New Measurement Instrument: The Behavioral-Cognitive Internet Security Questionnaire (BCISQ)

Original scientific paper

**Tena Velki**
J. J. Strossmayer University of Osijek,
Faculty of Education
Cara Hadrijana 10, Osijek, Croatia
tena.velki@gmail.com

**Krešimir Šolić**
J. J. Strossmayer University of Osijek,
Faculty of Medicine
Josipa Huttlera 4, Osijek, Croatia
kresimir.solic@mefos.hr

***Abstract*** *– Rapid changes in internet use and, consequently, digitalization of almost every aspect of human life lead inevitably to significant problems in information security and social engineering. As previous studies have shown, the biggest problem in internet security is the behavior of internet users. The aim of this study was to develop and validate a new and reliable instrument that would measure information security and awareness of every information-communication user in a short period of time. The development and validation of the new measurement instrument, the Behavioral-Cognitive Internet Security Questionnaire (BCISQ), was conducted in three phases. The final version consists of 4 subscales (2 behavioral and 2 cognitive) with a total of 17 items. The results revealed good psychometric characteristics of the BCISQ and showed that a short and reliable questionnaire measuring information security (i.e. behavioral aspects of internet security) and users' awareness (i.e. cognitive aspects of internet security) was successfully developed.*

***Keywords*** *– awareness, ICT user, information security, questionnaire, validation*

## 1. INTRODUCTION

Previous research on the topic of testing the behavior of ICT users in the Republic of Croatia preceded the development of a validated measurement instrument – the UISAQ, but such studies were quite rare among world scientists [1-4]. In the studies, the authors tried to point out the problem of system users as the weakest links within the system of information security and privacy protection [5].

In the last five years (2014), first in Croatia and later in three other countries, the first validated questionnaire was developed for the assessment of knowledge, risky behavior and awareness of dangers in the use of different ICT systems that are nowadays part of the internet. In the Republic of Croatia, the first version of the validated scientific measuring instrument *Users' Information Security Awareness Questionnaire* (in Croatian: UZRPKIS) [6] was developed. Information security in the questionnaire was assessed based on ICT users' risk behavior and knowledge. Risky behavior on the internet was operationalized as disobedience of the internet safety rules (e.g. revealing passwords and personal information, installation of unknown programs, opening and answering unknown emails, forwarding chain emails, not logging out of the system, etc.), whereas knowledge was operationalized as the awareness of possible risks while using information communication systems and the importance of obeying security protocols. In order to examine a wide range of users' potentially risky behaviors that can significantly affect the total security level of different information communication systems, it was essential to develop a reliable measuring instrument which would measure the level of awareness of information communication users in relation to security issues. It consisted of a total of 33 items grouped into 6 subscales measuring usual computer users' risk behaviors, maintenance of personal computer systems,

lending of access data to others, data security, security in online communication and backup quality. This questionnaire was used in further research on different national samples in order to test the level of internet security among online users in Croatia [7-9].

### 1.1. RELATED WORK

One year after the development of the UISAQ, scientists from the USA developed a questionnaire entitled *Security Behavior Intentions Scale* (SeBIS) [10]. In the same year, scientists from Turkey developed a more elaborate questionnaire called the *Four Measurements Scales*, which measures risk behaviors conservatively, exposure to violation and risk perception of ICT users [11]. The most recently validated questionnaire *Human Aspects of Information Security* (HAIS-Q) was developed by scientists from Australia [12]. The HAIS-Q is divided into seven large domains (password management, email use, internet use, social media use, use of mobile devices, information management and reporting about incidents), and each domain is divided into 3 smaller domains (knowledge, attitudes and behavior), which in the end means that the questionnaire consists of 21 subscales.

### 1.2. DISADVANTAGES OF THE EXISTING SOLUTIONS

The development of the questionnaire in 2014 [6], its use, and particularly international recognition of the work and citing in other countries, led to the need to develop a new measuring instrument that would be universal and international. Another reason was the fact that the UISAQ as well as other aforementioned validated questionnaires were criticized by researchers from the USA, Turkey and Australia.

The main disadvantage of the existing measurement instruments was their length. The UISAQ [6] has 33 items, whereas the HAIS-Q [12] has 63 items, and the Four Measurements Scales [11] has as many as 89 items. The problem with most of the research is the fact that ICT system users lack motivation and focus when giving answers to a great number of questions, which is why data collected in that way are not completely reliable, thus giving a distorted image of the human component in terms of information communication security. For both the government and the public sector, it is extremely important to have reliable and validated instruments that can provide a quick risk behavior assessment of ICT system users, considering the fact that the government and the public sector are in charge of a huge number of personal and therefore sensitive data. Scientists require measurement instruments which will enable collection of reliable data for generalization and comparison between various populations. Another drawback that only concerns the UISAQ was its publication in the Croatian language, so the problem was the impossibility of international use and data comparison. Generally, the drawbacks mentioned above can be summarized as follows:

- The questionnaires are too long and contain too many questions, which makes one feel tired.
- They are based only on self-assessment, which can be distorted, particularly due to giving socially desirable answers.
- They do not measure the level of actual behavior.
- Due to the use of different methodologies in various studies, it is impossible to make generalizations about the obtained results, i.e. a comparison of data between different countries is not possible.

The main goal of the current study was to develop and validate a new measurement instrument based on the previous version of the UISAQ [6, 13] and the initial version of the *Behavioral-cognitive internet security questionnaire* (BCISQ) [14] in order to be able to collect reliable data in a short time. For testing model fit for all versions of the BCISQ, packages lavaan [15] and lavaanGUI [16] in R [17] were used. Factor analysis (principal component analysis with oblimin rotation) was used to confirm a four-factor structure of the BCISQ, and reliability analysis was used for testing internal consistency, in the IBM SPSS Statistics 24.0 software.

The next section explains the methodology and the procedure used by the authors to validate the questionnaire. Then there follows a section with results and explanations, while the conclusion and future work are given in the last section.

## 2. METHOD

### 2.1. SAMPLE

The first sample

The participants were students from Croatia (N=250), from J.J. Strossmayer University of Osijek. There were a total of 45.6% male and 54.4% female participants. The average student age was 20.58 +/- 1.39 (arithmetic mean +/- SD). Furthermore, 225 young adults from Germany participated in the study, 25.7% of whom were men and 74.3% women. The average age of German adults was 27.48 +/- 12.20 (arithmetic mean +/- SD).

The second sample

The participants were students from Croatia (N=174) from J.J. Strossmayer University of Osijek, 32.2% of whom were male and 67.8% female. 61.5% of students were between 18 and 20 years old, whereas 38.5% of them were between 20 and 25 years old.

The third sample

The participants were students from Croatia (N=165) from J.J. Strossmayer University of Osijek, 23.5% and 76.5% of whom were male and female, respectively. 34.7% of students were between 18 and 20 years old,

61.2% were between 20 and 25 years old, and others (4.1%) were between 26 and 40 years old.

### 2.2. INSTRUMENT AND PROCEDURE

For the purpose of research and based on previous work of authors on the creation of various versions of the UISAQ [6, 13] and the *BCISQ* on the German and Croatian sample [14], the authors designed a new international instrument in English - the *Behavioral-cognitive internet security questionnaire*. The first part of the BCISQ consisted of 2 behavior scales measuring information security, i.e. computer user potentially risky behavior (risky behavior self-assessment (k=4) and risky behavior simulation (k=4)). The second part of the BCISQ consisted of 2 cognitive scales, which measured the level of user information security awareness (risk (k=5) and importance (k=4) scales).

**Table 1.** Model fit indices for initial and final models with referent values[1]

| Model fit indices | First sample (Croatian students N=250, German young adults N=225) | | Second sample (Croatian students N=174) | | Third sample (Croatian students N=165) | Reference values | |
|---|---|---|---|---|---|---|---|
| | Final Croatian model (df=32) | Final German model (df=32) | Basic model (df=131) | Final model after corrections (df=115) | Final model (df=111) | Good fit | Adequate fit |
| $\chi^2$ | 46.61/32 = 1.45 (n.s.) | 51.44/32 = 1.61 | 234.92/131 = 1.79 | 216.10/115 = 1.87 | 159.707111 = 1.43 | p > 0.01 (n.s.) | $\chi^2$ / df ≤ 2 |
| CFI | 0.97 | 0.93 | 0.93 | 0.94 | 0.96 | ≥ 0.95 | ≥ 0.90 |
| TLI | 0.96 | 0.90 | 0.92 | 0.93 | 0.96 | ≥ 0.95 | ≥ 0.90 |
| RMSEA | 0.04 | 0.05 | 0.07 | 0.07 | 0.05 | ≤ 0.06 | ≤ 0.08 |
| SRMR | 0.04 | 0.05 | 0.20 | 0.20 | 0.05 | ≤ 0.08 | ≤ 0.10 |

[1] http://davidakenny.net/cm/fit.hm

During the last academic year (2018/2019), Croatian students and German young adults were required to voluntarily give some general demographic data (age and gender) online and to fill out the new *Behavioral-cognitive internet security questionnaire*. Different student samples were tested at different time points, after every modification of the BCISQ.

Although a validated questionnaire as a measurement instrument is usually used as a paper-and-pencil method, for the BCISQ it was necessary to use an online method. The first scale of the BCISQ is a simulation scale that examines real online behavior by its simulation. There are many open-access software solutions for constructing an online questionnaire and in this paper, a BCISQ survey is based on the Joomla 3.x open source platform. The basic components of this Joomla instance are as follows:

- Linux CentOS,
- PHP 7.0.33,
- MySQL database 5.5.60, and
- Apache web server 2.4.6.

An additional component used as a Joomla extension is a free version of BreezingForms. Responsive web design has made it possible for the site to work across all platforms like mobile, tablet or PC, irrespective of the operating system used. Survey results are archived in the database and can be exported as files in .csv (comma-separated values) format.

The BCISQ is available online at: http://security.o-i.hr.

## 3. RESULTS AND DISCUSSION

For the purpose of developing the BCISQ, appropriate questions measuring (1) information security (i.e. potentially risky behavior) and (2) security awareness (i.e. evaluation of risk and importance of some online risky behavior) were chosen from several versions of the UISAQ [6, 13] and tested first on the Croatian and German sample (the first sample in Table 1). For both models, results have shown good model fit, which confirmed satisfactory design of the new instrument (Table 1). When compared to the German sample, model fit was slightly better for the Croatian sample.

In order to improve model fit additional analysis was done. For the cognitive scale, results showed a high covariance between measurement errors of the last two items (r = 0.67, the modification index for error covariance = 110.54 for the Croatian sample; r = 0.47, the modification index for error covariance = 39.51 for the German sample). In order to improve the exiting model, a cognitive subscale, which is a measure of security awareness, was divided into two subscales: risk and importance (for details, see [14]).

**Table 2.** Reliability analysis

| Cronbach α | Second sample (Croatian students N=174) | | Third sample (Croatian students N=165) |
|---|---|---|---|
| | Basic model (k=20) | Final model after corrections (k=17) | Final model (k=17) |
| Behavior scale (BA): risky behavior self-assessment (k=5 for basic model only, k=4 for final model) | 0.75 | 0.79 | 0.81 |
| Behavior scale (BS): risky behavior simulation (k=5 for basic model only, k=4 for final model) | 0.63 | 0.71 | 0.68 |
| Cognitive scale (CI): importance (k=4 for final model) | 0.82 | 0.82 | 0.78 |
| Cognitive scale (CR): risk (k=6 for basic model only, k=5 for final model) | 0.90 | 0.93 | 0.93 |

**Table 3.** Factor analysis (principal component analysis with oblimin rotation)

| Item | Factor loadings for the second sample after corrections (Croatian students N=174) | | | | Factor loadings for the third sample (Croatian students N=165) | | | |
|---|---|---|---|---|---|---|---|---|
| | Factor 1 | Factor 2 | Factor 3 | Factor 4 | Factor 1 | Factor 2 | Factor 3 | Factor 4 |
| behavior self-assessment BA1 | | .730 | | | | .802 | | |
| behavior self-assessment BA2 | | .871 | | | | .817 | | |
| behavior self-assessment BA3 | | .688 | | | | .743 | | |
| behavior self-assessment BA4 | | .814 | | | | .833 | | |
| behavior simulation BS1 | | | | .739 | | | .850 | |
| behavior simulation BS2 | | | | .850 | | | .850 | |
| behavior simulation BS3 | | | | .848 | | | .818 | |
| behavior simulation BS4 | | | | .433 | | | .374 | |
| cognitive importance CI1 | | | .770 | | | | | .788 |
| cognitive importance CI2 | | | .729 | | | | | .749 |
| cognitive importance CI3 | | | .826 | | | | | .834 |
| cognitive importance CI4 | | | .727 | | | | | .700 |
| cognitive risk CR1 | .870 | | | | | .873 | | |
| cognitive risk CR2 | .888 | | | | | .898 | | |
| cognitive risk CR3 | .878 | | | | | .909 | | |
| cognitive risk CR4 | .794 | | | | | .800 | | |
| cognitive risk CR5 | .895 | | | | | .910 | | |
| **Eigenvalue** | **3.97** | **2.77** | **2.63** | **2.30** | **4.11** | **2.73** | **2.16** | **1.76** |
| **Explained variance (%)** | **22.05** | **15.41** | **14.60** | **12.78** | **26.22** | **16.78** | **12.71** | **10.37** |

For testing data on the second sample a third subscale (measuring the evaluation of risk) of the BCISQ was developed because only two questions are insufficient to make an entire subscale (for a new scale k=6). Furthermore, a new scale simulating real online behavior was developed (k=5) resulting in a total of 20 items of the new questionnaire. After reliability analysis (Table 2), three items were deleted due to low internal consistency (small Cronbach's alpha). Factor analysis, type principal component analysis (with oblimin rotation) confirmed the BCISQ structure of four stable factors (Table 3) and hence the model fit indices (Table 1).

The final version of the BCISQ (k=17 items, 4 scales) was tested on the third sample. Reliability analysis (Table 2) showed good internal consistency and principal component analysis (the oblimin rotation method) confirmed the BCISQ structure (Table 3) and hence the model fit indices (Table 1).

For the second and the third sample, factor analysis showed a significant amount of explained variance (Table 2). A total of 64.85% and 66.08% variance were explained in the second and the third sample, respectively. Each factor explained between approximately 10% and 26% of variance, meaning that each one was equally important in the explanation of internet security and data privacy issues. With only a small number of items (4 or 5 per scale), variation in user risky online behavior and security awareness was almost entirely explained.

Good psychometric characteristics (internal consistency $\alpha > 0.66$, factor loadings > 0.3 for specific factor and good fit indices) showed that the new questionnaire was successfully developed.

Overall, the BCISQ showed to be a stable and reliable instrument measuring two main aspects of internet security (user behavior, i.e. information security and user cognition, i.e. security awareness).

## 4. CONCLUSION

In general, it can be concluded that a newly developed measurement instrument, Behavioral-Cognitive Internet Security Questionnaire (BCISQ), has good psychometric characteristics, i.e. it is reliable, with a clear factor structure consisting of 4 subscales, and with good model fit indices. In comparison to previous well-known questionnaires [6, 11-12], the BCISQ is notably shorter and the only instrument which has a simulation scale measuring real risky behavior of online users (not only user self-assessment).

Future studies should try to test the BCISQ in different cultural settings and among different age groups (children, adults) in order to verify reliability and stability of the factor structure of the new measurement instrument. Furthermore, future research should try to examine potential risk factors (characteristics of ICT users) of online risky behavior and information security problems in order to develop target prevention programs for users engaged in a risky online behavior.

An additional plan for future work is to develop a self-assessment software solution based on the BCISQ. The idea is that a software solution could offer feedback to a user referring to his/her results in comparison to a specific age group. When a user fills out an online questionnaire, software would produce his/her current results graphically according to reference values and guidelines. Some short guidelines on safer internet use would also be included in the final version of a software solution.

## 5. REFERENCES:


[1] K. Solic, V. Ilakovac, "Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study", Medicinski glasnik Dobojsko-tuzlanskog kantona, Vol. 6, No. 2, 2009, pp. 261-264.

[2] K. Šolić, F. Jović, D. Blažević, "An Approach to the Assessment of Potentially Risky Behavior of ICT System's Users", Technical Gazette, Vol. 20, No. 2, 2013, pp. 335-342.

[3] K. Šolić, K. Nenadić, D. Galić, "Empirical Study on the Correlation between User Awareness and Information Security", International Journal of Electrical and Computer Engineering Systems, Vol. 3, No. 2, 2012, pp. 47-51.

[4] K. Šolić, B. Tovjanin, V. Ilakovac, "Assessment methodology for the categorization of ICT system users' security awareness", Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 21-25 May 2012, pp. 1560-1564.

[5] M. A. Sasse, S. Brostoffand, D. Weirich, "Transforming the 'weakest link' - a human/ computer interaction approach to usable and effective security", BT Technology Journal, Vol. 19, No. 3, 2001, pp. 122-131.

[6] T. Velki, K. Šolić, H. Očevčić, "Development of User's Information Security Awareness Questionnaire (UISAQ) – Ongoing Work", Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 26-30 May 2014, pp. 1564-1568.

[7] T. Velki, K. Romstein, "User Risky Behavior and Security Awareness through Lifespan", International Journal of Electrical and Computer Engineering Systems, Vol. 9, No. 2, 2019, pp. 9-16.

[8] K. Šolić, T. Velki, T. Galba, "Empirical Study on ICT System's User's Risky Behavior and Security Awareness", Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 25-29 May 2015, pp. 1623-1626.

[9] T. Velki, K. Šolić, V. Gorjanac, K. Nenadić, "Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results", Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 22-26 May 2017, pp. 1496-1500.

[10] 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, 7-12 May 2016, pp. 7-12.

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

[12] K. Parsons et al., "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", Computers & Security, Vol. 66, 2017, pp. 40-51.

[13] T. Velki, K. Šolić, K. Nenadić, "Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS)", Psihologijske teme, Vol. 24, No. 3, 2015, pp. 401-424.

[14] T. Velki, A. Mayer, 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, Opatija, Croatia, 20-24 May 2019, pp. 1410-1413.

[15] Y. Rosseel, "lavaan: An R Package for Structural Equation Modeling", Journal of Statistical Software, Vol. 48, No. 2, 2012, pp. 1-36.

[16] A. Mayer, lavaanGUI: Graphical User Interface for lavaan. R package version 0.1-1.004, https://github.com/amayer2010/lavaanGUI (accessed: 2018)

[17] R Development Core Team, R: A language and environment for statistical computing, http://www.R-project.org (accessed: 2018)