Development of a New International Behavioral-Cognitive Internet Security Questionnaire: Preliminary Results from Croatian and German samples

Velki, Tena; Mayer, Axel; Norget, Julia

Source / Izvornik: **MIPRO 2019. Proceedings, 2019, 1410 - 1413**

Conference paper / Rad u zborniku

Publication status / Verzija rada: **Published version / Objavljena verzija rada (izdavačev PDF)**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:141:470784

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**



Repository / Repozitorij:

FOOZOS Repository - Repository of the Faculty of Education





Development of a New International *Behavioral-Cognitive Internet Security Questionnaire*: Preliminary Results from Croatian and German samples

T. Velki*, A. Mayer ** & J. Norget**
* J.J. Strossmayer University of Osijek, Faculty of Education, Osijek, Croatia
** RWTH Aachen University, Faculty of Arts and Humanities, Institute of Psychology, Aachen, Germany
tena.velki@gmail.com, axel.mayer@psych.rwth-aachen.de, julia.norget@rwth-aachen.de

***Abstract* - This study is based on previous results obtained with the validated Users' Information Security Awareness Questionnaire (UISAQ) and its main critiques concerning length and international usage. The aim was to develop a new international short version of the UISAQ, Behavioral-cognitive internet security questionnaire (BCISQ, Velki & Šolić, 2018). Authors gathered information on risky behavior and security awareness among 250 Croatian students and 225 German adults using the same instrument translated to German. The BCISQ consisted of 2 subscales with a total of 10 items. Model fit for both groups (Croatian and German) was tested using the Software program R. For both groups, the analyses did not confirm a two-factor structure. Due to large covariances between the measurement errors of the last two questions on the cognitive scale it is recommended to split this scale into two separate subscales, risk and importance. The resulting three-factor model shows a good fit for the Croatian (CFI=0.97, TLI=0.96, RMSEA=0.04, SRMR=0.04, χ^2=46.61) and the German sample (CFI=0.93, TLI=0.90, RMSEA=0.05, SRMR=0.05, χ^2=51.44). Future studies should try to further develop the third subscale (risk) of the BCISQ as well as to test the BCISQ in other cultures and languages.**

Key words – information security, international questionnaire, risky online behavior

I. INTRODUCTION

Today, in the digital age, information security and data privacy emerge as important issues in different areas of human life (e.g. security with online bank accounts, medical documentations, students' e-transcript and other online private data). While there is more and better security software available (antivirus, spam-filters, encryption, etc.), the user still remains the weakest link in online security [1]. The first scientific studies on this matter mostly focused only on examining password usage and password quality and strength [2-7]. But the problem regarding password security represents only a small portion of human online risky behavior. Further studies have used different methodological approaches to examine security awareness, to test the relationship between information security awareness and information security threats, to examine the extent of social engineering or to give recommendations for safer internet use [8-15], but still did not cover the whole range of human online behavior.

A. Development of information security questionnaires

In order to examine a wide range of users' potentially risky behavior when using different information and communication systems, it was necessary to develop a very general, but reliable and validated questionnaire which measures information systems users' awareness on security matters. The first validated scientific measurement instrument on this issue was the Users' Information Security Awareness Questionnaire (UISAQ), which was developed five years ago in Croatia [16,17] and later the same authors used this new instrument in order to do systematic research on information security awareness on a Croatian population [18,19]. The UISAQ consists of two parts: the first part measures users' potentially risky behavior, and the second part measures the level of user's information security knowledge and awareness. The questionnaire has 6 sub-areas that measure: usual risky behavior, personal computer maintenance, borrowing access data, knowledge and awareness, security in communications, secured data and backup quality. Later, only few other scientists have developed similar instruments. Turkish scientists developed their Four Measurements Scales [20] measuring risky behavior, conservative behavior, exposure to offence and risk perception. Australian scientists [21] have followed with the Human Aspects of Information Security Questionnaire (HAIS-Q). The HAIS-Q measures seven focus areas: password management, email use, internet use, social media use, mobile devices, information handling and incident reporting. Each focus area is further divided into three specific sub-areas, knowledge, attitude and behavior, resulting in 21 areas of interest.

The main critiques of the developed and validated instruments primarily concerned their length. The UISAQ consists of 33 items, the HAIS-Q of 63 items, and the Four Measurements Scales even has 89 items. Questionnaires that take a long time to complete can be inconvenient for academic and non-academic studies, because the participants could not keep their interest in so

many questions, sometimes giving false answers without even reading the questions. Especially for the public sector and the governments it would be useful to have a short, reliable and validated instrument that can quickly assess the problem of security awareness and provide data that can be generalized and compared between different populations. Another issue of the UISAQ was that it was only available in Croatian language, making international usage and comparison of data impossible.

B. Study aim

The aim of this study was to develop a new international short questionnaire, based on the previous version of the UISAQ [16,17] in order to provide an international validated instrument that could gather reliable data in a short time. For the new questionnaire, the most reliable items were selected from the UISAQ. Firstly, the selected items were translated into English and tested. After initial testing, the 10 most reliable items were tested again in English and after that translated into German. Model fit for both versions of the questionnaire (English and German) was tested using the packages lavaan [22] and lavaanGUI [23] in R [24].

II. METHOD

A. Participants

The participants in this study were Croatian students (N=250) from the J.J. Strossmayer University of Osijek. 45.6% of the participants were male and 54.4% female. The average age of the student participants was 20.58 +/- 1.39 (arithmetic mean +/- SD). In addition, 225 young adult Germans participated in the study, with a proportion of 25.7% of men and 74.3% of women. The average age of young adult participants was 27.48 +/- 12.20 (arithmetic mean +/- SD).

B. Procedure

During the winter semester Croatian students were asked to voluntarily provide some general demographic information (age and gender) online and to fill out the new *Behavioral-cognitive internet security questionnaire* (BCISQ, Velki & Šolić, 2018) in the English language. Later during the semester, German participants were recruited online to answer the same questionnaire, which had been translated into German.

C. Instruments

For the purpose of this research the authors created a new international instrument *Behavioral-cognitive internet security questionnaire* (BCISQ, Velki & Šolić, 2018) in English and German, which is based on previous research on the development of different versions of the UISAQ [16-19]. The first part of the BCISQ consisted of 4 items measuring computer users' potentially risky behavior (Behavior scale, Cronbach $\alpha_{(\text{English version})} = 0.71$; Cronbach $\alpha_{(\text{German version})} = 0.62$)). The second part of the questionnaire consisted of 6 questions measuring the level of users' information security awareness (Cognitive scale, Cronbach $\alpha_{(\text{English version})} = 0.72$; Cronbach $\alpha_{(\text{German version})} = 0.63$).

III. RESULTS

For the development of the BCISQ suitable items to assess (1) potentially risky behavior and (2) information security awareness (i.e. judgments of risk and importance of some potentially risky online behavior) were selected from different version of the UISAQ [16-19].

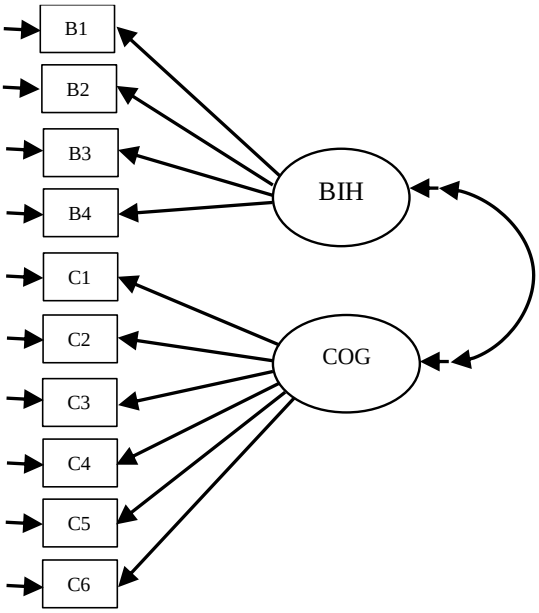


Figure 1. Theoretical model for both versions of the BCISQ (English and German)

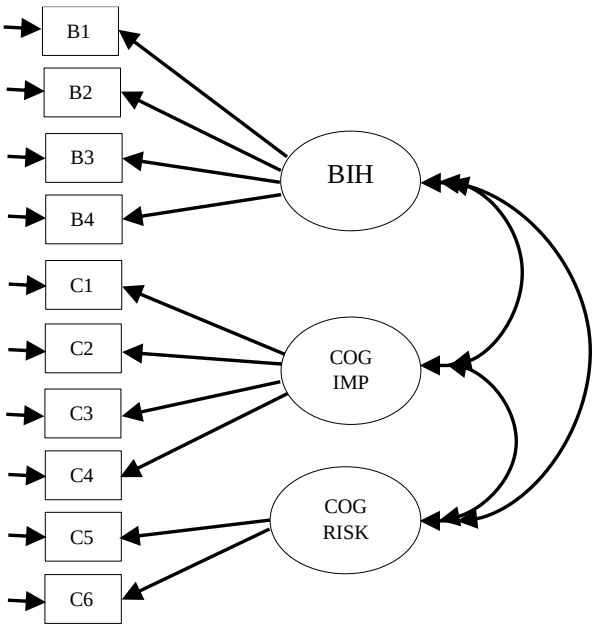


Figure 2. Final model for both versions of the BCISQ (English and German)

TABLE I. MODEL FIT INDICES FOR THEORETICAL AND FINAL MODEL WITH REFERENT VALUES[1]

Model fit indices	Theoretical Croatian model (df=34)	Theoretical German model (df=34)	Final Croatian model (df=32)	Final German model (df=32)	Reference values	
					Good fit	Adequate fit
χ^2	164.18/34 = 4.82	102.16/34 = 3	46.61/32 = 1.45 (n.s.)	51.44/32 = 1.61	p > 0.01 (n.s.)	χ^2 / df ≤ 2
CFI	0.76	0.75	0.97	0.93	≥ 0.95	≥ 0.90
TLI	0.68	0.66	0.96	0.90	≥ 0.95	≥ 0.90
RMSEA	0.12	0.09	0.04	0.05	≤ 0.06	≤ 0.08
SRMR	0.07	0.08	0.04	0.05	≤ 0.08	≤ 0.10

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

The model fit for both groups (Croatian and German) was first tested for the theoretical models (Figure 1). For both, the Croatian and the German models, the results did not show adequate model fit (Table 1).

Additional analysis showed high covariances between the measurement errors of the last two questions of the cognitive scale (r = 0.67 for the Croatian sample and r = 0.47 for the German sample; modification index for the error covariance in the Croatian sample = 110.54; modification index for the error covariance in the German sample = 39.51). Therefore, the cognitive subscale, which measures security awareness, was split into two subscales: risk and importance.

The final model, consisting of 3 scales (Behavior, Cognitive Risk and Cognitive Importance) was tested for both groups (Figure 2). Results showed a good model fit of both models, which confirmed a good construction of the new instrument. The model fit was slightly better for the Croatian than the German sample.

For both theoretical scales, differences between the Croatian and German samples were tested using ANOVA. On both scales, there were statistically significant differences (Table 2). Croatian students had a slightly higher security awareness and less risky online behavior. These differences could be a result of cultural, language and age differences between those two groups but also due to the inadequate model fit of the theoretical model and the necessity of developing a new one.

TABLE II. Mean comparison between the Croatian and the German samples using ANOVA

Analysis results		N	Mean	SD	F
B scale - online risky behavior	Croatian	250	4.74	0.41	57.04**
	German	225	4.41	0.56	
	Total	475	4.58	0.51	
C scale - security awareness	Croatian	250	3.68	0.72	119.78**
	German	225	2.99	0.64	
	Total	475	3.35	0.76	

** p < 0.01

IV. CONCLUSION

The newly developed international instrument, i.e. a modified version of the *Behavioral-cognitive internet security questionnaire with 3 subscales,* showed good potential for future study purpose. It can be used as an international instrument to gather reliable data in a short time.

The model fit for the Croatian sample (English version of the questionnaire) was better than in the German sample. In addition, Croatian students showed less risky online behavior and better information security awareness. Maybe these results could be explained due to language differences. In Croatia, the majority of information systems that people work with every day are in the English language and most young people have a better understanding of specific information security terms in English. Nevertheless, in Germany most operating systems and programs do actually have a German version. It is not clear are the obtained differences result of language or cultural differences between Croatian and German students. It can be concluded that the English language should be used as a basis for international usage and future data comparison.

Both models (with Croatian and German samples) point at the same problematic area. The original cognitive scale should be split into two separate subscales, one that would examine the cognitive importance of information security and another that would examine the cognitive risk of information security.

Future studies should try to develop a third subscale (risk) of the BCISQ because only two items do not suffice to represent a whole subscale. Furthermore, it would be interesting to develop a behavior scale that represents a simulation of real online behavior in potentially risky situations. In addition, the BCISQ should be tested in other cultures and age groups in order to confirm its reliability. It is also recommended to apply longitudinal designs in future studies to test the stability and consistency of the BCISQ.

REFERENCES

[1] 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, pp. 122-131, July 2001.

[2] A. Keszthelyi, "About Passwords", Acta Polytechnica Hungarica, vol.10, pp. 99-118, September 2013.

[3] K. Solic, H. Ocevcic and D. Blazevic, "Survey on PasswordQuality and Confidentiality"", Automatika, vol. 56, April 2015.

[4] A.G. Voyiatzis, C.A. Fidas, D.N. Serpanos and N.M. Avouris, "An Empirical Study on the Web Password Strength in Greece", 15th Panhellenic Conference on Informatics, (Kastonija Greece), pp. 212-216, September-October 2011.

[5] M. Dell'Amico, P. Michiardi and Y. Roudier, "Password Strength:An Empirical Analysis", Proceedings IEEE INFOCOM, (San Diego, CA) pp. 1-9, March 2010.

[6] Wanli, J. Campbell, D. Tran and D. Kleeman, "Password Entropy and Password Quality", 4th International Conference on Network and System Security, (Melbourne, VIC), pp. 583-587, 1-3, September 2010.

[7] P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L.F. Cranor and J. Lopez, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms", IEEE Symposium on Security and Privacy, (San Francisco, CA), pp. 523-537, May 2012.

[8] A. Tsohou, S. Kokolakis, M. Karyda and E. Kiountouzis, "Process-variance models in information security awareness research", Information Management & Computer Security, vol.16, pp. 271-287, July 2008.

[9] S. Williams and S. Akanmu, "Relationship between Information Security Awareness and Information Security Threats", IJRCM, vol.3, pp. 115-119, August 2013.

[10] P. Tasevski, "Methodological approach to security awareness", CyberSecurity for the Next Generation. (Politechnico di Milano, Italy), 11-12, December 2013.

[11] P. Puhakainen and M. Siponen, "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study", MIS Quarterly, vol. 34, pp. 757-778, December 2010.

[12] K. Solic, D. Sebo, F. Jovic and V. Ilakovac, "Possible Decrease of Spam in the Email Communication", Proceedings IEEE MIPRO, (Opatia), pp. 170-173, May 2011.

[13] K. Beckers, L. Krautsevich, and A. Yautsiukhin, „Analysis of Social Engineering Threats with Attack Graphs", Proceedings of the 3rd International QASA - Affiliated workshop with ESORICS, (Wroclow, Poland), September 2014.

[14] K. Solic and 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, pp. 261-264, August 2009.

[15] R. E. Crossler, A. C. Johnston, P. B. Lowry, Qing Hu, M. Warkentin and R. Baskerville, "Future directions for behavioral information security research", Computers&Security, vol. 32, pp. 90–101, June 2013.

[16] T. Velki, K. Solic and H. Ocevcic, "Development of Users' Information Security Awareness Questionaire (UISAQ) - Ongoing Work", Proceedings IEEE MIPRO, (Opatia), pp. 1417-1421, May 2014.

[17] T. Velki, K. Solic and K. Nenadic, „Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS)", Psihologijske teme, vol. 24, pp. 401-424, December, 2015.

[18] T. Velki, K. Solic and T. Galba, „Empirical study on ICT system's users' risky behavior and security awareness", Proceedings IEEE MIPRO, (Opatia), pp. 1356-1359, May 2015.

[19] T. Velki, K. Solic, V. Gorjanac and K. Nenadic „Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results", Proceedings IEEE MIPRO, (Opatia), pp. 1496-1500, May 2017.

[20] G. Öğütçü, Ö.M. Testik and O. Chouseinoglou, „Analysis of personal information security behavior and awareness", Computers & Security, vol. 56, pp. 83–93, February 2016.

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

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

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

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