Psychologists as information-communication system users: Is this bridge between information-communication and behavioral science enough to prevent risky online behaviors?

Velki, Tena

Source / Izvornik: **MIPRO 2022 Proceedings, 2022, 1196 - 1200**

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:141:453796

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

FOOZOS Repository - Repository of the Faculty of Education

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Psychologists as information-communication system users: Is this bridge between information-communication and behavioral science enough to prevent risky online behaviors?

T. Velki*
* J.J. Strossmayer University/ Faculty of Education, Osijek, Croatia
tena.velki@gmail.com

***Abstract* - The research aimed to examine the level of security awareness and knowledge and online risky behavior of psychologists as information-communication systems users, i.e., experts in the field of behavioral sciences with some work experience in the Internet security area. Participants were 55 employed psychologists. They completed an online Behavioral-Cognitive Internet Security Questionnaire, consisted of two scales that measure cognitive risk and importance of data privacy and two scales that measure self-assessed risky online behavior and actual risky online behavior (simulated). The results showed that a large number of psychologists show risky online behaviors: 40% left their e-mail addresses, and 45.5% gave their passwords. No statistically significant association was obtained between self-assessed and simulated risk behavior, i.e. what they say about their online activities and how they actually behave online was not associated. Furthermore, results showed statistically significantly more actual risky online behavior (simulated) than reported by self-assessment. Psychologists are also more aware of the importance of data storage in relation to the potential risks of their alienation. Obviously, previous education and the current level of information security awareness are insufficient to prevent risky online behaviors even of well-informed users. Moreover, what users report about their online behavior is inconsistent with their actual behavior, leading to the need to develop additional simulation scales to measure computer users' actual risk behaviors and new prevention programs to decrease actual online risky behaviors in users.**

Keywords - psychologists; information-communication users; Behavioral-Cognitive Internet Security Questionnaire (BCISQ); risky online behavior

I. INTRODUCTION

Initially, the most effective security measure against social engineering was considered to be to increase user awareness of the tricks social engineers use against them [1]. Therefore, information security awareness has become part of many international standards as a prerequisite for introducing prevention programs. Suppose organizations want to obtain an internationally recognized certificate on information security. In that case, they must adopt an information security awareness plan aimed at reducing the number of security incidents, adopting international standards or best practices in information security, covering all problems in information security and systems management, and harmonization of work with legal regulations related to data security and privacy protection [2].

A. Paradox of education

In the 21st century, an educational paradox has emerged in many fields. Knowledge is abundant, nearly free, and can be easily accessed without critical thinking. To understand these trends, we must move beyond the argument that education is simply the acquisition of certain attributes in order to succeed in the modern society. These arguments fall short because they view education solely in terms of knowledge and skills that can be tested but these effects on people behavior are neglected and at least questionable [3]. Furthermore, there is no evidence of strong association between people's knowledge and attitudes with their actual behavior [4].

Accordingly, the mere increase in the level of awareness and knowledge of users has not always led to a decrease in their online risk behavior, even among the highly educated population such as university professors [5, 6]. This phenomenon is also explained by the paradox of education. While many users show theoretical interest about their online privacy and knowledge about maintaining computer data, they actually rarely show that protective online behavior in real-life situations [7, 8, 9]. Moreover, some research has shown that more excellent knowledge and higher information security awareness lead to riskier user behavior when using information systems [10, 11, 12].

Only the knowledge and awareness that a person has specific knowledge about some topics creates a false sense of security in computer users, contributing to not paying attention and not adhering to the learned information security rules. Even electrical engineers (generally more technically experienced users) are unexpectedly less cautious and behave riskier [10, 12, 13].

B. Privacy paradox

Privacy paradox explains the discrepancy between positive privacy attitudes and actual risky online behavior

[14, 15]. A certain degree of risk perception implies greater knowledge of privacy protection strategies but appears an insufficient motivator to apply such strategies [16]. Accordingly, many previous research on online risky behavior has revealed this discrepancies between users attitudes and their actual online behavior, i.e. users who claim to be very concerned about their privacy usually undertake very little to protect their personal data [17 - 20]. The way a person intends to protect their online privacy is totally opposite to how they actually behave online. Of particular concern is that users generally have higher knowledge (higher level of risk awareness) during the last decade but behave riskier [10, 11, 21].

Furthermore, not only that paradox of education and privacy was confirmed, but also no correlation was obtained between actual and self-assessed risk behavior among student Internet users [22, 23]. It is evident that only knowledge, and even awareness of information security, do not always serve as protective factors in risky online behavior. It is necessary to investigate this phenomenon, i.e., additional factors affecting users' information security awareness and online behavior [23].

Given that preliminary data among the student population show that the users' actual behavior in the virtual world is not related to their assessments [21, 23], the question arises: 1) what is the cause of this unexpected result ?; 2) could information security and/or behavioral experts, however, provide more reliable estimates than average students' population ?

C. Study aim

The research aimed to examine psychologists' information security awareness and behavior as information-communication systems users, i.e., cognitive and behavioral aspects of information security in psychologists. The peculiarity of this sample of psychologists is that they all deal with some aspects of digitalization, i.e., the experts in the field of behavioral sciences who also deal with internet security were selected. Therefore, first hypothesis assumed that their information security awareness and behavior would be better than in the average users, i.e., more secure and with a higher level of awareness. Secondly, it was also assumed that the level of previous knowledge and education about internet security would affect information security awareness and their risky behavior.

II. METHOD

A. Participants

The study involved 55 employed psychologists from all over Croatia (89 % of women) with an average age of 35.18 +/- 8.65 (arithmetic mean +/- SD). About 11 % of them finished some form of postgraduate study. Most of them worked in the public sector (74.5 %), and some of them in private (20 %), others were unemployed at the time of conducting the research (5.5 %). Most of participants reported about satisfactory (good) general technical knowledge of computers (80%) and some of them had additional previous education about data privacy and internet security (38.2%).

The including criteria for participation in this study was that participant has at least master degree in field of psychology and that is active participant of conference with central topic "Psychology and the Digital World". Based on these criteria it was assumed that participants have expertise in the field of behavioral sciences (psychology) with some work experience in the Internet security area (information-communication science).

B. Procedure

The research was conducted during the Croatian psychologists' annual conference whose central topic was "Psychology and the Digital World". Participants were asked to fill out a short questionnaire on their smartphones during the invited lecture "Risky behaviors of computer users in the digital world". Out of a total of 98 participants, 86 agreed to participate. For the purposes of this paper, only psychologists were selected (students and participants of other professions were excluded from further analyzes).

C. Instruments

The Behavioral-Cognitive Internet Security Questionnaire (BCISQ; Croatian version) [24] with some general and demographical data was used. The first part of the BCISQ consisted of two behavior scales measuring information security, i.e., computer user potentially risky behavior (risky behavior self-assessment (k[1]=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:_____)). The second part of the BCISQ consisted of 2 cognitive scales, which measured the level of 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?*). On behavioral scales, higher results indicate more risky behavior, but higher results indicate a higher level of Internet security awareness on cognitive scales. As this is a new measurement instrument, the factor structure was also checked. CFA [2] showed adequate model fit for four subscales (TLI[3] = 0.90; CFI[4] = 0.89; RMSEA[5] = 0.08; SRMR[6] = 0.09), as well as satisfactory internal reliability (Cronbach α from α = 0.62 for risky behavior self-assessment scale to α = 0.90 for cognitive risk scale). Participants also filled out data about their gender, age, education, profession, and data on the general technical

[1] k - number of items in scale
[2] CFA - Confirmatory Factor Analysis
[3] TLI - Tucker Lewis Index, a relative reduction in misfit per degree of freedom
[4] CFI - Comparative Fit Index, compares the fit of a target model to the fit of an independent, or null, model
[5] RMSEA - Root Mean Square Error of Approximation, an absolute measure of model fit based on the non-centrality parameter
[6] SRMR - Standardized Root Mean Square Residual, an absolute measure of model fit based on correlation

knowledge of computers and previous education of data privacy and internet security.

III. RESULTS

Before selecting the appropriate statistical procedures, pre-analyzes were made (Table 1). It was concluded that inferential statistics could be applied based on descriptive indicators (asymmetry indices do not exceed value +/- 4).

TABLE I. DESCRIPTIVE STATISTICS FOR SUBSCALES OF BCISQ

BCISQ subscales	Min	Max	M	SD	Skewness	Kurtosis
Risky behavior simulation scale	0.00	4.00	1.64	1.50	0.45	-1.28
Risky behavior self-assessment scale	0.00	1.75	0.32	0.38	1.68	3.61
Cognitive importance scale	0.25	4.00	3.02	0.75	-1.15	1.99
Cognitive risk scale	0.00	4.00	2.32	0.99	-0.02	-0.52

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

In order to examine psychologists' information security awareness and behavior as information-communication systems users descriptive analysis was performed.

Mean values of cognitive scales (Cognitive importance scale and Cognitive risk scale) indicates that participants had a relatively high level of Internet security awareness; especially they were aware of importance of keeping online data protected.

Mean values of behavioral scales have shown that participant self-assed low level of risky online behavior and slightly higher level of simulated risky online behavior. However, based on individual results on the Risky behavior simulation scale, psychologists showed poor results; 40% of them left their e-mail addresses, and 45.5% gave their passwords (in 29% of cases both data), 34.5% indicated that they wanted to receive information about similar research from partners and 43.6% that they wished to via mail receive free antivirus software from a third party. Their actual online behavior was rather risky.

A paired-sample t-test was performed to check for behavioral and cognitive subscales differences. Results showed statistically significantly more simulating risky behavior compared to reported self-assessed risky behavior ($t = 6.68$; $p < 0.01$). Psychologists are also more aware of the importance of data storage in relation to the potential risks of their alienation ($t = 4.57$; $p < 0.01$).

First hypothesis assumed that psychologists' information security awareness and behavior would be better than in the average users. Compared to data from general students population (Table 2, details in Velki & Šolić, 2020) [21], psychologists showed more simulated online risky behavior ($t = 2.36$; $p < 0.05$), more self-assessed risky online behavior ($t = 2.05$; $p < 0.05$), less awareness of cognitive risk ($t = 3.39$; $p < 0.01$), and there was no statistically significant difference on Cognitive importance scale ($t = 0.09$; $p > 0.05$).

TABLE II. BASIC DESCRIPTIVE STATISTICS ON GENERAL STUDENT POPULATION (N=287, DETAILS IN VELKI & ŠOLIĆ, 2020) [20]

BCISQ subscales	Min	Max	M	SD
Risky behavior simulation scale	0.00	4.00	1.21	1.18
Risky behavior self-assessment scale	0.00	2.75	0.20	0.40
Cognitive importance scale	0.50	4.00	3.01	0.71
Cognitive risk scale	0.00	4.00	2.87	1.12

Second hypothesis assumed that the level of previous knowledge and education about internet security would affect information security awareness and their risky behavior. One-way ANOVA was performed to check for main effects of previous general technical knowledge about computers and the Internet, prior knowledge about information security and data privacy, and previous education related to security and privacy issues on the Internet on behavioral and cognitive aspects of internet security among psychologist as computer users (Table 3).

TABLE III. RESULTS OF ONE-WAY ANOVA: TESTING MAIN EFFECTS OF PREVIOUS KNOWLEDGE AND EDUCATION ABOUT INTERNET SECURITY ON SECURITY AWARENESS AND BEHAVIOR OF PSYCHOLOGISTS

BCISQ subscales / Previous education	Risky behavior simulation scale	Risky behavior self-assessment scale	Cognitive importance scale	Cognitive risk scale
previous general technical knowledge about computers and the Internet	$F_{(2,52)} = 1.21$ $p > 0.05$	$F_{(2,52)} = 0.59$ $p > 0.05$	$F_{(2,52)} = 0.22$ $p > 0.05$	$F_{(2,52)} = 1.91$ $p > 0.05$
previous knowledge about information security and data privacy	$F_{(2,52)} = 0.14$ $p > 0.05$	$F_{(2,52)} = 1.17$ $p > 0.05$	$F_{(2,52)} = 2.05$ $p > 0.05$	$F_{(2,52)} = 1.39$ $p > 0.05$
previous education related to security and privacy issues on the Internet	$F_{(1,53)} = 1.53$ $p > 0.05$	$F_{(1,53)} = 0.24$ $p > 0.05$	$F_{(1,53)} = 3.39$ $p > 0.05$	$F_{(1,53)} = 1.37$ $p > 0.05$

Prior knowledge and education did not affect either user awareness or user behavior indicating existence of educational paradox in psychologist.

TABLE IV. PEARSON CORRELATION COEFFICIENTS BETWEEN SUBSCALES OF BCISQ

BCISQ subscales	1.	2.	3.	4.
1. Risky behavior simulation scale	1	0.207	0.002	-0.114
2. Risky behavior self-assessment scale	0.207	1	-0.195	0.057
3. Cognitive importance scale	0.002	-.195	1	0.163
4. Cognitive risk scale	-0.114	0.057	0.163	1

No statistically significant association was obtained between self-assessed and simulated online risk behavior, indicating that reported and actual user behavior are not correlated. Furthermore, there were no statistically significant correlations between any of the BCISQ subscales (Table 4), indicating that level of user information security awareness is not associated with any type (reported or simulated) risky online behavior.

IV. CONCLUSION

The interpretation of obtained results are pretty devastating. As the main topic of the research was to check whether psychologists, as information-communication system users, are sufficient to bridge the educational and privacy paradox, i.e. whether knowledge of both areas, information-communication and behavioral sciences, is enough to prevent risky online behaviors, the results clearly show that experts in this field with their specific knowledge are not sufficient to prevent online risky behavior.

Although previous research has clearly shown the existence of an educational and privacy paradox among students and professors, but also among IT professionals [7 - 17], it was expected that theses paradox will be expressed to a lesser extent in experts who are who are well acquainted with it. However, obtained results have shown that previous knowledge and education have no impact on reducing risky behavior, even when it comes to experts in the field of internet security and behavioral sciences. There is no correlation between the level of information awareness and online risk behavior (neither simulated nor assessed). Even more worrying is that simulation (actual behavior) has not been associated with users' self-assessments of online behavior. Obviously, psychologists do not base self-assessment of their risky behavior on their actual online risky behavior.

The results of the simulation scale are particularly disappointing, especially if we take into account the specifics of the sample, i.e., highly educated experts in the field of behavioral science with experience in working on Internet security issues. Psychologists have shown significantly more simulated risk behaviors than they have self-assessed. Not only their estimates are inconsistent with the simulated behavior, but they also show that their actual online behavior is quite risky and worrying (29% of them voluntarily provided their email address and associated password). Some of these participants are professors at different universities, that is, the persons responsible for the student's acquisition of knowledge as well as their behavioral models. Given these results, it is questionable how well and what they actually transfer to their students or employees.

Could information security and/or behavioral experts, however, provide more reliable estimates than average students' population? In relation to the general student population, unexpected, devastating results were also obtained. Although the results obtained are in line with previous research [5, 6], especially those where the existence of educational and privacy paradox has been confirmed [7-20], given the specificity of the sample, we expected a lower level of simulated online risk behavior and more reliable self-assessment, that is, their interconnectedness.

What is the possible cause of this unexpected result? Some methodological shortcomings are worth of mentioning. Although this was first study on psychologists, as experts in field of information-communication and behavioral sciences, the sample size was rather small (N=55). The main criteria for including these experts in study was active participation in annual psychology conference with central topic "Psychology and the Digital World", and not measuring the actual level of knowledge from both field of expertise. Data on their general technical knowledge of computers and previous education of data privacy and internet security was gathered but only using self-assessments. Different including criteria, with more strict measures of actual knowledge and wider range of simulated online risky behavior, could give us better insight in educational and privacy paradox within experts.

However, the main scientific contribution of conducted study relates to the verification of educational and privacy paradoxes in the field of information security on a specific population of experts which has not been examined in previous research. In addition, for the first time a simulation scale of online risky behavior was applied, and not only the self-assessment of participants as in previous research. Obtained results with these two different measures proved to be very important and significant because they show that reports from experts about their online behavior is not reliable measure per se and it differ from their actual online behavior.

Future research should develop additional simulation scales that will measure actual online risk behavior more closely. As education itself has so far proved insufficient, at least in its current form, to reduce online risk behavior, future practitioners should make it more interactive by simulating the real potential consequences of risky online behavior. Learning through trial and error, with consequences on one's own skin, has so far always proved effective [25]. Therefore, in the context of reducing risky online behavior, the same principles could be applied, simulating actual user errors and consequences that they can cause in real life.

REFERENCES

[1] H. Wilcox, M. Bhattacharya and R. Islam, R. "Social Engineering through Social Media: An Investigation on Enterprise Security", in Communications in Computer and Information Science, L. Batten, G. Li, W. Niu and M. Warren, Eds. Berlin: Heidelberg Springer, 2014, pp. 243-255.

[2] S. Bauer, E. Bernroider and K. Chudzikowski, "End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study". Proceeding from Eighth Workshop on Information Security & Privacy, pp. 1-16, May 2013.

[3] J. Ganem, "The Robot Factory". Springer, Cham, 2018.

[4] A. Bainbridge Frymier and M. K. Nadler, "The Relationship Between Attitudes and Behaviors" in Persuasion: Integrating Theory, Research, and Practice, A. Bainbridge Frymier and M. K. Nadler, Eds. Dubuque, Iowa: Kendall Hunt Publishing Company, 2017, pp. 41-58.

[5] 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.

[6] K. Solic, V. Ilakovac, A. Marusic and M. Marusic, "Trends in using insecure e-mail services in communication with journal editors", 6th Peer Review and Biomedical Publication, Vol. 33, No. 2, 2009, pp. 50.

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

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

[9] J. Tsai, L. Cranor, A. Acquisti and C. Fong, "What's it for you? A survey of online privacy concerns and risk", NET Institute Working Paper, No. 06–29, 2006, pp. 1–20.

[10] T. Velki and K. Romstein, "User Risky Behavior and Security Awareness through Lifespan", International Journal of Electrical and Computer Engineering Systems, Vol. 9, No. 2, 2018, pp. 9-16.

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

[12] 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.

[13] 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.

[14] A. Acquisti, "Privacy in electronic commerce and the economics of immediate gratification". Proceedings of the 5th ACM Conference on Electronic Commerce, USA, pp. 21-29, May 2004.

[15] S. B. Barnes, S.B., "A privacy paradox: Social networking in the United States", First Monday, Vol. 11, No. 9, September 2006, doi:10.5210/fm.v11i9.1394.

[16] I. Oomen and I. Leenes, "Privacy risk perceptions and privacy protection strategies", in Policies and Research in Identity Managemen, E. de Leeuw, S. Fischer-Hübner, J. Tseng and J. Borking, Eds. Boston: Springer Verlag, 2008, pp. 121-138.

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

[18] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, Vol. 64, 2017, pp. 122-134.

[19] D. P. Snyman, H. Kruger and W. D. Kearney, "I shall, we shall, and all others will: Paradoxical Information Security Behaviour", Information and Computer Security, Vol. 26, No. 3, 2018, pp. 290-305.

[20] S. Barth and M. D. T. de Jong, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review", Telematics and Informatics, Vol.3 4, No. 7, November 2017, pp. 1038-1058.

[21] T. Velki and K. Šolić "Razvoj instrumenta za istraživanje socijalnog inženjeringa u populaciji studenata: Bihevioralno-kognitivni upitnik internetske sigurnosti (BKUIS)", Policija i sigurnost, Vol. 29, No. 4, 2020, pp. 341-355.

[22] B. Lebeck, J. Uffen, M. Neumann, B. Hohler and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review", Management Research Review, Vol. 37, No. 12, 2014, pp. 1049-1092.

[23] 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 IEEE MIPRO, (Opatia), pp. 1410-1413, May 2019.

[24] 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, Vol. 10, No.1, 2019, pp. 19-24.

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