Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work

T. Velki[*], K. Solic[**] and H. Ocevcic[***]
[*] J.J. Strossmayer University/ Faculty of Teacher Education, Osijek, Croatia
[**] J.J. Strossmayer University/ Faculty of Medicine, Osijek, Croatia
[***] J.J. Strossmayer University/ Faculty of Electrical Engineering", Osijek, Croatia
tena.velki@gmail.com, kresimir@mefos.hr, ocevcic@gmail.com

Abstract - The user is still weakest link regarding information security matters, but studies on this subject are rare. The aim of this work is to develop general Users' Information Security Awareness Questionnaire (UISAQ). Development consists of selecting suitable items for which is assumed that measure the level of security awareness and testing impact of each item in measurement. Questionnaire consisted of 4 parts with total of 37 items. Results showed that first part of questionnaire, that examine the common user's risk behavior, should consist of 17 items (3 items had low factor loadings) separate in 3 subscales. Second part of questionnaire, which consisted of 6 items that measured the level of user's information security, had high internal consistency (k=6, α=0.89) and a satisfactory factor loadings. Third part of questionnaire, which consisted of 5 items that measured the level of user's beliefs about information security, should consist of 3 items (2 items significantly disrupted internal consistency) with high factor loadings and good internal consistency (α=0.76). Descriptive statistics showed that all the questions (n=6) in the fourth part of the questionnaire, which had examined the password quality and security, had a full range of answers and that normal distribution wasn't significantly violated. Although developed questionnaire requires more work and validation, first results showed that UISAQ has potential to become a good and reliable measure of users' security awareness in the future.

I. Introduction

Through the years, user of information system is still its weakest link regarding information security matters [1, 2]. Information system's user can, with his potentially risky behavior, significantly influence on overall system's security [3 - 5] and all hacker attacks usually combine social engineering with technical hacking skills [6]. However scientific studies on this subject are rare and there is need for universal measurement instruments [7, 8]. These instruments should enable measurement of user's influence on overall systems' security for state analysis and future studies.

Some previous solutions are proposed, but are partial and not universal enough [9, 10]. Actually most of the previous research on user's behavior is focused only on examining password usage and password quality and strength [11 -14].

The aim of this work was to develop reliable universal instrument which will measure level of information system's users' awareness on security matters, as general as possible, the Users' Information Security Awareness Questionnaire (UISAQ).

Development of this kind of questionnaire comprises selection of suitable items and testing impact of each item. Impact of each item which is assumed that measures the level of security awareness among users, is measured by using descriptive statistics, factor analysis and reliability analysis. Results of those analyses will exclude items with low impact and point out items with higher impact that present well defined questions [15].

With internationally validated questionnaire it should be possible to gain general conclusions about user's security awareness and potentially risky behavior. Results of those kinds of studies will enable concrete improvements of existing [16 - 18] and development of new information security solutions focused on user's education.

II. Method

A. Participants

Participants in this study were students (N=135) on second year of undergraduate study, from three different faculties of J.J. Strossmayer University of Osijek: Faculty of Teacher Education (N=41), Faculty of Medicine (N=51) and Faculty of Electrical Engineering (N=43). Proportion of mail students was 47.6% while proportion of female students was 52.4%. The average age of participants was 19.85 +/- 0.58 (arithmetic mean +/- SD).

B. Procedure

During regular classes students were asked to voluntarily give some general information about self (age and gender) and to fill out the UISAQ. Filling out the questionnaire lasted for approximately 30 minutes. Survey was done on all three groups of participants during one week period.

C. *Instruments*

For the purpose of this research authors created UISAQ consisting of four parts with total of 37 items collected from different security guidelines and results of previous studies [19 - 24]. Each item is a question in the UISAQ presenting variable for the statistical analysis.

The four parts of UISAQ are as follows:

- First part of UISAQ consisted of 20 items measuring computer users' potentially risky behavior.
- Second part of questionnaire consisted of 6 items that measured the level of user's information security awareness.
- Third part of questionnaire consisted of 5 items which measured the level of user's beliefs about information security.
- The last part of UISAQ consisted of 6 questions that examined the quality and security of passwords.

TABLE I. STRUCTURE MATRIX FOR THE FIRST PART OF UISAQ EXTRACTION (METHOD: PRINCIPAL COMPONENT ANALYSIS; ROTATION METHOD: OBLIMIN WITH KAISER NORMALIZATION)

Items	**Factors**		
	1	***2***	***3***
sc1	.404		.521
sc2	.518	-.337	.519
sc3			.687
sc4			.799
sc5			.653
sc6		.666	
sc7		.741	
sc8		.810	
sc9	.598		
sc10			
sc11	.427		
sc12	.677		
sc13	.624		
sc14	.410		
sc15		.343	
sc16	.646		
sc17		.405	
sc18		.561	
sc19			
sc20			

TABLE II. RELIABILITY ANALYSIS: ITEM - TOTAL STATISTICS FOR THE FIRST PART OF UISAQ EXTRACTION

Items	**Analysis results**			
	Scale Mean if Item Deleted	***Scale Variance if Item Deleted***	***Corrected Item - Total Correlation***	***Cronbach's Alpha if Item Deleted***
1. factor (subscale)				
sc9	8.1756	6.084	.405	.539
sc11	8.7643	7.044	.274	.592
sc12	9.0153	6.569	.444	.532
sc13	8.8397	6.659	.423	.540
sc14	9.1832	7.997	.265	.602
sc16	7.6260	5.051	.365	.586
2. factor (subscale)				
sc6	15.4809	21.944	.471	.599
sc7	15.7176	22.866	.473	.600
sc8	15.5725	21.585	.594	.556
sc15	15.5038	25.929	.223	.688
sc17	16.6718	24.930	.293	.664
sc18	14.6031	25.703	.373	.637
3. factor (subscale)				
sc1	5.3806	3.410	.432	.609
sc2	5.2239	3.002	.515	.565
sc3	5.7015	4.136	.502	.580
sc4	5.8507	4.248	.417	.611
sc5	5.9925	5.060	.321	.658

The participants had to evaluate to which extend each statement refers to him/her on a scale from 1 to 5. This implies that each variable, for each examinee, can have only one value in range from 1 to 5.

Unanswered questions were not included in the statistical analysis.

III. RESULTS

Development of questionnaire consisted of selecting suitable items for which there was assumption that measure the level of potentially risky behavior of computer users, level of information security awareness, users' believes about safety or password quality issues. Using descriptive statistics, factor analysis and reliability analysis we tested if selected items were good measure of hypothesized construct.

For the first part of UISAQ Exploratory factor analysis (method principal components, oblimin rotation) was used. Analyses have shown extraction of 8 factors (using the Guttman-Kaiser criterion) with eigen values larger than 1 and explanation of 66.11 % of overall variance. Given factor structure shown only 3 dominant factors (each explained more than 10% of variance and 37.42% of overall variance) and other factors had smaller eigen

TABLE III. MEASURES OF SENSITIVITY FOR THE FIRST PART OF UISAQ EXTRACTION

Items	Analysis results					
	Min	*Max*	*Range*	*Mean*	*Std. Deviation*	*Test of normality*
sc1	1.00	5.00	4.00	1.674	.937	.330^{a}
sc2	1.00	5.00	4.00	1.822	.984	.264^{a}
sc3	1.00	4.00	3.00	1.348	.615	.434^{a}
sc4	1.00	5.00	4.00	1.187	.627	.497^{a}
sc5	1.00	5.00	4.00	1.045	.365	.526^{a}
sc6	1.00	5.00	4.00	3.201	1.685	.227^{a}
sc7	1.00	5.00	4.00	3.007	1.549	.225^{a}
sc8	1.00	5.00	4.00	3.142	1.513	.199^{a}
sc9	1.00	5.00	4.00	2.134	.916	.284^{a}
sc11	1.00	5.00	4.00	1.552	.771	.332^{a}
sc12	1.00	5.00	4.00	1.303	.730	.454^{a}
sc13	1.00	4.00	3.00	1.478	.723	.373^{a}
sc14	1.00	3.00	2.00	1.149	.434	.517^{a}
sc15	1.00	5.00	4.00	3.195	1.612	.218^{a}
sc16	1.00	5.00	4.00	2.699	1.273	.228^{a}
sc17	1.00	5.00	4.00	2.038	1.600	.422^{a}
sc18	1.00	5.00	4.00	4.120	1.273	.303^{a}

a. p < 0.01

values and very small proportion (less than 7%) of explained variance. First factor explained 14.30 % of overall variance, second factor explained 12.92% of overall variance and third factor explained 10.19 % of overall variance. Than, Confirmatory factor analysis was used in order to test 3 hypnotized factors which were extracted from previous Exploratory factor analysis. The saturation (factor loadings) was defined as larger than 0.3 which interpreted the three mentioned factors.

The factor structure of the first part of UISAQ is shown in Table 1. As shown in table, 3 items had factor loading lower than 0.3 on all of three factors and they were suppressed and thereby not shown in table (items sc10, sc19 and sc20) so they were excluded from further analysis. Final version of first part of UISAQ should consist of 17 items separate in 3 subscales: first subscale measures risky behavior of computer users (k=6), second subscale measures maintenance of computer systems (k=6), and third ones measures using other users' data (k=5). Than reliability analysis was done for three new scales (Table 2). First subscale had little bit lower internal consistency (k=6; Cronbach α=0.61), but all items contributed significantly to good internal consistency which implies that this form of subscale should be kept as finale one. Second subscale had a satisfactory internal consistency (k=6; Cronbach α=0.67), as well as third one (k=5; Cronbach α=0.66) which implies that both of these two forms of subscales should be kept as finale ones.

TABLE IV. COMPONENT MATRIX FOR THE SECOND PART OF UISAQ EXTRACTION (METHOD: PRINCIPAL COMPONENT ANALYSIS)

Items	Factor
sc1	.694
sc2	.731
sc3	.853
sc4	.880
sc5	.868
sc6	.768

TABLE V. RELIABILITY ANALYSIS: ITEM - TOTAL STATISTICS FOR THE SECOND PART OF UISAQ EXTRACTION

Items	Analysis results			
	Scale Mean if Item Deleted	*Scale Variance if Item Deleted*	*Corrected Item - Total Correlation*	*Cronbach's Alpha if Item Deleted*
sc1	13.7615	20.540	.582	.888
sc2	14.6385	20.000	.620	.882
sc3	13.7308	17.795	.771	.858
sc4	13.9538	17.192	.806	.852
sc5	14.1692	18.064	.793	.855
sc6	13.9769	19.030	.662	.876

Results of sensitivity test of new formed questionnaire are shown in Table 3. Only 3 items did not have full range (sc3, sc13, sc14) which implies about good sensitivity of new formed scales. Distribution of results was not normal (Kolmogorov-Smirnov Statistic was significant for all items), which was expected. For first and third subscales means were at lower part of subscale (positive asymmetry) meaning less risky behavior of computer users and for second subscale means were at higher part of subscale (negative asymmetry) meaning more risky behavior of computer e.g. low level of users' maintenance of personal computer systems.

The Exploratory factor analysis (method principal

TABLE VI. MEASURES OF SENSITIVITY FOR THE SECOND PART OF UISAQ EXTRACTION

Items	Analysis results					
	Min	*Max*	*Range*	*Mean*	*Std. Deviation*	*Test of normality*
sc1	1.00	5.00	4.00	3.083	.946	.233^{a}
sc2	1.00	5.00	4.00	2.203	.975	.283^{a}
sc3	1.00	5.00	4.00	3.121	1.126	.252^{a}
sc4	1.00	5.00	4.00	2.893	1.172	.207^{a}
sc5	1.00	5.00	4.00	2.667	1.068	.213^{a}
sc6	1.00	5.00	4.00	2.872	1.076	.189^{a}

a. p < 0.01

TABLE VII. COMPONENT MATRIX FOR THE THIRD PART OF UISAQ EXTRACTION (METHOD: PRINCIPAL COMPONENT ANALYSIS)

Items	Factor
u7	.391
u8	.796
u9	.856
u10	.758
u11	.428

components) was also used for the second part of UISAQ, which have shown extraction of 1 factors and explanation of 64.37 % of overall variance. In table 4 is shown factor structure of the second part of UISAQ which consisted of 6 items that measured the level of user's information security awareness, and which had a satisfactory factor loadings for all items on one factor.

Reliability analysis (Table 5) had shown high internal consistency (k=6, Cronbach α=0.89) and a satisfactory factor loadings which implies that it should be kept in their original form. All items had full range of response which implies good sensitivity (Table 6) of a new formed scale. Distribution of results was not normal (Kolmogorov-Smirnov Statistic was significant for all items), which was expected. Means were at higher part of subscales (negative asymmetry) meaning low level of user's information security awareness.

For the third part of UISAQ, Exploratory factor analysis (method principal components) was also appropriate. Analysis had shown extraction of 1 factors and explanation of 45.55 % of overall variance. In table 7 is shown factor structure of the second part of UISAQ which consisted of 5 items that measured the level of user's beliefs about information security and which had a satisfactory factor loadings for all items on one factor.

Reliability analysis (Table 8) had shown lower internal consistency (k=5; Cronbach α=0.60) with two items significantly violating internal consistency (items u7 and u11) so those items were excluded from further analysis and form with 3 items which had high factor loadings and good internal consistency (k=3; Cronbach α=0.76) was kept. All items had full range of response (Table 9) which was a measure of good sensitivity of a new formed scale. Distribution of results was not normal (Kolmogorov-Smirnov Statistic was significant for all items), which was expected. Means were at lower part of subscale (positive asymmetry) meaning high level of user's beliefs about information insecurity.

TABLE VIII. RELIABILITY ANALYSIS: ITEM - TOTAL STATISTICS FOR THE THIRD PART OF UISAQ EXTRACTION

Items	Analysis results			
	Scale Mean if Item Deleted	*Scale Variance if Item Deleted*	*Corrected Item- Total Correlation*	*Cronbach's Alpha if Item Deleted*
u7	8.5564	10.158	.205	.698
u8	9.0977	11.422	.510	.496
u9	9.1880	10.654	.611	.445
u10	8.9699	10.772	.484	.492
u11	9.4511	12.825	.200	.626

TABLE IX. MEASURES OF SENSITIVITY FOR THE THIRD PART OF UISAQ EXTRACTION

Items	Analysis results					
	Min	*Max*	*Range*	*Mean*	*Std. Deviation*	*Test of normality*
u8	1.00	5.00	4.00	2.218	1.003	.188^{a}
u9	1.00	5.00	4.00	2.128	1.040	.233^{a}
u10	1.00	5.00	4.00	2.346	1.175	.197^{a}

a. $p < 0.01$

On the last, fourth part of UISAQ was applied Descriptive statistics as this part consisted of different types of questions with different possible answers. Results (Table 10) showed that all the questions (k=6) in this part of the questionnaire, which had examined issues regarding quality and safety of passwords, had a full range of answers for all items which implies good sensitivity. Although, test of normality of distribution (Kolmogorov-Smirnov Statistic) was significant, normal distribution wasn't significantly violated (asymmetry coefficients Skewness and Kurtosis were not greater than - / + 2).

IV. CONCLUSION

Although this questionnaire requires more work, first results look promising. Results show that UISAQ has potential to become a good and reliable instrument for measurement of users' information security awareness. After validation it may become first international measurement tool of its kind as basis for ongoing professional and scientific research.

With the UISAQ IT professionals will be able to analyze information systems' users in order to identify issues with low security level, while scientists will be able to generally categorize information systems' users regarding level of their information security awareness. By analyzing enough samples of all kinds of information system's users it should be possible to gain some general

TABLE X. DESCRIPTIVE STATISTICS FOR THE FOURTH PART OF UISAQ EXTRACTION

Items	Analysis results					
	Min	*Max*	*Range*	*Mean*	*Std. Deviation*	*Test of normality*
p1	1.00	5.00	4.00	3.531	1.576	.286^{a}
p2	1.00	5.00	4.00	3.712	.993	.250^{a}
p3	1.00	5.00	4.00	2.909	1.723	.274^{a}
p4	1.00	5.00	4.00	2.015	1.680	.452^{a}
p5	1.00	5.00	4.00	3.692	1.201	.187^{a}
p6	1.00	5.00	4.00	2.977	1.479	.216^{a}

a. $p < 0.01$

conclusions about user's potentially risky behavior, correlation with level of security awareness and identification of most insecure kinds of users.

As future work, authors will repeat collecting data analyzing them and that way improving UISAQ as many times as needed in order to develop as-good-as-possible questionnaire. The end of development process should be international validation of this questionnaire.

REFERENCES

[1] M. A. Sasse, S. Brostoffand, and D. Weirich, "Transforming the 'weakest link' - a human/ computer interaction approach to usable and effective security", BT Technology Journal, vol. 19, pp. 122-131, July 2001.

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

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

[4] 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.

[5] M.E. Johnson and S.L. Pfleger, "The Human Side of Risk Management", IEEE Security&Privacy, vol. 9, pp. 51, January-February 2011.

[6] K. D. Mitnick, The Art of Deception - Controlling the Human Element of Security, John Wilwy & Sons, 2002.

[7] 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.

[8] Kim-Kwang and R. Choo, "The cyberthreat landscape: Challenges and future research directions", Compures&Security, vol. 30, pp. 719-731, June 2011.

[9] K. Solic, B. Tovjanin and V. Ilakovac, "Assessment Methodology for the Categorization of ICT System Users Security Awareness", Proc. IEEE 35th MIPRO, pp. 1560-1564, May 2012.

[10] K. Solic, F. Jovic and D. Blazevic, "An Approach To The Assessment Of Potentially Risky Behavior Of ICT System's Users", Technical Gazette, vol. 20, pp. 335-342, February 2013.

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

[12] 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.

[13] Ma 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.

[14] 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.

[15] C. Jackson, Psihologijsko testiranje. Jastrebarsko: Naklada Slap, 2003.

[16] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public", IEEE Security&Privacy, vol. 10, pp. 76-79, March-April 2012.

[17] I. Kirlappos and M.A. Sasse, "Security Education against Phishing: A Modest Proposal for a Major Rethink", IEEE Security&Privacy, vol. 10, pp. 24-32, March-April 2012.

[18] S. Furman, M.F. Theofanos, Yee-Yin Choong and B. Stanton, "Basing Cybersecurity Training on User Perceptions", IEEE Security&Privacy, vol. 10, pp. 40-50, March-April 2012.

[19] K. Solic and I. Horvat, "Weaknesses of global free-of-charge email services – analysis and recommendations", MEDIX, vol. 17, pp. 212-214, December 2011, URL: http://www.kardio.hr/images/stories/medix/m97/212-214.pdf

[20] International ISO/IEC standard 27001, Second edition 2013.10.01, URL: http://www.27000.org/iso-27001.htm

[21] System and Information Integrity family publication, NIST, URL: http://www.nist.gov/publication-portal.cfm

[22] IT Security Guidelines. Federal Office for Information Security, Bonn, Germany, URL: http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/intl.html

[23] ENISA publications, URL: http://www.enisa.europa.eu/publications

[24] CNiL Security of Personal Data. France, URL: http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf