Awareness About Information Security And Privacy Among Healthcare Employees

Šolić, Krešimir; Pleša, Mateo; Velki, Tena; Nenadić, Krešimir

Original article

Awareness About Information Security And Privacy Among Healthcare Employees

Kresimir Solic [1], Mateo Plesa [1], Tena Velki [2], Kresimir Nenadic [3]

[1] Department of Medical Statistics and Medical Informatics, Faculty of Medicine, Josip Juraj Strossmayer University of Osijek
[2] Department of Social Sciences, Faculty of Education, Josip Juraj Strossmayer University of Osijek
[3] Department of Software Engineering, Faculty of Electrical Engineering, Computer Science and Information Technology, Josip Juraj Strossmayer University of Osijek

Corresponding author: Kresimir Solic, kresimir.solic@mefos.hr

Abstract

Aim: The aim of this study was to analyze healthcare employees' knowledge of information security and potentially risky behavior on the Internet considering demographic parameters and in comparison with the standardized behavioral norms among Internet users in Croatia.
Methods: The study was conducted as a cross-sectional study. Healthcare employees from three hospitals in different geographical areas (Osijek, Pula and Zagreb) were included in this study. The validated UISAQ (Users' Information Security Awareness Questionnaire) was used for data collection. The questionnaire contains 33 questions, grouped in two scales and six subscales, and participants were self-evaluated using Likert scale. The time period of data collection was the summer of 2017.
Results: Surveyed healthcare employees show significantly less risky behavior and overall better knowledge than the average Internet user in Croatia. Female participants display online behavior that is less risky than that of the male participants; participants with a university degree are better at PC maintenance, while participants with a high school diploma are more skeptical in regard to loss of personal or professional data. Older people are significantly more careful and lend their access data to other colleagues at work less often.
Conclusion: Healthcare employees included in this study display partially better results than the average Internet users in Croatia when it comes to their knowledge and potentially risky online behavior. However, their average estimations are only partially better than referent estimations and their scores are not very high, especially when it comes to their awareness measured in the "Security in Communications" and "Secured Data" subscales. As there is high risk of losing data because of the nature of business protocols, healthcare employees need more education and training in order for their awareness regarding the importance of information security and privacy to increase.

(Solic K, Plesa M, Velki T, Nenadic K. Awareness About Information Security And Privacy Among Healthcare Employees. SEEMEDJ 2019; 3(1); 21-28)

Received: November 6, 2018; revised version accepted: May 7, 2019; published: May 31, 2019

KEYWORDS: information security, privacy protection, risky behavior, Internet, UISAQ

Introduction

Since the Internet has become an integral part of human life, more and more opportunities are being created, both in the positive sense for the advancement of technology and communication between people as well as in the negative sense, which refers to the existence of risks regarding personal security and privacy. Therefore, there exists a great need to protect personal data in order to reduce the risk of theft of information from users of all age groups, from the youngest to the oldest. New services on the Internet (applications, electronic healthcare, shopping, etc.) that are becoming increasingly necessary and involve more and more users require users to disclose some of their personal information. With this potential risk increasing and seeing as numerous users are ignorant when it comes to the information and communication systems involved, they accept imposed rules and readily start using new services as soon as they appear in the digital market. Since previous research has shown that a person as an information system user may be the most critical security element in said system (1 4), the issue of privacy and user protection will most likely never be solved, even though program security, security procedures and backup automation are at a high level. It is certain that the above is not enough to fully protect the user. Responsibility and conscientious use of Internet services by the user are also required. Therefore, reducing said risk is possible, and one of the best ways of doing so is increasing user awareness by educating them about the various types of unwanted events like frauds and privacy loss on the Internet. For example, installing additional apps or divulging a small piece of personal data may ultimately result in financial or other, less significant loss, which was by no means the intention of the user who installed or provided said information (5).

In general, data protection, not just on the Internet, is carried out in order to prevent data theft or data manipulation. There are two reasons for protecting electronic data: the possibility of their loss and the possibility of unauthorized use of data by an unreliable person with malicious intent. There are several ways to protect data, and the most common one is the use of antivirus programs that protect your computer's operating system from different kinds of malware. Before using the computer's operating system, it is useful to update both the antivirus program and its virus definitions to secure the personal data stored on the computer. Malicious people who want to cause harm to computer users and software or operating system manufacturers tend to do so in order to prove that manufacturers did not create the application, program or operating system with sufficient protection mechanisms. Malicious people do not benefit greatly from developing and producing viruses and other types of malware (6, 7).

Healthcare employees are users and integral parts of a hospital's information and communication system. The Hospital Information System (HIS) is a unique information system within a hospital that combines medical and non-medical data created at various hospital departments for a better and more effective way of exchanging information and more successful way of communicating with patients (8). Modernizing medicine with accessible information technology in patient management systems provides many benefits, but it is possible to manipulate and abuse the privacy. Patient's personal data availability is important to medical staff in order to provide better medical care, healthcare and treatment (9). The protection of personal data, in particular data relating to the health of persons, is primarily carried out with the aim of protecting the right to privacy of personal and family life, which is one of the personal rights protected by our legislation.

Similar empirical studies were conducted on the subject using the UISAQ, but they focused on other groups of Internet users (10 12). The latest study was conducted at the national level as part of the EU project under agreement number INEA/CEF/ICT/A2015/115320. Those results are used as referent values for comparison with results of this study (13).

Therefore, the aim of this study was to analyze knowledge on information security and potentially risky behavior on the Internet among healthcare employees considering demographic parameters and in comparison with the standardized behavioral norms among Internet users in Croatia.

Methods

The authors used the validated Users' Information Security Awareness Questionnaire (UISAQ) for data collection in three Croatian hospitals located in different geographical areas: Osijek, Pula and Zagreb. The data were collected during the summer of 2017. The study was conducted as a cross-sectional study.

The UISAQ has two major scales with three subscales each; each subscale contains five or six items (questions). Associated abbreviations are used in the subsequent text and tables:

• Potentially Risky Behavior (PRB; k = 17)

o Usual Behavior (UB; k = 6)

o Personal Computer Maintenance (PCM; k = 6)

o Access Data Lending (ADL; k = 5)

• Knowledge and Awareness (KA; k = 16)

o Security in Communications (SC; k = 5)

o Secured Data (SD; k = 5)

o Backup Quality (BQ; k = 6)

These subscales describe the user's behavior, knowledge and awareness (5, 11). Participants were asked to estimate how much they agree with a statement on a 5 point Likert type scale, where five means excellent, from the aspect of information security. At the end of the UISAQ, two additional questions about behavioral security of users were given, as well as a section for the provision of demographic data.

Statistical Analysis

The statistical software tool MedCalc 14.12.0 was used for statistical analysis in this paper. Statistical significance, when comparing differences in estimations among groups, was defined as $P < 0.05$ using Student's T-test and one way ANOVA with post hoc Scheffé test. Correlations with age were tested using the Spearman's rank correlation test.

Results

The surveyed healthcare employees were 38.5 ± 11.3 (x ± SD) years old, mostly female (83.8%, $P < 0.001$, Chi-square Test) and mostly with a high school diploma (94.1%, $P < 0.001$, Chi-square Test). Average estimation in the "Usual Behavior" subscale (Student's T-test, $P = 0.03$) was significantly higher for women than for men. There was no significant difference between the genders in the case of other subscales used to describe behavior or the subscales that assess the level of knowledge (Table 1).

Table 1. Gender differences among healthcare employees

Scales and subscales	Arithmetic mean (standard deviation)		P*
	Male (n = 45)	Female (n = 242)	
PRB	3.99 (0.42)	4.03 (0.36)	0.51
UB	4.29 (0.59)	4.48 (0.50)	**0.03**
PCM	3.10 (0.98)	2.92 (0.85)	0.22
ADL	4.59 (0.43)	4.70 (0.38)	0.10
KA	3.10 (0.52)	3.20 (0.50)	0.20
SC	3.16 (0.98)	3.33 (0.83)	0.22
SD	2.12 (0.74)	2.30 (0.86)	0.18
BQ	4.02 (0.80)	4.00 (0.70)	0.86

**Student's T test*

In regard to qualifications, average estimation regarding personal computer maintenance was significantly higher for highly educated participants (one way ANOVA, P = 0.01), while participants with a high school diploma were the group that was most aware of the importance of data protection and of the risk of loss of personal and professional data, money or identity on the Internet (one way ANOVA, P = 0.03), as seen in Table 2.

Table 2. Qualification differences among healthcare employees

Scales and subscales	Arithmetic mean (standard deviation)			P*
	High school diploma (n = 176)	Bachelor's degree (n = 69)	Master's degree (n = 42)	
PRB	4.01 (0.37)	4.02 (0.36)	4.09 (0.39)	0.52
UB	4.47 (0.55)	4.47 (0.49)	4.35 (0.42)	0.43
PCM	2.85 (0.87)	2.99 (0.84)	3.29 (0.88)	**0.01**†
ADL	4.72 (0.39)	4.62 (0.39)	4.61 (0.37)	0.08
KA	3.21 (0.54)	3.16 (0.48)	3.16 (0.41)	0.75
SC	3.29 (0.87)	3.39 (0.81)	3.18 (0.87)	0.46
SD	2.37 (0.90)	2.08 (0.70)	2.14 (0.75)	**0.03**‡
BQ	3.97 (0.77)	4.00 (0.63)	4.16 (0.63)	0.29

*One way ANOVA
†between high school diploma and master's degree (Scheffé test)
‡between high school diploma and bachelor's degree (Scheffé test)

A relatively low, statistically significant positive correlation was found between age and the "Usual Behavior" subscale, meaning that older participants display more secure online behavior on the Internet (Spearman's Correlation Test, rho = 0.29, P < 0.001). Likewise a very low, but statistically significant positive correlation was found between age and the "Access Data Lending" subscale (Spearman's Correlation Test, rho = 0.13, P = 0.03), which mostly means that older participants lend their access data to other colleagues at work less often (Table 3).

Table 3. Age differences among healthcare employees

Scales and subscales	Age of healthcare employees (n = 287)		
	rho	95% CI	P*
PRB	0.09	-0.03 to 0.20	0.13
UB	0.29	0.18 to 0.39	**< 0.001**
PCM	-0.08	-0.20 to 0.03	0.16
ADL	0.13	0.01 to 0.24	**0.03**
KA	0.10	-0.01 to 0.21	0.09
SC	0.03	-0.08 to 0.15	0.58
SD	0.06	-0.05 to 0.18	0.30
BQ	0.10	-0.01 to 0.22	0.09

*Spearman's Correlation Test

Average estimations per scale and subscale are shown in the first column of Table 4. The lowest average estimation for participants was 2.27 ± 0.84 (x ± SD) for the "Secured Data" subscale, which measures awareness of privacy, while the highest average estimation 4.68 ± 0.39 (x ± SD) was for the "Access Data Lending" subscale, which measures risky behavior (Table 4).

Table 4. Differences between healthcare employees and standardized behavioral norms among Internet users in Croatia

Scales and subscales	Arithmetic mean (standard deviation)		P‡
	Healthcare employees (n = 287)	Standardized behavioral norms* (n = 4859)	
PRB	4.03 (0.37)	4.00 (0.42)	0.24
UB	4.45 (0.52)	4.16 (0.59)	**< 0.001**
PCM	2.95 (0.87)	3.27 (0.83)	**< 0.001**
ADL	4.68 (0.39)	4.66 (0.49)	0.50
KA	3.19 (0.51)	3.07 (0.53)	**< 0.001**
SC	3.30 (0.85)	2.93 (0.82)	**< 0.001**
SD	2.27 (0.84)	2.32 (0.87)	0.34
BQ	4.00 (0.72)	3.83 (0.78)	**< 0.001**

*average Internet user in Croatia (25)
‡Student's T test

The results of the comparison between the surveyed healthcare employees and the standardized behavioral norms among Internet users in Croatia collected in a national project (N = 4859) show statistically significant differences for the majority of the subscales, often in favor of healthcare employees (Table 4). The surveyed healthcare employees achieved better results in the "Usual Behavior" subscale (Student's T test, $P < 0.001$), in the "Security in Communications" subscale (Student's T test, $P < 0.001$), and in the "Backup Quality" subscale (Student's T test, $P < 0.001$). They achieved better results in the overall "Knowledge and Awareness" scale (Student's T test, $P < 0.001$), but significantly worse results in the "Personal Computer Maintenance" subscale (Student's T test, $P < 0.001$).

Discussion

Analysis of the results has shown that healthcare employees included in this study are statistically better than the average Internet user in Croatia when it comes to their knowledge about digital security and their potentially risky online behavior. However, their average estimations per scale and subscale are better than referent estimations only in part and are not very high, especially when it comes to awareness measured in the "Security in Communications" and "Secured Data" subscales.

Female users are the most skeptical of the surveyed healthcare employees, so they are more careful in their online behavior. The results were similar for older participants. Both results are in accordance with previous studies based on the same questionnaire (11, 12).

The results that show that participants with a high school degree are the most skeptical in regard to data protection and the risk of loss of personal and professional data, money or identity on the Internet are also partially in accordance with those of previous studies. On the other hand, participants with higher education achieved better results when it comes to their personal computer maintenance.

Hospitals' business information systems include both business and private data, i.e. digital data about healthcare processes and patients' private information. Since the user is often the weakest element of the information and communication system when it comes to data protection (1 4), healthcare employees have an obligation to be familiar with and behave in accordance with security protocols at their workplace. Employees typically need additional education courses organized by their institution and alert messages sent on a regular basis by system administrators (14 17) in order to acquire better knowledge regarding security threats and to increase their own awareness regarding the importance of information security for the system, for the patients and for themselves (18, 19).

Some general recommendations for more secure behavior on the Internet that may help healthcare employees and all other Internet users are presented below (13):

- Limit posting personal data on the Internet because what is once posted on the Internet remains permanently recorded!
- Different systems are not equally secure or equally dangerous; you should exercise increased caution in an unknown setting!
- User access data are personal and they are used to verify identity on the Internet. They should be handled with extreme caution because they represent the electronic identity of a user. Users should know that NO ONE should EVER request that he/she disclose their access data, neither a system administrator nor a bank clerk!
- The Internet is similar to the real world and public spaces. Maintain a healthy dose of mistrust when communicating with strangers ¬– creating a fake identity on the Internet is much simpler than in the real world!
- Keep your operating systems, applications you use, and particularly antivirus protection up to date, both on personal and portable devices, as well as on mobile phones.

- Back up important documents and files periodically and copy them to another location, removed from the original data.

- Try to differentiate business communication from private communication.

- A high-quality password significantly increases the level of security. Use a combination of capital and small letters, numbers and special characters.

Some limitations of this study are the relatively small number of healthcare employees surveyed in only three hospitals. In addition, the participants were compared to standardized behavioral norms in Croatia. However, those referent values do not refer to secure behavior and extensive knowledge of data protection, but to the average Internet user. In a future research, a comparison is planned between healthcare employees and different target-groups, such as students, employees in the government sector or in the banking sector.

As there exists a high risk of data loss because of the nature of business protocols, healthcare employees need more education and training in order for their awareness regarding the importance of information security and privacy to increase.

Acknowledgment (Funding):

This paper was financed by the Croatian Government Office for Cooperation with NGOs and co-financed by the European Union's Connecting Europe Facility, under the project named "Safer Internet Centre Croatia: Making internet a good and safe place", Agreement Number: INEA/CEF/ICT/A2015/115320.

The sole responsibility of this publication lies with the authors. The European Union is not responsible for any use that may be made of the information contained therein.

References

1. Solic K, Ilakovac V. Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study. Med Glas (Zenica) 2009; 6: 261 4.

2. Sasse MA, Brostoffand S, Weirich D. Transforming the 'weakest link' - a human/ computer interaction approach to usable and effective security. BT Technology Journal 2001; 19: 122 31.

3. Solic K, Sebo D, Jovic F, Ilakovac V. Possible Decrease of Spam in the Email Communication. Proceedings of the 34th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2011. p. 170 3.

4. Thompson H. The Human Element of Information Security. IEEE Security & Privacy 2013; 11: 32-5.

5. Velki T, Solic K, Nenandic K. Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). Psihologijske teme 2015; 24: 401-24.

6. James FK, Keith WR. Computer Networking: A Top-Down Approach. 5. ed. Addison Wesley: University of Massachusetts Amherst, 2007.

7. Varga M. Zaštita elektroničkih podataka. Tehnički glasnik 2011; 5: 61-73.

8. Vukovic D. Uvođenje integriranog bolničkog informacijskog sustava. MEDIX 2004; 54/55: 104-6.

9. Petric S. Građanskopravna odgovornost zdravstvenih djelatnika. Zbornik Pravnog fakulteta Sveučilišta u Rijeci 2005; 26: 81-145.

10. Velki T, Solic K, Gorjanac V, Nenadic K. 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

(MIPRO), Opatija, Croatia, 2017. p. 1496 500.

11. Velki T, Solic K, Ocevcic H. Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work. Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2014; p. 1564 8.

12. Solic K, Velki T, Galba T. Empirical study on ICT system's users' risky behavior and security awareness. Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2015; p. 1623 6.

13. Velki T, Solic K. Priručnik o informacijskoj sigurnosti i zaštiti privatnosti. Osijek: Fakultet za odgojne i obrazovne znanosti, 2018 (u tisku).

14. Mitnick KD, Simon WL, Wozniak S. The Art of Deception: Controlling the Human Element of Security, Indiana: John Wiley & Sons, 2002.

15. Kirlappos I, Sasse MA. Security Education against Phishing: A Modest Proposal for a Major Rethink. IEEE Security & Privacy 2012; 10: 24-32.

16. Furman S, Theofanos MF, Choong Yee-Yin, Stanton B. Basing Cybersecurity Training on User Perceptions. IEEE Security & Privacy 2012; 10: 40-50.

17. Galba T, Solic K, Lukic I. Towards Information Security and Privacy Self Assessment (ISPSA) Tool for Internet Users. Acta Polytechnica Hungarica 2015; 12: 149 62.

18. Beckers K, Pape S, Fries V. HATCH: Hack and Trick Capricious Humans - A Serious Game on Social Engineering. Proceedings of the 30th International BCS Human Computer Interaction Conference (HCI 2016) Bournemouth University, Poole, UK, 2016; p. 11 5.

19. Da Veiga A. An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA) Lesvos, Greece, 2015; p. 95 107.