User Risky Behavior and Security Awareness through Lifespan

Velki, Tena; Romstein, Ksenija

Source / Izvornik: **International journal of electrical and computer engineering systems, 2019, 9, 9 - 16**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:141:663769

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

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



Repository / Repozitorij:

FOOZOS Repository - Repository of the Faculty of Education





User Risky Behavior and Security Awareness through Lifespan

Preliminary Communication

Tena Velki
Faculty of Education,
J. J. Strossmayer University of Osijek,
tena.velki@gmail.com

Ksenija Romstein
Faculty of Education,
J. J. Strossmayer University of Osijek,
kromstein@foozos.hr

Abstract – *In the last decade, the Internet has become a crucial part of human life. Everyday usage of the Internet has enabled rapid development of social engineering. The weakest link in this chain are naive users with their risky online behavior who are unaware of Internet security risks. As knowledge, awareness and behavior depend on human characteristics, such as maturity, age and education, the main goal of this study was to investigate trendlines of user risky behavior and security awareness through the lifespan. Results have shown the growth of online risky behavior through the lifespan and the growth of knowledge and security awareness in middle adulthood. In general, we can conclude that people who are more knowledgeable about and more aware of potential security risks are at the same time more prone to risky behavior when using information systems.*

Keywords – *information security, security awareness, user risky behavior*

1. INTRODUCTION

The omnipresence of the Internet in everyday life has led to the emergence of the virtual world becoming more and more part of the real world or reality, i.e., the clear boundaries between the virtual and the real world are lost. It increasingly encompasses the existing real world and as such inputs in all areas of human life where today's contemporary life becomes unthinkable without using the Internet in our everyday life. This change in modern society, where activities move from the real to the virtual world, enables both rapid development of social engineering and the development of Internet fraud and deception focused on a naive user [1, 2].

From an early age, children, adolescents and adult people use the Internet for education, work, fun, etc. Proper use of the Internet is necessary in terms of information security. Children start using the Internet early in their childhood, i.e., children aged 3 or 4 use the Internet on iPads, their parents' smart phones, etc. [3]. The critical period for becoming a victim of social engineering attacks is the age of adolescence. Adolescents are at risk of developing various inappropriate behaviors, both in real life and especially in virtual reality. In the virtual world, there is no actual control over their behavior. In comparison with the virtual world, in the real world adolescent problem behavior is supervised and controlled by parents and teachers, and furthermore, control and monitoring of their behavior are usually subject to arguments with parents and teachers. The non-existent boundaries on the Internet make adolescents the most vulnerable group [4, 5]. Previous studies have shown a positive correlation between real-world risk and delinquent behavior and risky online behavior of adolescents [6, 7].

One of the major problems in research is the definition of risk behavior. Although it seems that risk behavior is a clear construct, the presence of individual perspective on risk behavior influences one's behavior [8]. Also, researchers are inconsistent when using terms such as safety, security and risk behavior, which may lead to differences in methodologies and results.

Studies have suggested that children in the European Union encounter virtual reality pretty early, under the age of 5. More than 75% of children aged 7-18 use the Internet up to 4 hours a day, increasing several risks such as cyberbullying, grooming and offline meetings [8, 9]. These risk behaviors switch the focus from basic ICT competencies to more advanced competencies of cyber security for teachers, suggesting that teachers should get an opportunity for lifelong learning in this particular area.

In the last two decades, studies have clearly shown that a computer user, or a human component, is the weakest link in information security [10, 11]. Informa-

tion system users with their unintentional and risky behavior can have a significant impact on the entire information security system. However, there is still scarcity of scientific research in this area [12, 13]. Most of research is mainly concerned with the quality and strength of the user's computer user password [14-17], while security awareness and user risky behaviors remain the main information security problem [7, 18].

1.2. AGE DIFFERENCES IN SECURITY KNOWLEDGE AND USER BEHAVIOR

European research referring to online behavior among children and young people reveals several interesting facts, e.g.: children aged 7 to 18 use the Internet up to 4 hours a day, mostly unattended. Parents use the Internet simultaneously with their children – 75% of children and 84% of parents use the Internet at the same time. Children get access to the Internet pretty early – under the age of 3, starting from 30 minutes a day, which is then increased to up to 3-4 hours a day for 6-year-old children. By the age of 11, over 80% of children use the Internet on a daily basis at home [8, 9]. Internet access at school is limited due to curricula and teaching activities. If the Internet is used at school, access is usually limited to 30 minutes a day and the activities are always incorporated into the teaching process. This means that parents, rather than teachers, should raise their awareness of an adequate approach to the Internet and online media at home. It is hard to find research on online safety in adulthood as risk stops after the age of 18. Instead, most research indicates adolescent years as the last period for risk behavior focusing on explicit contents. Further research on risk behavior in adulthood should also be addressed as part of awareness raising among the general public.

Most common risk behaviors among children aged 7 to 18 include giving away personal data (name, surname, address, etc.), and revealing passwords and usernames to unknown persons online, accepting friendships and messages from unknown persons online and arranging offline meetings without parental knowledge [8]. Parental non-involvement in child online safety contributes to rather late disclosure of problems - children's perspective on assessment of risk behavior is rarely discussed at home, and in school, it is often oriented towards safeguarding private data such as name, surname, passwords, etc., while other forms of online risk behaviors are not implemented in school curricula [9].

These results indicate that children are insufficiently protected online, which should be given more attention in further research and practice.

Although cyber and internet security in early years and childhood is a well-known problem to researchers, Croatia has never participated in this kind of survey. This is the first study in Croatia about security awareness and user risky behavior, which has revealed disturbing information. More than 30% of employees voluntarily revealed their official e-mail passwords to researchers [17]. Even more disturbing data was obtained in relation to high-school students, 78% of whom have revealed their private e-mail passwords to researchers [18]. Compared to lower-grade employees (high-school graduates), employees with a higher level of education (university education) were more reliable. In general, people who did not reveal their password showed greater knowledge of information security and less risky behavior [17]. Compared to adult employees, high-school students have shown more risky online behaviors, more problematic online communication, and rare backup of computer data, but they have shown better knowledge regarding information security awareness, i.e., greater awareness of data theft and abuse [18]. In comparison to younger people (under 30 years of age), older employees showed greater overall knowledge of information security and less risky behavior [17], while compared to employees, students maintained their computers better, but were at the same time reluctant and practiced more risky online communication [7]. Another study shows a statistically significant correlation between the information security scales and the scales of risk behavior of computer users, where persons with higher knowledge who are more aware of potential security risk at the same time behave in a more risky manner as information system users [18]. Also, some recent research has shown that awareness itself and awareness of information security are insufficient for a person to behave accordingly, even among highly educated university professors [19, 20].

In this paper, the authors analyze empirical data collected on a national sample in order to investigate a trendline of user risky behavior and security awareness through the lifespan. The initial premise is as follows: a person as a user of an information system with potentially risky behavior can influence directly data security and indirectly the overall security of the information system. However, its impact on information security depends on a person's maturity, knowledge and responsibility. Different participant age groups as well as different life periods will have a great influence on their online risky behavior and security knowledge. The youngest age group in the study is made up of adolescents as they are at a greater risk of inappropriate online behavior. The oldest group consists of working adults (older adults before retirement) as they are at a greater risk of security awareness and knowledge.

2. METHOD

2.1. SAMPLE

The national sample was used (N=4859). Most of the participants come from northwestern and central Croatia (N=2064), eastern Croatia (N=1690), then Dalmatia (N=741) and the smallest number of participants comes from Istria (N=364), which is shown in Fig. 1. Participants were high-school students (N=3250), college students (N=883) and employees (N=726) from Croatia, with ages ranging from 14 to 65 years (M=20.78 ± 9.515). A detailed classification of age groups is shown in Table 1.

2.2. INSTRUMENT AND PROCEDURE

Data was collected during 2017. Headmasters and directors of institutions (schools, faculties and corporations) were contacted and asked for permission to collect data on their students/employees. When they gave informed consent for the study, they were sent a link with questionnaires for participants to fill in.

Table 1. Age of participants included in the study divided into groups.

Participants	N	Mean Age	Min.	Max.
High-school students				
Group 1 1st and 2nd grade	2199	15.65 ± 0.679	14	18
Group 2 3rd and 4th grade	1051	17.47 ± 0.665	16	20
Total	3250	16.24 ± 1.083	14	20
College students				
Group 3 1st, 2nd and 3rd year of college (undergraduate study)	740	21.51 ± 4.385	18	53
Group 4 4th, 5th, 6th and 7th year of college (graduate study)	143	24.06 ± 2.981	19	38
Total	883	21.93 ± 4.291	18	53
Employees				
Group 5 Young employees (age 17 to 29)	148	24.94 ± 3.357	17	29
Group 6 Middle age employees (age 30 to 49)	400	38.28 ± 5.591	30	49
Group 7 Older employees (age 50 to 65)	170	55.09 ± 3.760	50	65
Total	726	39.68 ± 11.255	17	65
Total	**4859**	**20.78 ± 9.515**	**14**	**65**

For research purposes, the Users' Information Security Awareness Questionnaire (UISAQ) was used, which measures the level of users' security awareness and their potentially risky behavior [21, 22]. UISAQ (k=33) is divided into two scales: the scale of computer users' potentially risky behavior (k=17), [split into three subscales: the subscale of computer users' usual behavior (e.g., leaving your personal data on social networks; k=6), the subscale of personal computer system maintenance (e.g., using different passwords for different systems, like using one password for Facebook and another one for an e-mail account; k=6) and the subscale of access data lending (e.g., lending your credit card PIN to friends and family members; k=5)] and the scale of information security knowledge (k=16) [also split into three subscales: the subscale of the level of communication security (e.g., how secure is communication through social networks like Facebook and Twitter; k=5), the subscale of belief in data security status (e.g., how much you believe in risk that someone will steal the money from your online bank account; k=5) and the subscale of the importance of backup (e.g., how much it is important to back up your data to another location, e.g. external hard disk; k=6)]. Internal consistency for UISAQ scales and subscales was Cronbach's α = 0.66 – 0.88.



Fig. 1. Distribution of the national sample of participants

3. RESULTS AND DISUCUSSION

Empirical data were tested by using trend analyses. The arithmetic means used for analyses are shown in tables 2 and 3.

Table 2. Means and standard deviations for UISAQ Scale Potentially Risky Behavior and its subscales (Lending Access Data, Personal Computer Maintenance & Usual Risky Behavior).

Participants		Mean	Min.	Max.
Potentially Risky Behavior				
High-school students	Group 1	3.95 ± 0.417	1.00	5.00
	Group 2	3.97 ± 0.415	1.41	5.00
College students	Group 3	4.05 ± 0.421	2.47	4.94
	Group 4	4.11 ± 0.409	2.65	4.94
	Group 5	4.06 ± 0.429	2.41	4.82
Employees	Group 6	4.12 ± 0.384	2.85	4.94
	Group 7	4.13 ± 0.358	3.00	4.88
Total		3.99 ± 0.417	1.00	5.00
Lending Access Data				
High-school students	Group 1	4.67 ± 0.508	1.00	5.00
	Group 2	4.67 ± 0.473	1.00	5.00
College students	Group 3	4.62 ± 0.512	1.80	5.00
	Group 4	4.58 ± 0.554	1.80	5.00
	Group 5	4.56 ± 0.583	1.00	5.00
Employees	Group 6	4.72 ± 0.371	2.80	5.00
	Group 7	4.79 ± 0.329	3.20	5.00
Total		4.67 ± 0.491	1.00	5.00

Personal Computer Maintenance				
High-school students	Group 1	3.20 ± 0.851	1.00	5.00
	Group 2	3.25 ± 0.763	1.00	5.00
College students	Group 3	3.42 ± 0.783	1.00	5.00
	Group 4	3.56 ± 0.762	1.00	5.00
	Group 5	3.44 ± 0.866	1.00	5.00
Employees	Group 6	3.37 ±0.839	1.00	5.00
	Group 7	3.13 ± 0.912	1.00	5.00
Total		3.27 ± 0.828	1.00	5.00
Usual Risky Behavior				
High-school students	Group 1	4.11 ± 0.624	1.00	5.00
	Group 2	4.09 ± 0.597	1.00	5.00
College students	Group 3	4.20 ± 0.535	1.83	5.00
	Group 4	4.27 ± 0.478	2.00	5.00
	Group 5	4.25 ± 0.577	1.00	5.00
Employees	Group 6	4.36 ± 0.507	1.50	5.00
	Group 7	4.57 ± 0.420	2.33	5.00
Total		4.16 ± 0.594	1.00	5.00

Table 3. Means and standard deviations for UISAQ Scale Knowledge and Awareness and its subscales (Communication Security, Secure Data & Backup Quality).

Participants		Mean	Min.	Max.
Knowledge and Awareness				
High-school students	Group 1	3.02 ± 0.538	1.00	5.00
	Group 2	3.07 ± 0.524	1.25	5.00
College students	Group 3	3.09 ± 0.519	1.66	4.83
	Group 4	3.04 ± 0.510	1.70	4.45
	Group 5	3.04 ± 0.475	1.44	4.08
Employees	Group 6	3.24 ± 0.483	1.93	4.83
	Group 7	3.19 ± 0.497	1.76	4.75
Total		3.07 ± 0.527	1.00	5.00
Communication Security				
High-school students	Group 1	2.81 ± 0.771	1.00	5.00
	Group 2	2.90 ± 0.808	1.00	5.00
College students	Group 3	3.03 ± 0.823	1.00	5.00
	Group 4	2.99 ± 0.819	1.40	5.00
	Group 5	2.98 ± 0.898	1.00	5.00
Employees	Group 6	3.23 ± 0.833	1.00	5.00
	Group 7	3.20 ± 0.883	1.00	5.00
Total		2.93 ± 0.815	1.00	5.00
Secure Data				
High-school students	Group 1	2.36 ± 0.930	1.00	5.00
	Group 2	2.30 ± 0.917	1.00	5.00
College students	Group 3	2.36 ± 0.773	1.24	4.44
	Group 4	2.20 ± 0.779	1.24	4.44
	Group 5	2.21 ± 0.753	1.00	4.80
Employees	Group 6	2.24 ± 0.742	1.00	5.00
	Group 7	2.18 ± 0.658	1.00	4.40
Total		2.32 ± 0.873	1.00	5.00
Backup Quality				
High-school students	Group 1	3.77 ± 0.856	1.00	5.00
	Group 2	3.86 ± 0.777	1.00	5.00
College students	Group 3	3.78 ± 0.690	1.00	5.00
	Group 4	3.80 ± 0.677	1.00	5.00
	Group 5	3.87 ± 0.682	1.00	5.00
Employees	Group 6	4.07 ± 0.553	2.00	5.00
	Group 7	4.03 ± 0.594	1.33	5.00
Total		3.83 ± 0.780	1.00	5.00

Polynomial regression analysis was carried out to predict a trendline in users' potentially risky behavior (Fig. 2). The results show that a polynomial function of 5th degree ($y = -0.0016x^5 + 0.0338x^4 - 0.2633x^3 + 0.9273x^2 - 1.3882x + 4.6441$) describes data very well ($R^2 = 0.9611$).

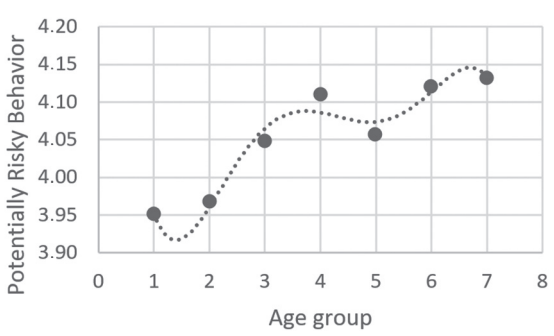


Fig. 2. Trendline for Potentially Risky Behavior scale results

Risky online behavior is on the rise in the period of adolescence reaching the peak at the end of formal education (i.e. final years at college). A slight decline in online risky behavior has been noticed in the period of the transition to adulthood and entering the labor market. Although these two groups are almost of the same age (group 4 students with M=24.06 and group 5 employees with M=24.94), a shift in data is probably a reflection of maturity and greater responsibility when a person enters the labor market. Other reasons could be social conformity and solid knowledge of desirable online behavior for this age group. Adults probably do not want to reveal forms and extent of risk behavior, or they feel quite confident in their ICT competencies. Results referring to senior citizens speak in favor of the aforementioned. A slight growth in risky online behavior is also noticed in adulthood (from entry into the labor market to retirement), which is probably due to lack of knowledge of potential online risks within older age groups. It is important for all information system users to recognize their own risky online behaviors and try to minimize them as much as possible.

The same analyses were done for all three subscales of potentially risky behavior to examine this problem in detail. The forth degree polynomial function or a quartic polynomial ($y = -0.0025x^4 + 0.0444x^3 - 0.2463x^2$

+ 0.4801x + 4.3928) described the given data for the Lending Access Data subscale best ($R^2 = 0.9387$), which is shown in Figure 3.

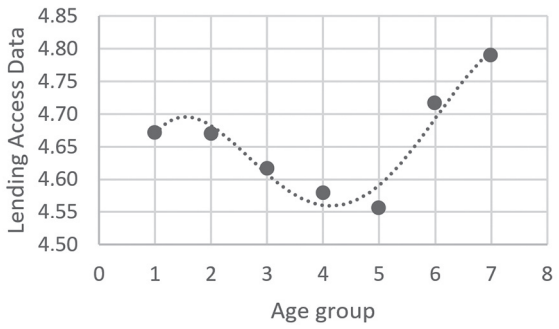


Fig. 3. Trendline for Lending Access Data subscale results

By growing up and gaining more experience with social engineering adolescents realize that lending access data can harm their privacy, so it has been noticed that this type of risky behavior decreases in this period. This trend continues in young adulthood, but in middle- and older age adult group lending access data increases with the peak in the oldest group, probably because of the same reason shared by all online risky behaviors in this age group, i.e., unawareness of risks. Lending any access data (referring to private or business e-mail accounts or the PIN of your credit card) to friends and family members significantly increases the chance of stealing your personal data that should be known only to you.

A polynomial function of 4th degree describes best trends in computer maintenance, too ($y = 0.0031x4 - 0.0551x3 + 0.2948x2 - 0.4707x + 3.4202$; $R^2 = 0.9617$). Problems with personal computer maintenance are on the rise through the period of adolescence, reaching the peak at the end of formal education, and decreasing with age, showing that members of the oldest age group have the least difficulty (Fig. 4).

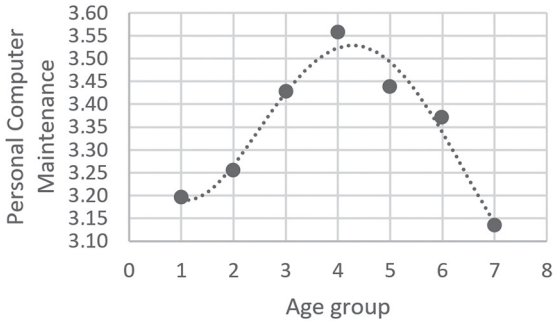


Fig. 4. Trendline for Personal Computer Maintenance subscale results

Students show least concern about maintenance of computers that are used on a daily basis. For high-school students, computer maintenance is an integral part of the school curriculum and it is no surprise that the highest maintenance rate is recorded in this group. It is possible that the oldest employees have computer experts in their corporation so these experts take cake care of computer maintenance instead of them. Regular update of anti-spyware, antivirus programs and an operating system is very important safe computer usage. New malware grows exponentially every day and the best and most effective way to protect the security of your computers is to maintain them properly and regularly.

The last subscale, Usual Risky Behavior (Fig. 5), data are described best by the quadratic polynomial function ($y = 0.0116x^2 - 0.0221x + 4.1192$; $R^2 = 0.9305$).

The results have shown almost a linear trend through the lifespan, showing usual risky behavior (e.g., opening e-mails from unauthorized or unknown sources, sending chain messages, etc.) increases with age.

Although it may be expected that, due to their development age and stage, adolescents show the most risky online behaviors, they are actually a group familiar with various information systems from their earliest days (e.g., smartphones, tablets, laptops) and with most direct experience in using different applications (e.g., social networks, communication applications, etc.) as well as other programs (e.g., various antivirus programs, etc.), which enables better management of information systems on an everyday basis. The best advice is: if you are not sure who has sent you an e-mail or what has been attached to your e-mail, just do not open it. Ask experts for information to be sure that your e-mails are not unwanted or potentially harmful.

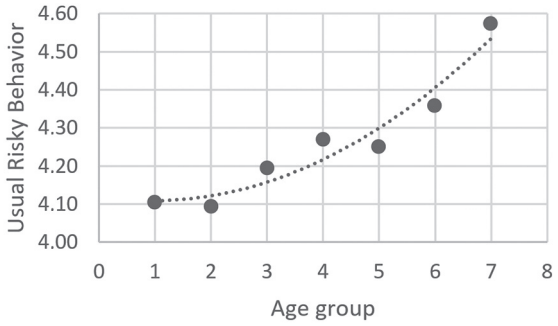


Fig. 5. Trendline for Usual Risky Behavior subscale results

Prediction of the level of knowledge and security awareness through the lifespan is also examined by means of polynomial regression analysis (Fig. 6). The trend was best described by a polynomial function of 5th degree ($y = -0.0058x^5 + 0.1115x^4 - 0.7798x^3 + 2.4428x^2 - 3.2678x + 4.305$; $R^2 = 0.9973$).

During the adolescent period, there is a growth in knowledge and security awareness, which is a reflection of formal education, high-school and college curricula. The transition from adolescence to early adulthood is marked by a decrease in knowledge and secu-

rity awareness, which is not expected. Maybe because of everyday usage of the Internet young adults did not become aware of potential online risks. Doing the same thing over and over makes people feel more safe and secure than they really are, not thinking about possible risks. In middle adulthood, people are most aware of potential online risks probably due to job requirements, and with older adults there is a decline in knowledge and awareness because Internet usage is not the primary issue for them like for younger people. It is important to remember that is not enough to know something but also to behave in accordance with that knowledge.

Detailed analyses were also carried out on all three subscales of the Knowledge and Awareness Scale.

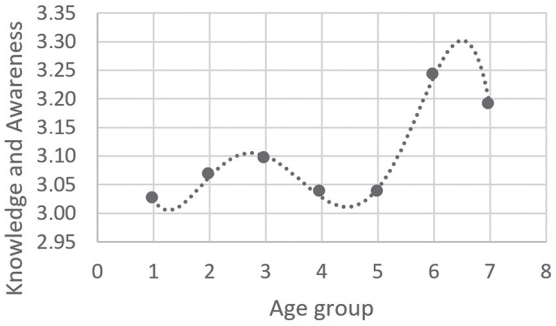


Fig. 6. Trendline for Knowledge and Awareness Scale results

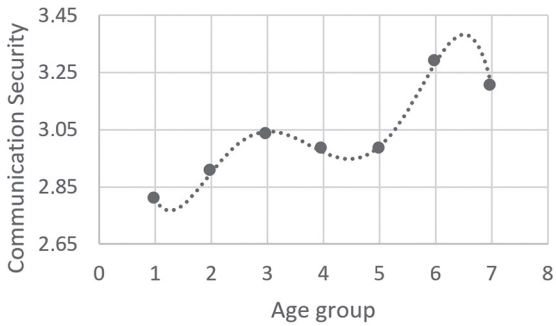


Fig. 7. Trendline for Communication Security subscale results

Almost the same trendline was obtained for the Communication Security subscale (Fig. 7) with a polynomial function of 5th degree ($y = -0.0058x5 + 0.1115x4 - 0.7798x3 + 2.4428x2 - 3.2678x + 4.305$; $R^2 = 0.9973$).

Through the age of adolescence there is a growth in secure online communications with a slight decline in young adulthood, probably because they think they are secure since they are aware of potential risks, but they do not behave accordingly. The peak of secure communication is reached in middle adulthood, which is the most responsible period of life (people between 30 and 50 are usually married, have children, care about older family members, have carriers, etc., which makes them more responsible and aware of risks), and then it declines slightly again within the older age group. Online communication is actually similar to face-to-face communication; if you do not know the person and their intentions, you do not communicate with them. In real life, we learned not to talk to strangers, the same advice also holds true for the online world.

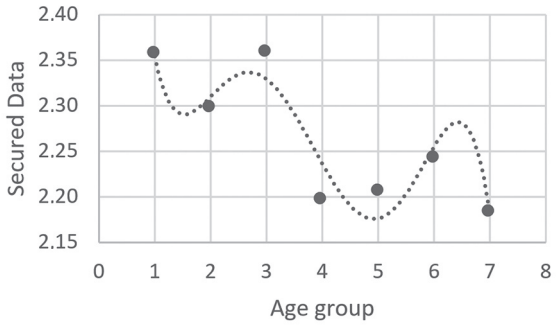


Fig. 8. Trendline for Secure Data subscale results

A polynomial function of 5th degree ($y = -0.003x^5 + 0.0583x^4 - 0.4179x^3 + 1.3505x^2 - 1.9529x + 3.3192$; $R^2 = 0.8886$) best describes a trendline referring to belief in computer data safety (Fig. 8).

Adolescents are more convinced that online abuse of data is possible (e.g., unauthorized disclosure, identity theft or stealing personal data like bankcard numbers, etc.), probably because they were victims of such abuse or know personally someone who was. Young adults are not very much convinced that something like that can happen to them and there is only a slight increase in this attitude. The oldest age group is least convinced that online abuse of data could happen to them, probably because they usually do not give away personal information online or use online services such as Internet banking or online shopping. Stealing and abuse of personal online data has the same consequences as abuse and misuse of your personal data in the real world. Money can be withdrawn from a user's bank account, someone can steal their identity or burglarize a house while there are away on vacation. Be careful with information that you put online.

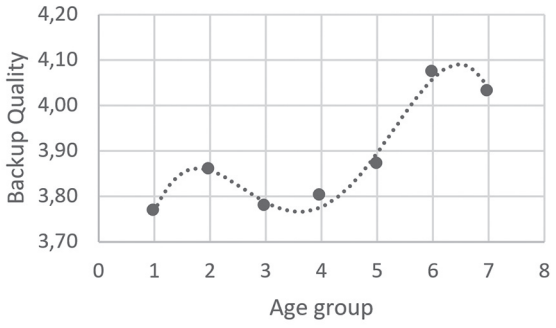


Fig. 9. Trendline for Backup Quality subscale results

A trendline similar to the Knowledge and Awareness Scale was also obtained for the Backup Quality subscale (Fig. 9). A quartic polynomial function best

describes data ($y = -0.0063x^4 + 0.0999x^3 - 0.522x^2 + 1.0531x + 3.1405$; $R^2 = 0.9851$).

As far as the importance of backup quality or proper data storage is concerned, growth has been recorded through the lifespan with a small positive peak at the end of high school, probably due to the final seminar and the state graduation exam (the so-called matura), which is very important to this specific group of participants. During the whole adulthood, proper data storage is necessary for daily work and activities. More responsibilities, both at work and in life, increases the perception of how important it is to keep the data safe on a daily basis. A slight decline in backup quality has been noticed with the oldest age group due to lack of knowledge in this growing field. Although we usually do not have much time to check memory sticks for viruses, or we are lazy to periodically change our passwords, once we lose our data or they become corrupted, it can be too late.

4. CONCLUSION

In general, we can conclude that user risky behavior increases with the age and the level of security awareness and knowledge, which is also in accordance with previous research stating that people who have a lot of knowledge and are more aware of potential security risks are at the same time more prone to risky behavior when using information systems [18]. Knowledge and education are obviously not the primary factor in protecting people from risky online behavior.

Furthermore, results obtained for some subscales were unexpected. It can be concluded that the age and the period of life (high-school students, college students and employees) is not the primary factor influencing the level of user risky behavior and security awareness as we could see that two same age groups (group 4 and group 5) have different results on some subscales due to their different life periods (students vs. employees). Some other participant characteristics could be more important for predicting trends in risky behavior and security risks, like formal education of employees, a field of education (i.e., technical fields vs. humanities), additional education in the informatics area, job requirements or Internet traffic. Comparing children- and adults-related data, it is obvious that the age and life-style can contribute to risky online behaviors. Bearing in mind the possibility of social conformity of adults in this survey, stakeholders and academic community should cooperate more closely in the field of cyber security through lifelong learning courses. Future studies should take into account this potential difference in testing predictions and trends in user risky behaviors and security awareness.

5. ACKNOWLEDGEMENTS

This work is financed by the Croatian Government Office for Cooperation with NGOs and co-financed by the European Union's Connecting Europe Facility, under project named "Safer Internet Centre Croatia: Making the 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.

6. REFERENCES:

[1] K. Haley, Information robbery - The 2011 Internet security threat report, http://www.infosectoday.com/Articles/Information_ Robbery.htm (accessed: 2018)

[2] K. D. Mitnick, W. L. Simon, S. Wozniak, "The art of deception: Controlling the human element of security", Wiley Publishing, Inc., 2002.

[3] M. Dinleyici, K. B. Carman, E. Ozturk, F. Sahin-Dagli, "Media Use by Children, and Parents' Views on Children's Media Usage", Interactive Journal of Medical Research, Vol. 5, No. 2, 2016, pp. e18.

[4] E. Burgess Dowdell, "Risky internet behaviors of middle-school students: communication with online strangers and offline contact", CIN: Computers, Informatics, Nursing, Vol. 29, No. 6, 2011, pp. 352-359.

[5] J. Suler, "The Online Disinhibition Effect", Cyberpsychology & Behavior, Vol. 7, No. 3, 2004, pp. 321-325.

[6] D. B. Branleya, J. Coveyb, "Is exposure to online content depicting risky behavior related to viewers' own risky behavior offline?", Computers in Human Behavior, Vol. 75, 2017, pp. 283-287.

[7] T. Velki, K. Šolić, K. Nenadić, "Development and Validation of Users' Information Security Awareness Questionnaire (UISAQ)", Psychological Topics, Vol. 24, No. 3, 2015, pp. 401-424.

[8] European Union Agency for Network and Information Security/ENISA, "Roadmap for NIS Education Programs in Europe", Madrid, ENISA, 2014.

[9] S. Livingstone, L. Haddon, "EU Kids Online: Final report", 2009, http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf (accessed: 2018)

[10] S. J. Lukasik, "Protecting Users of the Cyber Commons", Communications of the ACM, Vol. 54, No. 9, 2011, pp. 54-61.

[11] 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.

[12] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, "Future directions for behavioral information security research", Computers & Security, Vol. 32, No. 1, 2013, pp. 90-101.

[13] K. Kwang, R. Choo, "The cyber threat landscape: Challenges and future research directions", Computers & Security, Vol. 30, No. 8, 2011, pp. 719-731.

[14] M. Dell'Amico, P. Michiardi, Y. Roudier, "Password Strength: An Empirical Analysis", Proceedings of the 29th IEEE International Conference on Computer Communications, San Diego, California, 15-19 March 2010, pp. 1-9.

[15] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, J. Lopez, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms", Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, California, 22-23 May 2012, pp. 523-537.

[16] A. G. Voyiatzis, C. A. Fidas, D. N. Serpanos, N. M. Avouris, "An Empirical Study on the Web Password Strength in Greece", Proceedings of the 15th Panhellenic Conference on Informatics, Kastoria, Greece, 30 September - 2 October 2011, pp. 212-216.

[17] M. A. Wanli, J. Campbell, D. Tran, D. Kleeman, "Password Entropy and Password Quality", Proceedings of the 4th International Conference on Network and System Security, Melbourne, Australia, 1-3 September 2010, pp. 583-587.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] K. Šolić, K. Grgić, V. Ilakovac, D. Žagar, "Usage of insecure E-mail services among researchers with different scientific background", Medicinski Glasnik, Vol. 8, No. 2, 2011, pp. 273-276.