Edita Butrimė, Vaiva Zuzevičiūtė

Students’

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 23, 46-55

2016

Kultura Bezpieczeństwa
Nauka – Praktyka – Refleksje
Nr 23, 2016 (46–55)

STUDENTS' / FUTURE LAW-ENFORCEMENT OFFICERS' PERSPECTIVE ON SAFETY IN THE DIGITAL SPACE

EDITA BUTRIMĖ, VAIVA ZUZEVIČIŪTĖ
Faculty of Public Security, Mykolas Romeris University, Lithuania

Abstract

Main purpose of article was to investigate the degree to which students: future law-enforcement officers, who will be obliged to provide security for other people, think about their own/personal safety in digital space. The paper presents both theoretical considerations and empiric data from a study, dedicated to investigating whether future law-enforcement students recognize the main dimensions of safety in digital space, because so much of contemporary social, personal and professional life is being carried out in digital spaces. If future law-enforcement officers are unable recognize the dimensions of safety, they, as a consequence, will not be professional enough to consult and to provide support to citizens on the issues that start in some cases dominate the functioning of a contemporary person in a contemporary world.

Introduction

Internet, as the phenomenon was introduced without some clear rules and requirements; it was such an innovation that no one thought of introducing it together with the set of rules in order to guarantee plan, control and safety. Therefore today, several decades later, it is sometimes difficult to ensure safety, as many of the measures have to be introduced (and were introduced) at a later date, as if a compensation[1]. B. Schneier[2] noted „computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people problem".

Moreover, with advancements of technologies, and, consequently, with advancements in internet (or-rather materials/entries in internet) becoming a product of almost everyone on the globe, the safety in digital space becomes a complex task that only joint efforts of users and IT professionals may face effectively.

If in early phases of internet‘s existence the jokes were rather benign (the first spam-message was sent in 1978), however, later they became much more serious. In 1988 the first virus was registered for the disruption of operational system, and for defacement of web-sites. Moreover, later on the seemingly benign pranks transformed into a conscious and financially motivated activity[3]. As an example, of intolerable behaviour is the Tay[4]; Microsof cancelled the testing of artificial intelligence, because in 24 hours the software began generating racist entries[5]. The introspection of a rather recent and short history is provided in order to provide arguments for the necessity not only to introduce, but also to discuss with each and every future law-enforcement officer the dimensions of safety in digital space.

Therefore **main purpose** of paper was to investigate the degree to which students: future law-enforcement officers, who will be obliged to provide security for other people, think about their own/personal safety in digital space.

For the development of this paper methods of critical references analysis and the empiric four-phases study (Wintre-Spring, 2016) were employed.

[1] Garšva Eimantas, and Skudutis Julius. "Secure Computer System design." Electronics and Electrical Engineering. 6(55) (2004): 43-48.

[2] Schneier Bruce. Secrets and Lies– Digital Security in a Networked World. John Wiley & Sons, 2015.

[3] Kalpokas, Vaidas, and Marcinauskaitė Renata "Identity Theft in Cyberspace: Technological Aspects and Criminal Legal Assessment." Teisės problemos. 3(77) (2012): 30-52.

[4] Lee, Peter. Learning from Tay's introduction. Official Microsoft Blog.

[5] Vincent, James. "Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day." March 24, 2016.

Dimensions of Safety in Digital Space: Alarms and Routines

EUROSTAT[6] data shows that in 2015, 1 out of 4 internet-users were alarmed by his/her safety in internet in the European Union. S.Jastiuginas[7] goes as far as to suggest that inability of individuals and organisations to manage safely the information-communication systems may result in problems for the states themselves, therefore, the ability to manage and use information safely may (and must) turn into a strategic priority for organisations and states. Only those states that ensure safety of information; also provide a basis for other dimensions of safety, and counter-measures for International risk management (CIO, CSO and PwC study, 2010; Ernst & Young's 12th Annual Global Information Security Survey; NATO, 20107). The most recent events (e.g., "Panama Papers") illustrate the controversy that each organization and state faces: on the one hand, this was leaking of a sensitive information, which shows the shortcoming of information management systems; on the other hand, the leaking disclosed unethical and even potentially criminal process (which, paradoxically may be considered a counter-criminal activity from some perspective)[8]. Those and other dimensions already became and will only become more dominant part of law-enforcement officer's work.

In 2008, when Facebook was still a relatively new technology, K. Lewis, J. Kaufman and N. Christakis[9] invited 1740 students from the USA to participate in a survey. Out them, 1710 of students (98.3 %) have been located on Facebook. K. Lewis, J. Kaufman and N. Christakis had found, that "a student is significantly more likely to have a private profile if (1) the student's friends, and especially roommates, have private profiles; (2) the student is more active on Facebook; (3) the student is female; and (4) the student generally prefers music that is relatively popular (high mean) and

[6] 2015 Europos Sąjungoje 1 iš 4 interneto naudotojų susiduria su saugumo problemomis (EUROSTAT). February 11, 2016.

[7] Jastiuginas Saulius. "Information Security Management in Lithuania's Public Sector." Informacijos mokslai 57 (2011): 7-25.

[8] The International Consortium of Investigative Journalists. The Panama Papers. Politicians, Criminals and the Rogue Industry That Hides Their Cash.

[9] Lewis, Kevin, Kaufman, Jason, and Christakis, Nicolas. "Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network." Journal of Computer-Mediated Communication. 14 (2008): 79-126.

only music that is relatively popular (low SD)" (94 p.). Therefore authors concluded that the boundaries between the private and the public had been transcended: "users venture too far into public space with private details, and the consequence is a crashed party, a lost job opportunity, or—at an extreme—sexual assault or identity theft"[10]. Authors, however, shared the conviction that the next generation may find the way in organising the digital space in a more safe way with the introduction of certain filters for safety, may be the digital space will become "self-regulating systems".

Some authors state forcefully that ensuring the safety of computers is simply impossible without ensuring the safety of internet. Internet provides a technical platform for self-realisation and the freedom of speech[11]. The anonymity of users contributes to self-realisation and the freedom of speech. And that is the great paradox: on the one side we all want to ensure safety in internet; and on the other hand it is the anonymity that adds to openness and freedom of speech. The paradox that comprises a large part of our contemporary life.

Methodology of an empiric study

I phase. N=80. The respondents are students of higher education, future law-enforcement officers, 19-21 years of age, in 2 or 3 years of their studies. In the beginning of semester all students were invited to carry out a survey, where one of the questions was as follows: "What is your estimation of your competence to use the information search on Internet tools?".

This phase of a study was aimed at identifying personal-subjective evaluation of students' IT competence as they evaluate it themselves. A half of respondents evaluated their competence as of an 'independent user' (Fig. 1).

Students were also asked to share which Internet tools they use every day. Fig. 2 presents the findings that the most popular was social network (Facebook), which they use every day. However, other tools are not used often, or are not used at all: the cloud technologies were among those used rarely or not used at all (Dropbox, SugarSync) (1 or 2 out of 80 respondents).

[10] Lewis, Kevin, Kaufman, Jason, and Christakis, Nicolas. "Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network." Journal of Computer-Mediated Communication. 14 (2008): 96p.

[11] Garšva Eimantas, and Skudutis Julius. "Secure Computer System design." Electronics and Electrical Engineering. 6(55) (2004).

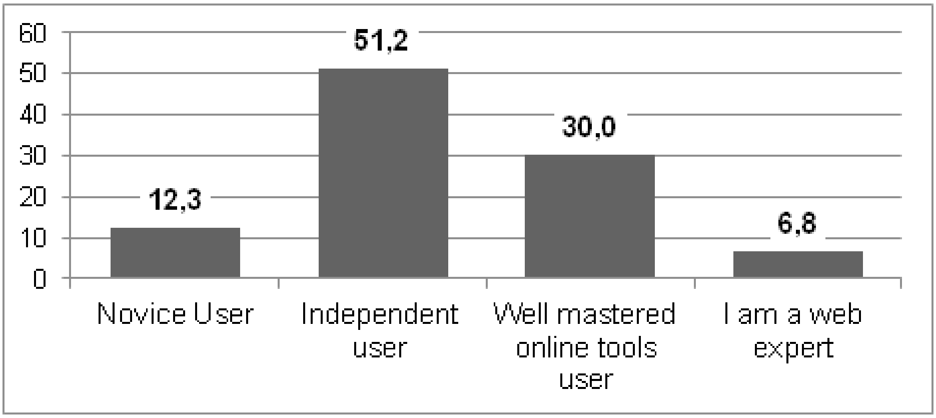

Fig.1: Students on their own competence to use the information search on Internet tools (in percentage)

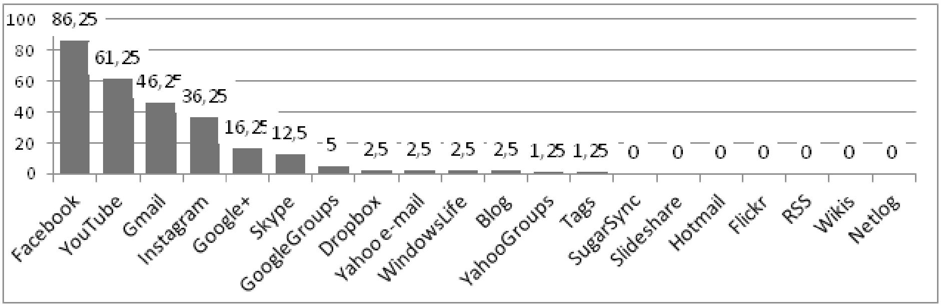

Fig. 2 The Internet tools that students use.

II phase. N=66. Further on, students were invited to participate in II phase. The test that was developed during the national project "Langas į ateitį"[12] was used for the purpose. While developing this test, standards of National IT proficiency of the Republic of Lithuania, also requirements set in other Programmes (ECDL[13], Microsoft Unlimited Potential Community Learning Curriculum, Microsoft Digital Literacy Curriculum v.2) were taken into consideration.

The estimations were designed as follows: if a respondent received a score less than (<) 60 %: he or she failed test, if the score was: 60 % - 70 %: he or she was identified as novice user, if a score was 70% -80 %: he or she

[12] Langas į ateitį ("Window to the Future"). Last modified 2015. http://www.epilietis.eu/index.php/about-the-project.

[13] European Computer Driving Licence (ECDL)

was identified an independent user, with a score of 80 % - 90: proficient; 90 % and more: advanced user (Fig. 3).

This phase of a study was aimed at identifying the level of the IT competence of students according to quite a standardised-objective perspective, using a standardised test.

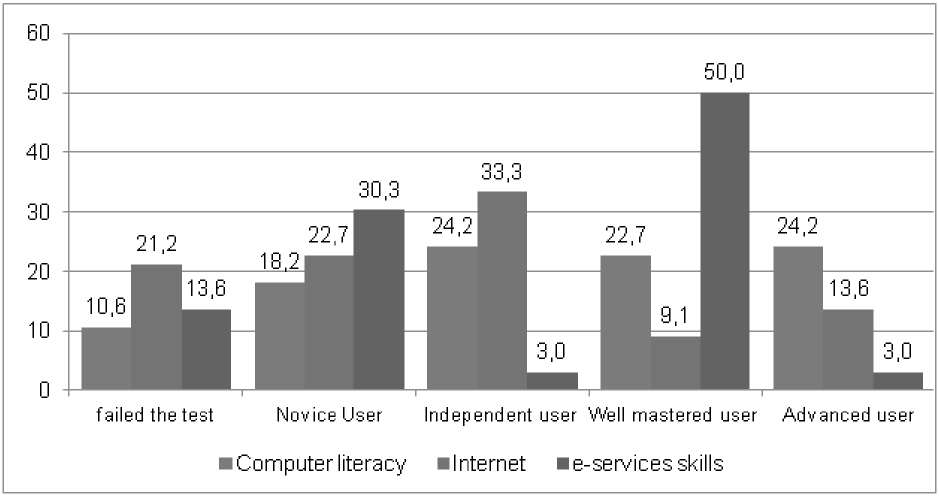

Fig. 3. Results of the II phase (students' level of competencies) (in percentage of respondents)

Among many other questions, the specific questions on safety in digital space were included. In the section of "Computer":

- What are the cases when you may expect a virus to attach your computer?
- Should anti-virus software be updated in order to recognise new viruses?
- What will you do if you suspect that your USB was infected by a virus?

In the section of "Internet":

- What are the differences between protocols for data transmission (http and https)?

In the section of "E-services":

- Is it safe to buy items on internet?
- What is an electronic signature?
- What should you do after receiving a banks message to provide your password for e-banking?
- What may happen if you disclose your personal data on internet (name, surname, birth date, credit card number)

III phase. N=23. Students were invited to fill in a specifically designed ECDL test, the purpose of which is to assess the readiness for safe behaviour in Digital space. After the class on ethics in internet, students were invited to fill in the survey; therefore the sample is a convenience sample, and any generalisations cannot be made. The results of the survey should only be used as certain indicators for possible tendencies, and also for designing future surveys on the theme in order to receive more reliable data. However, the data is presented here, because, even if not-reliable, it is, nevertheless, quite instructive.

Fig. 4 illustrates that students (may we remind a reader that respondents were future law-enforcement officers) invest some efforts to protect personal data; privacy safety is, therefore, quite important to them.

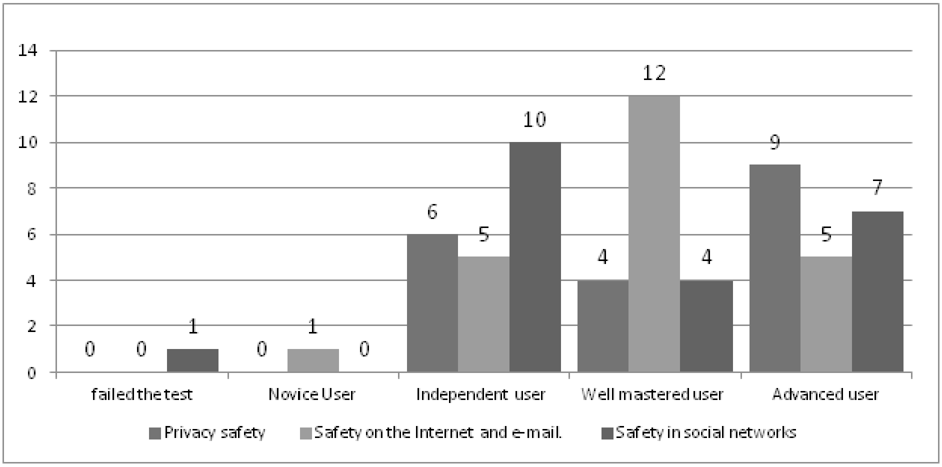

Fig. 4. Students' competencies on Privacy safety, Safety on the Internet and e-mail and Safety in social networks (frequency in cases of respondents).

For those who indicated this as an important issue, 9 (out of 23) were also advanced users). Students‘ competence on safety in internet and in using e-mail are quite high, because appr. half of students (12 out of 23 students) according to the aspects enlisted above were identified as proficient users. However, students' competencies in social networks (which, let us remind the reader, is the most popular tool for students) are lower. Almost half of the students (10 out of 23) were identified as independent users, according to the test results.

IV phase. N=32. Students were invited to share their perspective on safety in digital space. Questions on Facebook were as follows: (Closed-type: How many friends do you have on Facebook?; To what extent do you know your Facebook-friends? Open-type: What are the advantages and shortcomings of social networks? Please, explain how you protect your privacy in a social network).

Analysis of results from closed-type type questions revealed that the number of 'Facebook friends" varied. The highest was almost a thousand: one student indicated having 938 'friends'; the lowest number: another student indicated having 219 'friends'. Also, students stated that they know 'personally' their friends. The highest number was 203 people 'personally known' among all the "Facebook friends"; the lowest: 12.

The analysis of an open-type question revealed that students may be grouped into the following three groups.

- Students are not really sure that they control the safety/privacy on Facebook to a significant level (from the perspective on what is available to other people) ("I do not control anything...")
- Students admit that they are not safe on Facebook ("I try that the minimal number of people whom I do not know personally have access to the contents I upload, because I do not know in what way that may be used; or for what purposes"; "I am not sure whether the information about me is accessible just to the level that I want and authorize…."; "The problem is that not always that I am sure who is behind the profile; therefore there might be problems while sharing info in profiles. Information may get somewhere that I do not want and cause some problems"; "So many people know what is it that you are interested in, what you do….."")
- Students state that they control their safety Facebook ("I feel safe in this environment, because I may decide what is public and what is not. Facebook has its regulations, rules, which ensure safety for a user…"; "I control everything the way I want. That is what applications are for. Only my friends are allowed to the whole account; it is only me who has access to contacts; I regulate the patters for communication; access to information."; "Well, I control the access by using applications according to how I see the necessity, including access to contacts, information, access to my profile.").

Conclusions

1. The empiric study revealed that the competence of 2 and 3 year students in higher education (future law-enforcement students) on safety in social networks we may label: "independent user" (or: incredibly naïve? - authors' note).
2. Qualitative study revealed three main perspectives of respondents:

- Students are not sure whether they control the access to their profiles (and contents) to a significant degree);

- Students admit not being safe in Facebook;
- Students state that they control their safety in Facebook.

Though the results of this four-phases study should be taken into consideration with caution because of the limitations stated above in the text: namely, the sample is a convenience sample, and the numbers of participants is not high, regardless, certain tendencies and insights are, nevertheless, instructive.

Firstly, young people, even future law-enforcement officers, do not really draw a line between 'private' and 'public' in their activities/information shared in digital spaces. Some of them do, or think they do, but, obviously (and thankfully), lack of personal experience in the dangers in being negligent in digital space, prevents them from being cautious. With digital space comprising so much of a contemporary person's life: e-banking; studies; regulation/monitoring of one's loans/mortgages, etc., it is imperative to remind young people about the necessity to keep certain areas of life private and as safe as it is technologically possible. Especially that applies to future law-enforcement officers, because they have to set a personal example and be ready to consult a citizen and community on the issue.

Secondly, we, educational professionals in higher education should be aware that the very fact that young people are quite proficient (according from their personal-subjective evaluation and a more objective-standardised evaluation) in using Internet and its tools, does not automatically mean that they are ready and proficient in using those tools in a safe way. And, therefore, our-educationalists' efforts to compensate for that are necessary.

References

1. 2015 Europos Sąjungoje 1 iš 4 interneto naudotojų susiduria su saugumo problemomis (EUROSTAT). February 11, 2016. Accessed April 20, 2016, http://ivpk.lrv.lt/lt/naujienos/europos-sajungoje-1-is-4-interneto-naudotoju-susiduria-su-saugumo-problemomis.
2. Garšva Eimantas, and Skudutis Julius, *Secure Computer System design.* Electronics and Electrical Engineering. 6(55) (2004): 43-48.
3. Jastiuginas Saulius, *Information Security Management in Lithuania's Public Sector.* Informacijos mokslai 57 (2011): 7-25. Accessed April 10, 2016. http://www.journals.vu.lt/informacijos-mokslai/article/view/3137/2755.
4. Kalpokas, Vaidas, and Marcinauskaitė Renata, *Identity Theft in Cyberspace: Technological Aspects and Criminal Legal Assessment.* Teisės problemos. 3(77) (2012): 30-52.

5. Langas į ateitį ("Window to the Future"). Last modified 2015. Accessed February 2, 2016, http://www.epilietis.eu/index.php/about-the-project.
6. Langas į ateitį ("Window to the Future"). Last modified 2015. http://www.epilietis.eu/index.php/about-the-project.
7. Lee, Peter. Learning from Tay's introduction. Official Microsoft Blog. Accessed August 20, 2016, http://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/#sm.000jh14di129ee0ov1u1atn7zsco3.
8. Lewis, Kevin, Kaufman, Jason, and Christakis, Nicolas, *Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, Journal of Computer-Mediated Communication. 14 (2008): 79-126. Accessed February 2, 2016, doi: 10.1111/j.1083-6101.2008.01432.x.
9. Microsoft's disastrous Tay experiment shows the hidden dangers of AI. Accessed August 20, 2016, http://qz.com/653084/microsofts-disastrous-tay-experiment-shows-the-hidden-dangers-of-ai/.
10. Schneier Bruce. Secrets and Lies– Digital Security in a Networked World. John Wiley & Sons, 2015.
11. The International Consortium of Investigative Journalists. The Panama Papers. Politicians, Criminals and the Rogue Industry That Hides Their Cash. Accessed August 20, 2016, https://panamapapers.icij.org/.
12. Vincent, James. "Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day." March 24, 2016. Accessed August 20, 2016, http://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist.

Assoc.prof. dr. **Edita Butrimė** (assoc. prof. at the Department of State Border Guard, at the Faculty of Public Security at Mykolas Romeris University, Kaunas/Vilnius, Lithuania) defended her PhD thesis in 2011 on the elements of e-learning as a socio-cultural system. Since then she published two monographs and other publications internationally (Germany, the USA), also, she is the author of several papers. Her teaching and research interests include enacting members of HE to use e-learning in a more authentic and rewarding way; also, her teaching includes analysis of specialised data-bases for law-enforcement and other issues.

Prof. dr. **Vaiva Zuzevičiūtė** (prof. at the Department of Humanities, Vice-dean of the Faculty of Public Security at Mykolas Romeris University, Kaunas/Vilnius, Lithuania) defended her theses in 2005, and completed a habilitation procedure in 2008; in 2013 she was granted a title of an Honorary prof. at Pecs University, Hungary. Her research interests include life-long learning, citizenship education of law-enforcement officers and other aspects of contemporary Higher education. She is an author of several monographs nationally and internationally.