Teaching digital security

Marjan Krašna, Tomaž Bratina
University of Maribor, Faculty of Arts & Faculty of Education
Department of Pedagogy, Department of Primary Education
Koroškacesta 160, 2000 Maribor, Slovenia
marjan.krasna@uni-mb.si, tomaz.bratina@uni-mb.si

Abstract.*In digital world a security becomes more and more important. For teachers this does not mean only protection of their computer and their data but also teaching students how to prevent side effects of using internet. Since contemporary students are called digital natives we thought that these topics should not be included at the university level of education. Survey of our student proves us wrong. We have found that our students (future teachers) are unaware of importance of data values in education processes and they rarely act preventive. The results of this research ensure us that we need to prepare elective course called digital security for students from educational programs. Article is structured to the topics that need to be covered in digital security and also the results of the survey.*

Keywords: digital security,survey,digital competences, curriculum development.

1 Introduction

Past few years demanded changes in the education processes. Our students have finished primary and secondary education with the help of computer and we can call them *digital natives* whose perspective to learning and time have changed dramatically. These generations of student have different perspective to the process of learning and they require information they want in the "real time" preferably "now". If information is not available "now" it is useless [1]. Term "now" means the average time from web server request to its response[2]. Therefore we have to change the paradigm starting with the problem presentation and continue with the problem solution [3]. Despite the fact that most of teachers have managed to prepare their learning materials in this manner we find out that this approach have also some drawbacks. Our students have few transferable skills;they have mostly just superficial knowledge; they suffer from decreased research stamina;inability to process complexity learning materials; and they also suffer decreased autonomy. Since these findings are not favorable we need to take corrective actions. Beside some other findings these were the reasons we started the project "Development of natural science competences" in 2009. In the initial phase we gathered all relevant information about competences and how to change the educational paradigm. We were able to prepare the project proposal to enhance learning by developing competences rather than teaching content.

Therefore we should know that competences are not monolithictopics in the educational processes. At least three levels of competences are highly important [3]:

- Competences of students,
- Competences of teachers; and
- Competences of teachers teaching teachers.

Even though we know that the final goal of the education is the competent student we first have to produce competent teachers. Since teachers need to know its profession and pedagogical and methodical approaches the best model for their training would be Pedagogical content knowledge [4] and its modern evolution Technological pedagogical content knowledge [5]

The key competences are the described in the eight topics framework in the European legislation [6].Our task was to research and develop digital competences. We have discovered that forthe problem based approach and project based learning multiple computer topics are required:[3][7] [8]

- Word-processing
- Spreadsheet manipulation
- Image processing
- Video & sound processing
- Presentation techniques
- Internet & Communication

It takes us more than two years to discover that digital security also needs to be the part of these topics. Digital security topics areactually hidden until disaster occurs.

Most of computer users have only minor computer problems which are solvable without significant losses. Students and even teachers who lost their work have impression that this is something normal in digital world. But we cannot afford data loss. Any long term analysis and trend analysis cannot be conducted if data is lost. On the other hand data loss is not the only problem we face in internet environment. The general opinion is that younger generations are familiar and impervious to the ICT threats.Since we have close contact with lot of students with their computer problems we want to test this general impression. To gain the actual level of knowledge, experience and awareness among the future teacher we conduct a survey. Prior to the preparation ofthe survey we made analysis of threats and their influence to the education processes. When we discovered most facts we prepared survey questions and performed on-line survey.

2 Digital security in education

When an expression digital security occurs most of teachers and students think about computer viruses. Professionals know that damage means data loss [9]. Viruses, worms and Trojans can be prevented even without active protection with antivirus software. A topic of security threats that becomes more problematic are computer frauds and Nigerian scam. In our research we have joined spyware and data gathering since both typeshave practically the same aim. Identity theft is low on the threat priority among digital natives. They often post too much personal data on social networks. We have therefore many problems we need to address in the education of teachers. In this section we are going to address them one by one.

2.1 Datasecurity

For students and teachers it is highly important to save their own data. Student seminar work often require significant amount of effort. Teachers are in the similar position.Since today most of work is in digital form and backup is necessary. Digital library of teacher may have data from many years and most of them are unique. How to perform a proper backup for home users is a matter of many articles on the web. Too many people think that copy on the portable disk is sufficient data protection. We have seen a lot USB drives which died with their data on them. With regret we also discover that some userswork directly on the USB drive. Delay write on a portable device may annihilate their work when drive is disconnected.

Second highly important topic in data security is availability of data. Computer usersin the education processes should have learning materials available when needed.

Third topic of data security is preventing access to the sensible data [10]. In the education this are mostly personal data which are protected by law. Less sensitive data which still require attention are tests for knowledge evaluation in schools. Whole idea of grading is lost if someone have access to the testsquestions before testing and can prepare himself for evaluation[11]. This topic also corresponds with the protection of username and password for accessing data on computer or on the web services. Most of contemporary network software require good password by default. Trivial passwords are not permitted in contemporary LMS and CMS systems.

In our environment we teach data security by answering of the following questions:

- How to make agood backup?
- How to properly store portable memory media?
- How to protect optical media (CD and DVD)?
- How to prepare better home backup system?
- How to create good password?

For highly computer literate students we prepare the advice how to make home NAS system; or prepare home server with mirror disks (RAID 1) and scheduled backup.

2.2 Virus, worms, and Trojans

Students generally know how to protect themselves from viruses. More problems with the viruses have teachers since they are not digital natives.Virus protection is not just a matter of installing antivirus software. Educated computer user will less likely be a victim of data loss resulting from the computer virus [9][10].

Worms are more sophisticated than virus. Theyexploit known vulnerabilities of computer software and most users are unaware of infection. The success of worms is better than virus because many users turn off automatic software upgrade. This is particularly true for computers used for presentation in the classrooms.

Among these three threats Trojans are the toughest since they exploit users. No operation system is immune to the Trojans. Contemporary operating systems warns user before running unauthorized program code but users often ignore these messages.

Teaching users about viruses and worms is fairly simple. But we have to give them advice that the best protection against viruses is to never be infected. In the complexity of operating system even cleaning of virus infected computer is not totally sure. Legal software and regular updates should prevent viruses and worms. We have discovered that despite the fact that our student can use Campus license for Microsoft products but they don't use them.

For computer more literate users we suggest checking network connections. If a connection is made and no apparent software is responsible for the traffic they should perform system check. We teach them how to read Task manager data and how simple home router effectively prevents worms spread. Students' knowledge about computer network is amazingly low. Most of the students do not know that meaning of HOSTS file in Windows.

2.3 Computer fraud and Nigerian scam

Students are quite capable to recognize computer frauds and Nigerian scams and they are rarely victims of such frauds. The problem is bit more threatening in the teachers' population. We have also find out that these types of threats are not effective in our country because of the language barrier. Even ifcomputer users are English literate they do not fall victim to English text. In the recent days we witness more scum text translated with Google translate butthe text is so bad that it is recognized as scum immediately. But in the future when computers will become more capable of translating text this type of threats will probably need elevated attention.

Teaching computer fraud and Nigerian scam require a lot of work. We have managed to make a huge collection of fraud e-mails from many years and analyze their content. The result of analysis is presented to our students and patterns that emerge in almost all such e-mails become evident. Today most popular e-mail scams require personal data to be sent to sender. These data may be used for identity theft of some other types of ill intentions.

2.4 Spyware and data gathering

Most of the time spyware is installed by users themselves. There is a thin line between spyware and adware but in our eyes they are the same threat with different names. Data gathering is actually performed routinely on the internet. Processes of data gathering are either legitimate or not. In legitimate data acquisition users often get e-mail or pop-up to participate in the survey. Such data gathering provide valuable feedback to the researchers and purposeor research is clearly explained.

The other types of data gathering are e-mails sent in HTML with links to the pictures on some web servers. In our opinion e-mail messages should be sent as text only. Text only messages prevent including graphics elements in the message. Despite the fact that most of e-mail programs prevent showing pictures unless user enable this option user often allow picture download. As soon as they download images from the server their IP number are stored on the picture web server.

Teaching the spyware prevention is not easy. In these efforts we too often get the response from students that this topic of digital security is too complicated. Nevertheless it is highly important that teacher do not suffer humiliating attack of (pornographic) popups in the classroom or spyware prevent normal operation of computer either by slowing it down or prevent opening some webpages because of continuous redirection.

2.5 Identity theft and certificates

Our students often misunderstood the identity theft.They post too much personal data on the social networks and enable perpetrators to gain access to their e-mail accounts, social network accounts and even bank accounts. Students' recovery from such attacks is much quicker than teachers'. Teacher's e-mails have ability to significantly disrupt the education processes. Another really bad think is that someone uses teacher's identity to send inappropriate messages to their students.

To prevent such events personal certificates should be used and all sensitive communication should be signed. Certificates must be appropriately stored in a safe place to prevent theft and protected with strong password.

Teaching identity theft should have high priority in the digital security. It is also necessary to teach users how to find and read e-mail headers. Google mail password should be very strong passwords. We must prepare our student to use certificates in their communications.

3 Student survey andresults

We prepared the on-line survey corresponding to the Web Survey Methodology guidelines[12].

The survey was performed on the sample of 147 students – future teachers, attending the 1st and 3rd year of study. The goal of the survey was to gain understanding of students'understanding and attitudeabout digital security. We have focused on the following topics:

- Personal data on the social networks.
- Data backup and protection
- Phishing
- Identity thefts
- Students' expertise self assessment in the area of digital security.

3.1 Personal data protection

Survey was made of 21 questions which were grouped into different categories. For example the street name, house number, postal code or the place of living was joined into *localization data*. The social security number, fiscal code, bank account and the amount of incomes were joined under *fiscal and administrative data*. The number of family members, parents, relatives and partners names was joined into *family data* group and so on.

Table 1: Personal data publishing

Published personal data (in social networks)	Real	Fake
Fiscal and administrative data	2,4%	33,6%
Family data	16,3%	22,8%
Localization data	9,4%	11,4%
Phone number	1,7%	9,9%
Social life data (entertainment, activities, membership..)	4,4%	5,0%
Name and/or family name	9,5%	3,3%
Other persons images	6,9%	3,3%
Sexual orientation	5,5%	3,3%
E-mail	8,2%	2,8%
Level of education	7,5%	2,2%
Own photos or pictures	8,9%	1,7%
Date of birth	9,1%	0,7%
Sex	10,2%	0,0%

The table 1 represents proportions publishing the specific personal data (see Table 1). Students were able to respond which type of data they present on the web as honest (real) data or fake data. The topics are later sorted according to real data descending. Table should be read as difference between real and fake numbers.

The results were surprising. In the topic of real names student were much more honest than we expect(9,5 % real

versus 3,3 % fake). Even whenthey submit the date of birth they arehonest in 9,1 % of cases.In the survey students said they exclusively submit their gender honestly. The level of the education is more likely published as real data than fake.

There is slight differenceinhidingof localization data. This data were published as fake in about 11,4 % and as real in about 9,4 %. Results are not encouraging because the localization data can be used for identity theft.

Far more cautious were users in publishing their fiscal and administrative data which were published as fake in about 33,6 % of cases. Their understanding of consequences of these data abuse is satisfying.

Publishing family data was pretty careless. About 16,3 % of users publish real family data and slightly more (22,8 %) publish fake family data. The attitude of the users to protect theirfamily data is not satisfying.

Publishingpersonal photos is problematic topic. Students often perceive photos as something that cannot be abused. They are a bit more careful in publishing other people's photos. Since publishing of the photos is common practice today this result may not be concerning.

Results have proven that these topics should be included in the teaching of digital security. Students and teachers, have to gain the awareness and the knowledge about the potential threats in the social networks. This knowledge should later be transferred to the scholars and/or their parents consecutively.

3.2 Personal data backup

Student's activity records, reports, seminar and finally diploma works are very important for the students and should be kept in the safe place. Keeping data safe is also very important for teachers. In the survey we tested the awareness of students about the data backup.

Table 2: Backing up of personal data

How often do you create backups?	**%**
Never	59,2
A few times in a year	17,6
Monthly	9,9
Weekly	4,9
Twice in a month	4,9
Every day	3,5

Survey showed very high degree of indifference about value of students' data protection. About 59,2 % of students have never made any backups and 17,6 % of them made backups only occasionally. If a sufficient backup should be done at least once a week then we see that only around 8,5 % of student make regular backups. All the rest are in the mercy of the hardware failure.

We wanted to test the hypotheses that older students are more aware of importance of backup than younger. The results show no statistically significant difference in the attitude toward the backup of important data (P=0,826). About 63% of younger students and 55,6% of experienced student do not create backups at all. Less than 20% of students of any group are creating the backups only few times a year (Table 3).

Table 3: Backing up of personal data by year of study.

Year of study	1st		3rd	
How often do you create backups?	f	f %	f	f %
Every day	2	2,9	3	4,2
Weekly	2	2,9	5	6,9
Twice in a month	3	4,3	4	5,6
Monthly	6	8,6	8	11,1
A few times in a year	13	18,6	12	16,7
Never	44	62,9	40	55,6
Total	70	100,0	72	100,0

3.3 Phishing

We have prepared nontrivial questions to test the concept of phishing among our students. Responses are shown in table 4.

Table 4: Understanding the conception of phishing

What is phishing?	**%**
Acquiring usernames or passwords by using fake webpage	52,1
Collecting new friends in social networks	19,7
Searching for information on the web	18,3
Introducing under the false identity	9,9

The results were encouraging. More than a half (52,1 %) of the students (future teachers) are familiar with the conception of phishing. But the resultsarefar fromsatisfying sincejust little less than a half of future teachers are totally unprepared for phishing threats.

Further analysis has shown some advantage in younger generations. By analysing only the correctly recognized concepts of phishing into the consideration the analysis shows statistically significant difference (χ^2=4,801, P=0,028) between the students of 1st and 3rd year of study. Students from 1st year of study were better in recognizing concept (61,4 %) of phishing that students from 3rd year (43,1 %). The advantage towards younger generations may be the result of increased digital literacy, higher level computer knowledge or better overall digital competency.

3.4 Identity theft

Well informed or educated user is rarely a victim of identity theft. Our students should be such users not just for themselves but also because they will have to teach younger generations about these threats.

Table 5: Understanding the identity theft phenomena

What is the identity theft?	%
Personal data misusage	73,9
Stealing of the personal documents	22,5
Message posting using nick name	2,1
Attending the exams in someone's name	1,4

About three quarters of the students (73,9 %) are informed and aware about the identity theft. This is good. But we still have 22,5 % of the students who consider the identity theft as stealing of the personal documents (like passport, personal identity card or social security card) and this is not good. No statistically significant difference

(χ2=0,085, P=0,771) was discovered between the students of 1st and 3rd year of study in understanding the principles of the identity theft. The topic of identity theft should be a part of teaching of digital security.

3.5 Personal expertise estimation

Survey has a question which allows students to grade their knowledge of digital security. Responses were structured into 5 grade scale (not familiar with digital security, weak understanding, very well understanding of digital security, familiar with almost everything and do not care about digital security). Students' responses are shown in table 6.

Table 6: Understanding the identity theft phenomena

Estimate your personal expertise or knowledge about the threats…	%
Weak	66,2
Very well	30,3
Familiar with almost everything	2,1
Don't care about	0,7
Not familiar with	0,7

The results are not good. Around two third of the students (66,2 %) have graded their level of personal expertise or knowledge about the digital threats as very low. Only about 30,3% of the students have estimated their personal expertise as well. The highest confidence in personal understanding of the present threats was estimated only by 2,1% of the students (Table 6).

The analysis did not discovered statistically significant difference (χ^2=7,466 P=0,113) between the students of 1st and 3rd year of study.

4 Conclusion

Daily use of different kinds of communications is part of our lives. In most cases the influence of modern communications is positive. But every now and then users face side effects of modern ICT. From hardware breakdowns to software malware users experience data loss or unwanted effect. These topics have to be included at all levels of education. They are not just responsibility of computer professionals but also other educators. Social networks become phishing ground for information theft and unwanted behavior of some individuals toward young users. Digital security education should also be a part of LLL (life-long learning) programs. For students of general pedagogy and special didactics we therefore prepare special course. We have assessed the needs and performed analysis of required topics for digital security. Survey's outcomeswere not complete surprise but we anticipate better results. The results are welcome guideline for preparation ofstudy course of digital security.

5 Acknowledgements

We greatly acknowledge the support of the Ministry of Education and Sport of Republic of Slovenia and European Social Fund in the frame of "Project: Development of Natural Science Competences" on Faculty of Natural Sciences of University of Maribor.

References

[1] R. Mayer and P. Chandler, "When learning is just a click away: Does simple user interaction foster deeper understanding of multimedia messages?," *Journal of educational psychology*, vol. 93, no. 2, pp. 390-397, Jun. 2001.

[2] M. Krasna and B. Kaucic, "Evaluating LMS/CMS performance," in *19th Central European Conference on Information and Intelligent Systems*, Varazdin, Croatia, 2008, pp. 181-185.

[3] M. Krasna and T. Bratina, "New Paradigm in Preparing E-Learning Materials," in *Mipro*, Rijeka, 2010.

[4] L. Shulman. (1986) Pedagogical Content Knowledge (PCK). [Online]. http://www.tpck.org/tpck/index.php?title=Pedagogical_Content_Knowledge_(PCK)

[5] P. Mishra and M. Koehler, "Technological Pedagogical Content Knowledge: A Framework for Teacher Knowledge," *Teachers College Record*, vol. 108, no. 6, pp. 1017-1054, Jun. 2006.

[6] EU legislation. Europa.eu/legislation_summaries. [Online]. http://europa.eu/legislation_summaries/education_training_youth/lifelong_learning/c11090_en.htm

[7] M. Krasna, "Digital competences and multimedia ," in *International Conference on New Horizons in Education, INTE-2010*, Famagosta, 2010.

[8] M. Krasna and T. Bratina, "Universal digital competences," in *21th Central European Conference on Information and Inteligent Systems CECIIS 2010*, Varazdin, 2010.

[9] R. C. Newman, *Computer Security: Protecting digital resources*. Jones and Bartlett publishers, 2010.

[10] B. Schneier, *Digital Security in a Networked World*. Yohn Willey & Sons, Inc, 2000.

[11] L. K. Robinson, A. H. Brown, and T. D. Green, *Security vs. Access: Balancing Safety and Productivity in the Digital School*. Eugene, Oregon: International Society for Technology in Education, 2010.

[12] (2010) EnKlikAnketa. [Online]. http://www.1ka.si/