Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

Multimedia password retrieval programs in information security education

Antónia Szász*, Gábor Kiss**

* Denis Gabor College, Institute of Basic and Technical Sciences, Budapest, Hungary
** Óbuda University, Institute of Mechanical Engineering and Security Sciences, Budapest, Hungary
* szasza@gdf.hu, ** kiss.gabor@bgk.uni-obuda.hu

***Abstract* — The main objective of our research is to examine the impact of the information security course on students' habits, attitudes, and everyday security awareness, furthermore, to analyze and develop educational methods.**
In this study, two groups are compared. In Group 1, students were watching video recordings exemplifying password decryption by using programs. In Group 2, students could test these programs as well.
When assessing the effectiveness of learning, exams focus on knowledge and skills, though hardly give insight into the change in attitude. Therefore, we tried to reveal the impact appearing in students' personal lives by examining their password and device usage.
Before and after the course an online survey was carried out among safety engineering students. Answers about password management were scored according to their safety, or security risk. Comparisons of the groups and analysis of changes were performed by descriptive statistics and nonparametric tests. Based on multivariate statistical methods and qualitative analysis of the students' comments on their password habits, we evaluated the changes in the dimensions of security and awareness.
In Group 1, password usage patterns did not change significantly. In Group 2, a significant improvement was demonstrated in the diversity and length of passwords, variety of character types used in passwords, frequency of password change, and in the use of foreign Wi-Fi.
In conclusion, the mixed educational method facilitating student activity had greater impact on students' information security practices and awareness than the method applying only video demonstration which provides purely a passive reception.

Keywords: information security awareness, attitude, multimedia, information technology, didactics, effectiveness of educational tools

I. Introduction

We study the efficiency of information technology (IT) training and the students' IT and information security competencies in several higher education institutions and in numerous training fields in the frame of an international, multi-year research project (e.g., [1, 2, 3, 4]). The study presented in this paper is a part of this project. The main objective of this study was to examine the impact of the information security course on students' habits, attitudes, and everyday security awareness. Furthermore, we aimed to analyze and develop educational tools and methods.

A. Background

Inclusion is a key concept of the European Digital Agenda and the Digital Competence Framework of the European Union [5, 6, 7]. It refers to both an inclusive and an accepting attitude, which is of paramount importance in IT training as well. It also has a clear role in the acquisition and application of competences, which is the main goal of the training system focusing on learning outcomes. Among the components of the professional competences, namely, (1) knowledge, (2) ability, (3) attitudes, and (4) autonomy and responsibility, the traditional technical higher education focuses on assessing the first two, while the other two barely get any feedback, even though they are immanent parts of IT and information security.

To find a solution to the aforementioned problem, in the design of this research we focused on studying the students' approaches, attitudes, and habits. Since in assessment of learning effectiveness the tests and papers examine merely material knowledge and professional application, but put less emphasis on attitudinal change, we also tried to reveal the impact of the information security course on students' personal lives by examining the individual password and device usage.

Information security inherently has far more levels and components. However, special emphasis needs to be put on the responsible and conscious use of passwords and devices concerning both individual and organizational data and system protection. Moreover, the competences, including relevant knowledge, awareness, and attitudes, developed during the training will determine the future information security behavior, comprehension of, and compliance to the related rules and protocols at workplace.

B. Didactical issues

We have been using various multimedia and IT tools for illustrative purposes, knowledge transfer, and competence development for several years. However, based on the results of our previous researches, these tools failed to evoke any relevant changes regarding the degree of, moreover, sometimes the direction of the supposed changes we wanted to achieve in information security awareness. For that reason, we thought that it is worth involving activity-centered educational informatics tools that can promote students' interactivity.

We endeavor to find appropriate educational informatics tools and technologies for the purpose, task, or phase of both teaching and learning. Creating a so-called

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

integrated learning environment applying these tools and technologies can even be more interesting for students, and consequently, can develop their competences even more efficiently [8, 9]. (On the use of the methods in educational informatics technology, see also [10].)

The impact of the information security course was studied by means of several methods. In this paper, we compared two groups, highlighting the analysis of tools and methods used in education as well.

II. Methods

A. Educational methods and tools

Nowadays in the media there is an abundance of news about system crash, unauthorized data collection, data leakage, passwords revealed from IT systems. Moreover, there are lots of movies and books about talented hackers, intrusion into personal, enterprise, and government systems. Yet we have noticed that students do not perceive the reality of danger in their own lives. Or, if so, their password usage habits are less secure. Therefore, we consider it important to bring them close to and introduce the nature of security risks, to emphasize the importance of information and system protection, and to make them aware of the significant role of the human factor in the information security [11, 12]. As part of this, we also introduce the technical solutions and the process of password breaking using multimedia support.

There are a variety of programs available on the internet to open password-protected files and connect to wireless networks by decrypting the originals of encrypted passwords. Developers incline to justify the existence of these programs by the reason that the users themselves can forget the password they had previously applied for security purposes and want to regain access to their own materials. However, these programs can be used to access foreign files or networks as well, and thereby to attack them. Among the others, those programs can be more expeditious by which the extra computing capacity provided by the video card in the computer can be exploited, extending the password breaking task to this hardware device suitable for parallel process as well. Password protection is based on the length and complexity of the password, because they determine how fast the password can be deciphered. These programs can be used to demonstrate the difference between weak and strong passwords expressed in time frame needed for decoding them, pointing to the benefits of using longer and more complex passwords.

The methods used by the programs aim at direct locating the original passwords or decoding their version encoded with the unidirectional (hash) function by comparing them with the encrypted version of the string generated by the software. The *dictionary attack*, for example, tries out the vocabulary of a particular dictionary. The *word attack* examines the different variants of words as well (based on a known part of the password or using the words of dictionaries). The *brute force attack* uses and replaces each character from the specified set. By *masking*, the password set up and character set can be defined (for example, many people start their passwords with a capital letter, continue with lower case letters, and put numbers or special characters at the end of the password). The *combination attack* can be used to decode passwords consisting of multiple words, applying different dictionaries previously specified. The *hybrid attack* could also test passwords converted by the *leet* alphabet (which uses, for example, 3 instead of letter *E*, @ symbol instead of letter *a*).

Students were watching video recordings exemplifying the decryption of passwords using various password-breaking programs. The recordings were demonstrating very impressively both the functioning and methods of the programs as well as the speed of password recovery.

The education was conducted in three groups. The students had chosen their groups previously according to their timetable. In two of the three groups, students were watching video recordings exemplifying password decryption by using programs, in the third group students could try out these programs testing their own passwords, regarding the decryption time and their retrievability.

B. Research methods

An online questionnaire survey was carried out among safety engineering students at Óbuda University before and after the information security course (actually, at the beginning and at the end of the academic year), with a two-thirds response rate. They were asked about their password management practices, namely, (1) how long (i.e., of how many characters) their passwords were; (2) what kind of characters were used by them; (3) how different passwords were used for their important services; (4) how often were their passwords changed by them; (5) how their passwords were stored; and (6) whether foreign Wi-Fi or mobile hotspot were used to enter their systems and services. The answers were scored according to their safety, or security risk (safer practice received higher score), and measured in ordinal scale; thereby the original, nominal variables were transformed into ordinal measurement level variables, so they were suitable to be analyzed by statistical methods based on ranks. The recoding of the variables is summarized in Table I.

TABLE I.
Recoding of variables

Score	Password length / Number of characters
1	< 8
2	8–10
3	11–13
4	14–16
5	> 16

Score	**Password complexity** / **Character types** used in passwords
1	only lowercase
2	capital and small letters
3	capital letters, small letters, and numbers
4	capital and small letters, numbers, and special characters (punctuation, #, &, @, etc.)

Score	Password diversity
1	identical passwords
2	partially different passwords (with common, constant part)
3	completely different passwords

Score	Password change frequency
1	never (I never replace them)
2	in case of suspicion of their being revealed
3	once a year or less frequently
4	every 3–6 month
5	every 1–2 month

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

Score	Password storage
1	I allow my browser to save my passwords
2	I note down all my passwords
3	I note down some of my passwords
4	I keep all my passwords in my head (I memorize all of them)
5	I use a password manager program

Score	Use of foreign Wi-Fi / mobile hotspot
1	whenever possible
2	sometimes, but mostly protected networks
3	never

Comparisons of the groups and analysis of changes were performed by descriptive statistics and nonparametric tests. To examine the relationship between the variables measuring the password usage multivariate statistical methods were used. The results were completed with the qualitative analysis of the students' comments on their own password habits. The changes therefore could be evaluated in the dimensions of security and awareness as well.

C. *Concise description of the sample*

In the analysis, *Group 1* represents 'video group', and *Group 2* represents the group of students participating education supported by password decrypter programs as well. In Group 1, there were 48 out of 70 students, while in Group 2, there were 22 students. Students who filled out the questionnaire both before and after the information security course were selected into the sample. (Or, in other words, whose pre-test and post-test data were available). The sample composition and the response rates by groups are shown in Table II.

TABLE II.
SAMPLE COMPOSITION: THE SUBSAMPLES AND THE RESPONSE RATES

Groups (methods)	**Population size**		**Sample size**		**Response rate**
	freq.*	%	**freq.**	%	
Group **1** (video)	**48**	68.6%	**27**	58.7%	**56.3%**
Group **2** (video+program)	**22**	31.4%	**19**	41.3%	**86.4%**
Total	**70**	100.0%	**46**	100.0%	**65.7%**

* freq. represents frequency.

III. RESULTS

Our null hypotheses were tested at a significance level of 0.05. The empirical significance level, the *p*-value will be reported at the results. (This is the probability of obtaining a test statistic at least as extreme as the one calculated from the sample data, assuming that the null hypothesis is true.)

A. *Comparisons and analyses of changes*

A.1. *Comparisons between the two groups*

The Mann–Whitney U tests did not show any significant differences between the two groups' password and device usage *before* the course. However, there were significant differences *after* the course. Regarding four password variables out of the five but password storage the results were significantly better in Group 2 than in Group 1, and the practice of using mobile hotspots significantly improved as well (Table III).

TABLE III.
COMPARISONS BETWEEN THE TWO GROUPS BEFORE AND AFTER THE COURSE: RESULTS OF THE MANN–WHITNEY TESTS

p-values	Password length	Password complexity	Password diversity	Password change	Password storage	Mobile hotspot
Before	0.820	0.447	0.706	0.142	0.168	0.556
After	**0.002**	**0.000**	**0.035**	**0.002**	0.990	**0.038**

A.2. *Analysis of changes*

Comparisons of the pre-test and post-test data were carried out by using Wilcoxon matched pairs tests. Our one-tailed counter-hypothesis suggested that password usage patterns improved after the course. *Group 1* did not show any significant improvement. Even so, in this group the frequency of password change improved the most (here the p-value is close to 0.05), or some students showed a positive change at one or two variables. In *Group 2*, there was a significant improvement in all variables, except password storage (Table IV).

TABLE IV.
ANALYSIS OF CHANGES:
RESULTS OF THE WILCOXON MATCHED PAIRS ONE-TAILED TESTS

p-values	Password length	Password complexity	Password diversity	Password change	Password storage	Mobile hotspot
Group **1**	0.391	0.353	0.500	0.053	0.111	0.240
Group **2**	**0.001**	**0.002**	**0.034**	**0.000**	0.308	**0.010**

Since there were no significant differences between the two groups at the beginning of the academic year, it can be assumed that the educational method had a role in the improvement perceived at the end of the academic year.

A.3. *Descriptive statistics*

Hereinafter, we will present a brief review about the changes within the groups, and the features that describe the groups as a whole based on the analysis of the data collected before and after the course.

The measures of location in Table V and Table VI show the direction and extent of change.

TABLE V.
MEASURES OF LOCATION (GROUP 1)
(B: BEFORE, A: AFTER)

Group 1	Password length		Password complexity		Password diversity		Password change		Password storage		Mobile hotspot	
scale:	**(1–5)**		**(1–4)**		**(1–3)**		**(1–5)**		**(1–5)**		**(1–3)**	
	B	A	B	A	B	A	B	A	B	A	B	A
mean	2.70	2.74	3.11	3.15	2.07	2.07	2.44	2.81	3.48	3.26	2.00	2.07
median	2.00	2.00	3.00	3.00	2.00	2.00	2.00	3.00	4.00	4.00	2.00	2.00
min	2	2	2	3	1	1	1	2	1	1	1	1
max	5	5	4	4	3	3	4	5	5	5	3	3

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

TABLE VI.
MEASURES OF LOCATION (GROUP 2)
(B: BEFORE, A: AFTER)

Group 2	Password length		Password complexity		Password diversity		Password change		Password storage		Mobile hotspot	
scale:	**(1–5)**		**(1–4)**		**(1–3)**		**(1–5)**		**(1–5)**		**(1–3)**	
	B	A	B	A	B	A	B	A	B	A	B	A
mean	2.68	3.63	3.21	3.68	2.16	2.53	2.84	3.68	3.11	3.32	1.89	2.37
median	2.00	3.00	3.00	4.00	2.00	3.00	2.00	4.00	4.00	4.00	2.00	2.00
min	1	2	3	3	1	2	2	3	1	1	1	1
max	5	5	4	4	3	3	4	5	4	5	3	3

There can be seen an increase in Group 2 to a greater extent in the mean of scores regarding all variables. Furthermore, the median, the minimum and the maximum also increased in relation to four of them.

The following series of diagrams (Fig. 1–12) show the rate of changes: what proportions of the respondents answered the questions and how they changed after the course. The overall results are supplemented by the analysis of individual changes.

PASSWORD LENGTH

Group 1: There was hardly any change: one less student uses 11–13-character-long, one more student uses 14–16-character-long passwords. Half of the respondents use 8–10-character-long passwords (Fig. 1). Individual changes: There were no changes at 17 out of 27 respondents (63.0%). 4 students use slightly shorter, 6 students slightly longer passwords after the course.

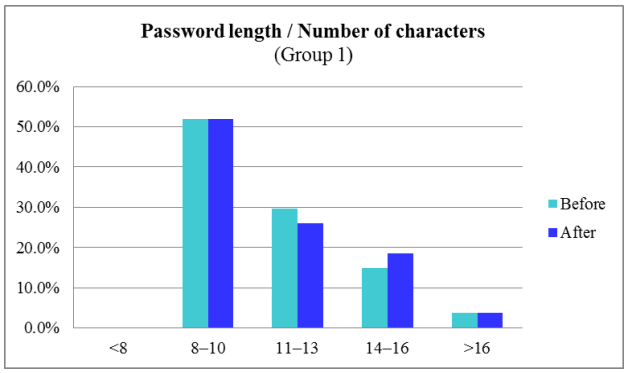

Figure 1. Change in password length (Group 1)

Group 2: After the course, more students use longer passwords (Fig. 2). Before the course, half of the respondents would use very short passwords. After the course, none of them uses shorter than 8-character-long passwords; and 1 student started to use 8–10-character-long passwords. Half of the respondents use 11–13 characters, the other half of them use even more characters in their passwords. Individual changes: 13 out of 19 respondents (68.4%) started to use longer passwords; 1 student slightly shorter. There were no changes in the case of 5 participants (2 of them still use very long passwords).

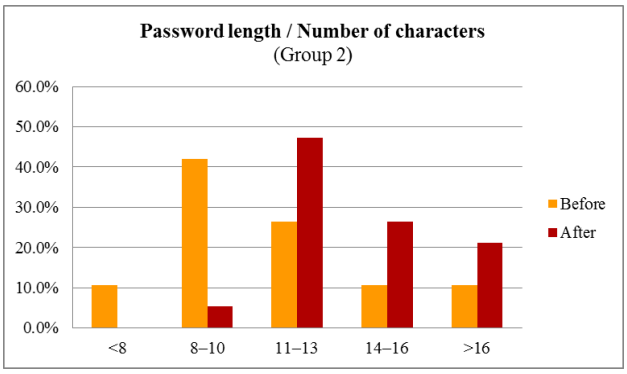

Figure 2. Change in password length (Group 2)

PASSWORD COMPLEXITY (CHARACTER VARIABILITY)

Group 1: The variability of character types used in passwords changed hardly anything (Fig. 3). (One more student uses numbers as well). Individual changes: in the case of the majority, namely, 23 out of 27 respondents (85.2%), there were no changes; 2 students improved, 2 students declined.

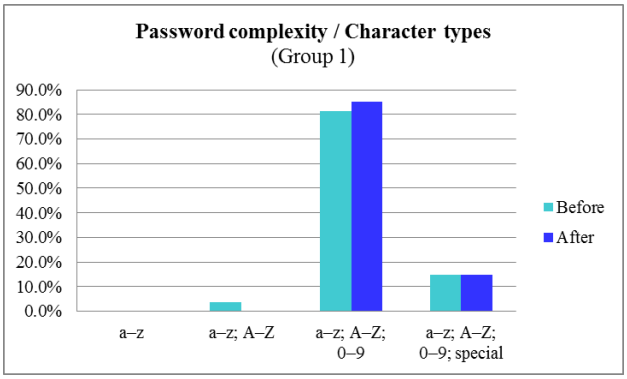

Figure 3. Change in password complexity (Group 1)

Group 2: The improvement is straightforward (Fig. 4). Before the course, one fifth of the respondents (21.1%) used special characters in their passwords besides small and capital letters and numbers, while two thirds of them (68.4%) at the end of the academic year. (4 students used special characters before the course and 9 more students after the course.)

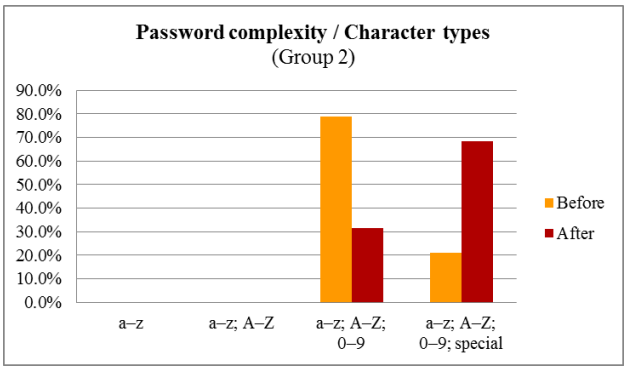

Figure 4. Change in password complexity (Group 2)

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

PASSWORD DIVERSITY

Group 1: On the whole, there was no change in frequency distribution (Fig. 5). On the basis of individual changes: 4 students were more risk-taking; 4 students moved to more secure password usage; 19 out of 27 students (70.4%) did not change. Half of the respondents (48.1%) use passwords with common, constant part. 21 students (77.8%) started to use completely or partially different passwords to different systems; 6 students (22.2%) use one password to all their systems.

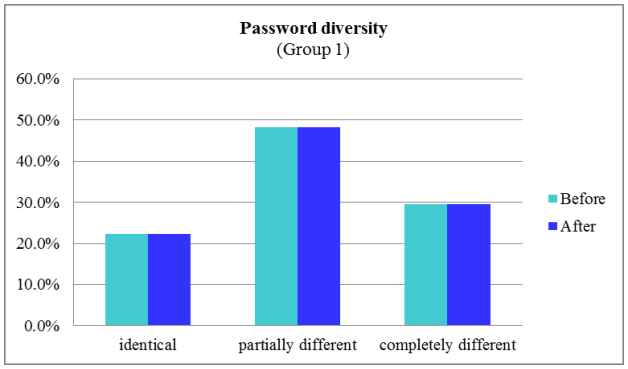

Figure 5. Change in password diversity (Group 1)

Group 2: At the beginning of the academic year, 3 students used identical passwords for each of their services; while no one of them at the end of the academic year. Before the course, half of the respondents (52.6%) would use partially identical and 31.6% of the respondents would use completely different passwords (Fig. 6). After the course, 57.9% of them use completely different, the others partially identical passwords. Individual changes: 8 out of 19 students (42.1%) switched to a safer, 3 students to a more risky password usage, and there were no changes at 8 students (42.1%).

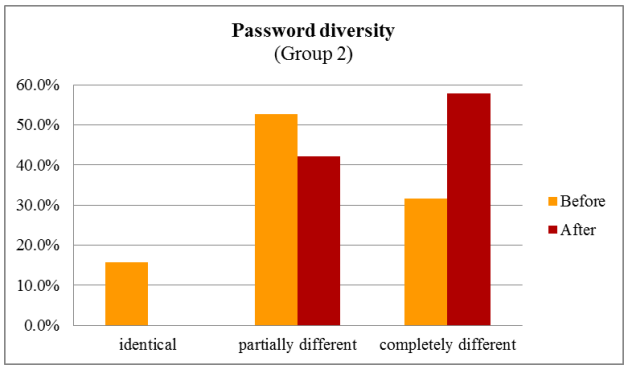

Figure 6. Change in password diversity (Group 2)

PASSWORD CHANGE FREQUENCY

Group 1: After the course, more students change their passwords more regularly, and there is no one who never replaces them (Fig. 7). One fifth of students change their passwords more frequently. Individual changes: 11 out of 27 respondents (40.7%) replace their passwords more securely; 5 of these students show greater improvement. (The others change their passwords annually or less frequently, or if suspicion arises that any of them may be revealed). There were no changes in the case of 13 participants (48.1%).

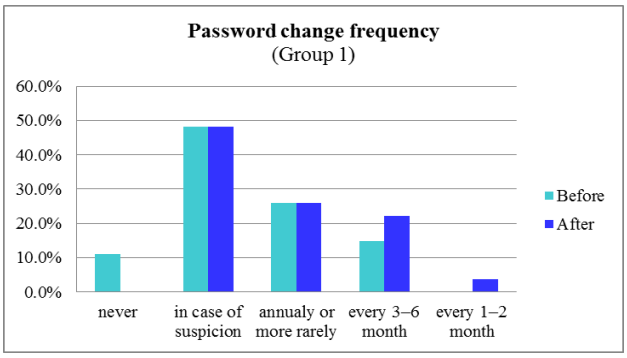

Figure 7. Change in password replacement frequency (Group 1)

Group 2: After the course, there are more students who change their passwords more frequently (Fig. 8). There is no one who never replaces them. Individual changes: 14 out of 19 respondents (73.7%) improved, 5 of them (26.3%) did not change. Before the course, 8 students changed their passwords in case of suspicion arises that they might have been revealed; after the course, they replace them annually. 6 out of 11 participants (54.5%) who changed their passwords on a regular basis change them even more frequently after the course.

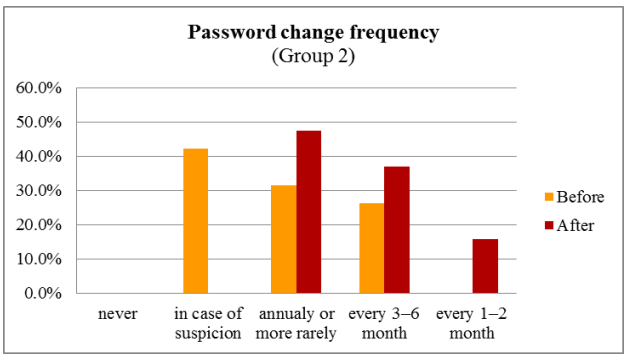

Figure 8. Change in password replacement frequency (Group 2)

PASSWORD STORAGE

Group 1: Some students show either a little improvement or decline, however, in overall, there are no significant changes (Fig. 9). The majority of respondents memorize their passwords. More students began to save them by the browser. Individual changes: 22 out of 27 respondents (81.5%) did not show change (2 of them use a password manager program, 15 participants memorize their password), 2 improved, 3 declined.

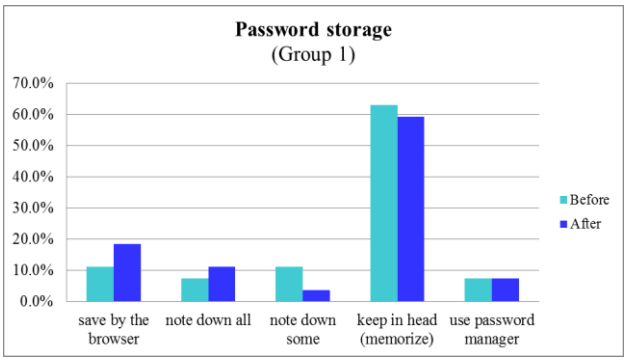

Figure 9. Change in password storage (Group 1)

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

Group 2: Similarly, some of the students have a little improvement or decline, however, in overall, there are no significant changes (Fig. 10). There is no one who notes all the passwords down, neither before nor after the course. More students memorize their passwords after the course than before (instead of noting down, or saving them into the browser). Individual changes: 10 out of 19 respondents (i.e., half of the students) did not change their habits, 6 (31.6%) improved, 3 (15.8%) declined.

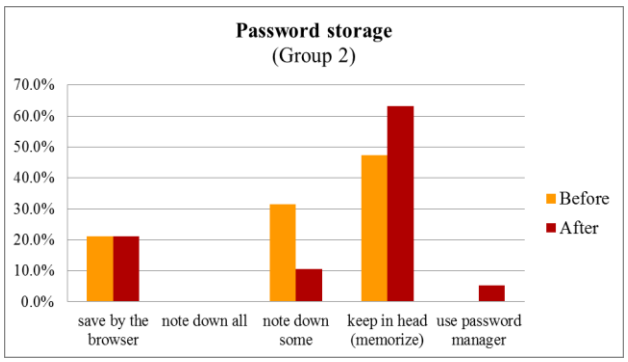

Figure 10. Change in password storage (Group 2)

USE OF FOREIGN WI-FI / MOBILE HOTSPOT

Group 1: The majority of the students 'sometimes' connect to foreign Wi-Fi or mobile hotspot (Fig. 11). By the end of the academic year, the number of them increased. (Before the course, 70.4% of the respondents used mobile hotspot, after the course, 85.2% of them.)

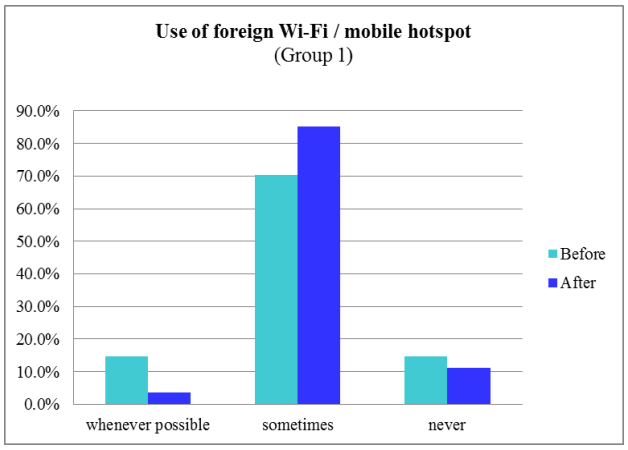

Figure 11. Change in the use of foreign Wi-Fi (Group 1)

Group 2: Half of the respondents 'sometimes' use foreign Wi-Fi (Fig. 12). The number of those who use foreign Wi-Fi at any time ('whenever possible') decreased from 6 to 1, and the number of those who 'never' enter, increased. Individual changes: 10 out of 19 respondents (52.6%) improved, 2 declined, 7 (36.8%) did not change (2 students kept the best practice).

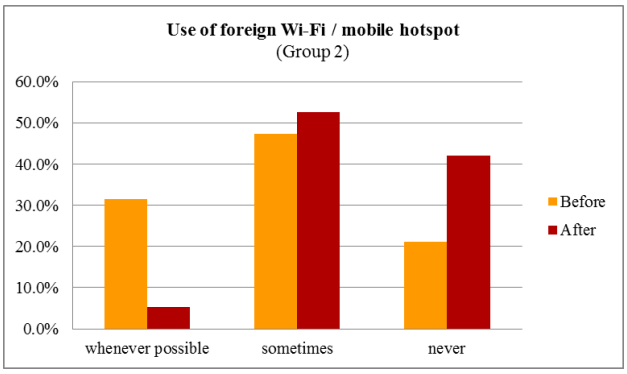

Figure 12. Change in the use foreign Wi-Fi (Group 2)

B. *Analysis of score differences*

After having reviewed the direction and the extent of changes regarding the observed variables, it is worth summarizing how many variables seem to be rather improved, or, in contrast, declined or actually stagnated in relation to each student, based on the analysis of score differences. In addition to the increase of the score, keeping the best practice is also reckoned to be a positive sign, therefore it was relevant to be recorded when students are stagnant at the maximum score can be obtained. Tables VII–X show the cumulated statistics of the variables.

TABLE VII.
SIMULTANEOUS IMPROVEMENT OF THE EXAMINED VARIABLES

Improvement (higher score achieved)				
Number of variables	**Group 1**		**Group 2**	
	freq.	**%**	**freq.**	**%**
0	8	29.63	1	5.26
1	11	40.74	2	10.53
2	6	22.22	5	26.32
3	2	7.41	4	21.05
4	0	0.00	3	15.79
5	0	0.00	4	21.05
Total	**27**	100.00	**19**	100.00

TABLE VIII.
KEEPING THE BEST PRACTICE REGARDING THE EXAMINED VARIABLES

Keeping the best practice (maximum score maintained)				
Number of variables	**Group 1**		**Group 2**	
	freq.	**%**	**freq.**	**%**
0	19	70.37	10	52.63
1	6	22.22	7	36.84
2	2	7.41	1	5.26
3	0	0.00	0	0.00
4	0	0.00	1	5.26
Total	**27**	100.00	**19**	100.00

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

TABLE IX.
SIMULTANEOUS STAGNATION OF THE EXAMINED VARIABLES

No change (earlier submaximal score maintained)				
Number of variables	**Group 1**		**Group 2**	
	freq.	**%**	**freq.**	**%**
0	0	0.00	4	21.05
1	0	0.00	4	21.05
2	6	22.22	2	10.53
3	5	18.52	7	36.84
4	8	29.63	1	5.26
5	5	18.52	1	5.26
6	3	11.11	0	0.00
Total	**27**	100.00	**19**	100.00

TABLE X.
SIMULTANEOUS DECLINE OF THE EXAMINED VARIABLES

Decline (lower score achieved)				
Number of variables	**Group 1**		**Group 2**	
	freq.	**%**	**freq.**	**%**
0	13	48.15	12	63.16
1	9	33.33	7	36.84
2	5	18.52	0	0.00
Total	**27**	100.00	**19**	100.00

Group 1: Half of the video group members took a step backwards regarding one or two variables, the majority of them presented stagnation with regard to several variables, though they could have been improved.

Group 2: In the group supported by both video demonstration and multimedia password retrieval programs, there was greater improvement concerning several variables. 63.2% of respondents did not take a retrograde step at all, moreover, 7 students (36.8%) did perform worse only in respect of one password variable. 21% of them did not change (i.e., they either showed an improvement regarding all variables or maintained the best score).

C. *Comparisons on background variables*

Password variables and mobile hotspot usage were examined using group comparisons on demographic and other background variables by means of nonparametric (Mann–Whitney and Kruskal–Wallis) tests.

According to our results, password usage habits and mobile hotspot usage could not have been differentiated by gender, place of residence (i.e., village, small town, city or capital), parents' educational qualifications, time spent on the internet either on school days or on free days, and interest in humanities or science. Except for two cases of password storage variable, comparisons on category variables did not show any significant difference either before or after the course. However, due to the small number of cases within categories (i.e., low cell frequencies), we are not allowed to draw a far-reaching conclusion.

Before the course, according to the comparison of password storage practices on the time spent on the internet on school days, there was a significant difference in the case of *Group 1* ($p = 0.024$); on the other hand, *after* the course, according to the comparison of password storage practices on the time spent on the internet on free days show a significant difference in *Group 2* ($p = 0.020$). Actually, those who spent 2–5 hours on the internet did not store their passwords securely (e.g., they allowed the browser to save them or noted down some of them).

After the course, in *Group 2*, there was a significant difference in password length ($p = 0.029$) between students with and without European Computer Driving Licence (ECDL) certification. Students having certificate proved more likely to use longer passwords.

D. *Relationships between variables*

The relationships between the password and mobile hotspot variables were investigated by the nonparametric Spearman rank correlation procedure. Spearman's rank correlation coefficient is denoted by the Greek letter ρ (rho).

D.1. *Correlations between paired variables of pre-test and post-test observations*

The results of the correlation analysis are given in Table XI.

TABLE XI.
CORRELATIONS BETWEEN PAIRED VARIABLES OF PRE-TEST AND POST-TEST OBSERVATIONS

Variable:	Password length		Password complexity		Password diversity	
Group:	**1**	**2**	**1**	**2**	**1**	**2**
ρ =	**0.657**	**0.535**	0.168	0.351	**0.699**	0.117
p =	0.000	0.018	0.401	0.141	0.000	0.634
Variable:	Password change		Password storage		Mobile hotspot	
Group:	**1**	**2**	**1**	**2**	**1**	**2**
ρ =	0.357	**0.666**	**0.775**	0.084	0.354	0.337
p =	0.067	0.002	0.000	0.732	0.070	0.158

Based on that, we found that the safer the password usage was before the course, the more secure was after it according to the following variables:

Group 1: In the case of password length, password diversity, and password storage variables, the correlation was stronger than moderate and significant even at a significance level of 0.01 too.

Group 2: In the case of password length and password change variables, the correlation was also stronger than moderate; and for the password change variable it was significant at a level of 0.01 as well.

Otherwise, the weak correlations can be interpreted as the earlier password usage patterns were not decisive in respect of the latter ones; as seen above, most variables in *Group 2* improved significantly.

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

D.2. Correlations of different variables before and after the course

Instead of the correlation matrix only the significant relationships are given below.

Group 1:

Before the course, the negative correlation between the password diversity and password length variables was slightly weaker than moderate ($\rho = -0.400$; $p = 0.039$); which means that the more characters were used in the passwords, the less diverse were the passwords themselves used in different systems. A significant, positive, weaker than moderate correlation was shown between password diversity and use of foreign Wi-Fi (mobile hotspot) ($\rho = 0.388$; $p = 0.046$); i.e., those who were more consistent in the use of different passwords for different services, they were likely to connect more cautiously to a foreign Wi-Fi or mobile hotspot, and vice versa.

After the course, the correlation between password diversity and password change frequency was significant, positive, slightly weaker than moderate ($\rho = 0.400$; $p = 0.039$); in other words, those who used more various passwords were more likely to change them more frequently.

Group 2:

Before the course, there was a relatively strong, negative, significant correlation between password diversity and password storage ($\rho = -0.722$; $p = 0.000$); in other words, the more different passwords were used, the less securely were they stored (for example, some of them were noted down).

After the course, there was no significant correlation between the examined variables. The correlation between the two variables previously showed a relatively strong relationship became much weaker ($\rho = -0.123$; $p = 0.616$).

E. Multidimensional scaling

To reveal the structure behind the variables measuring the password usage patterns, multidimensional scaling (MDS) [15] was applied with standardized variables, based on Euclidean distance definition. By this method, the relationship between the variables could be studied in a reduced dimensional space.

The password variables were measured not on the same scale, therefore they were standardized in order to be more comparable (actually, by dividing the score values by the maximum score of the particular scale).

In the case of *Group 2*, the two-dimensional derived stimulus configuration of standardized variables has very good measures of goodness-of-fit before the course (Stress = 0.00384; RSQ = 0.99982) and after the course as well (Stress = 0.00498; RSQ = 0.99983). The Stress values are much smaller than 0.025, which indicate that the original and the reduced spatial distances have excellent correspondence, and the dimension reduction produced no relevant information loss. The RSQ value is very close to 1, which shows an excellent fit with respect to the original and the reduced structure.

The two-dimensional configurations of the data before and after the course are shown in Fig. 13 and in Fig. 14, respectively. The variables for the pre-course measurements are marked with index 1, and for the post-course measurements are followed by index 2.

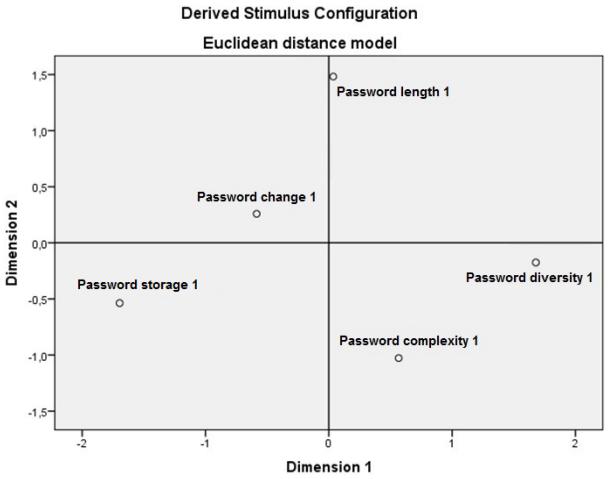

Figure 13. Two-dimensional model before the course

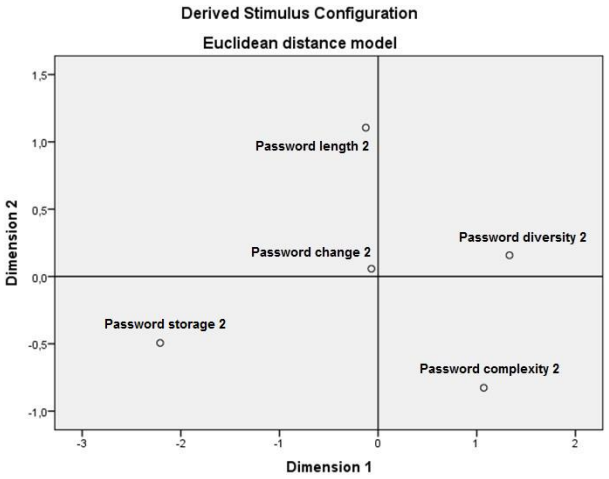

Figure 14. Two-dimensional model after the course

The *horizontal* axis (Dimension 1) represents the dimension of safe/unsafe password usage: higher coordinate value indicates safer password usage; smaller coordinate value indicates lower security, and thus, greater security risk.

The *vertical axis* (Dimension 2) can be interpreted as the dimension of awareness: higher coordinate value indicates more conscious password usage (i.e., information security awareness is of higher level).

The points right on the axis (with a coordinate value of 0) show the average.

Interpretation of the results: Based on the examination of the 'aggregate standardized password scores' (which are defined as the summation of the standardized password variables), a significant improvement can be indicated (according to the result of the Wilcoxon test: $p = 0.000$). The average values showed an increase in both dimensions. If a variable shows an average degree of improvement in a dimension, its position relative to the axis (i.e., its coordinate value) does not change in the dimension implied. If the improvement is greater than the average, the related coordinate value increases, if it is lesser, then it decreases.

The coordinates of the stimuli (two-dimensional MDS representations of the variables) are provided in Table XII.

Journal of Applied Multimedia 3./XIII./2018
DOI: 10.26648/JAM.2018.3.002

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

TABLE XII.
STIMULUS COORDINATES

Stimulus coordinates	Before (1)		After (2)	
	Dimension		**Dimension**	
Stimulus name	**1**	**2**	**1**	**2**
Password length	0.0361	1.482	-0.1246	1.1053
Password complexity	0.5666	-1.028	1.0711	-0.8268
Password diversity	1.6789	–0.175	1.3314	0.1578
Password change	-0.5854	0.2586	-0.0681	0.0574
Password storage	-1.6963	-0.538	-2.2097	-0.4937

In the followings, a more detailed explanation will be presented regarding each variable.

a) *Password length:* The security level in connection with password length is average. It shows a significant improvement, but less than the average compared to other variables, so its coordinate slightly decreased (to a small negative value). (The majority of the students use passwords shorter than 14 characters.) This variable indicated the most conscious behavior before and after the course. It is also supported by the students' comments on their password habits: their use of longer passwords is conscious and on the increase.

b) *Password complexity (variability of character types)*: The security level was and remained above average. The level of awareness was and remained below average, but showed improvement. The reason behind this may be the similarity in students' practice of using many character types in their passwords, which make it difficult to differentiate and express awareness numerically. However, many students mentioned that they did not change their passwords more often because they use (long and) complex passwords with a variety of characters.

c) *Password diversity:* The security level of this variable was above average, moreover, the highest before and after the course (the majority of students used partially or completely different passwords), however, the related coordinate value slightly decreased (since the security level increased in the case of other variables; causing a shift to a higher value of average consequently). The level of awareness increased slightly above the (new) average from a former below-the-average level.

d) *Password change frequency:* Its security level was below average before and after the course, but improved, approaching the average. The change of passwords requires conscious behavior. Before and after the course, it was more conscious than the average; though its coordinate value slightly decreased.

e) *Password storage:* Both the level of security and awareness were below the average for this variable. Awareness showed a slight improvement, while security showed a bigger downturn. Many of the students commit their passwords to memory, which is not necessarily a conscious behavior. 10 out of 19 students (half of the respondents) did not change, 6 students improved, 3 declined. The number of students who save their passwords into the browser is not high (4 out of 19), but did not decrease by the end of the academic year. Saving password into the browser is a comfortable but not a conscious (moreover, unsafe) behavior.

In the case of *Group 1*, there were no significant changes, so MDS maps and their analysis will not be presented here. (Nevertheless, the goodness-of-fit of the two-dimensional reduced configurations are excellent both at the beginning and at the end of the academic year. Measures before the course: Stress = 0.02418; RSQ = 0.99559; and after the course: Stress = 0.00298; RSQ = 0.99988.)

F. Qualitative analysis

Students' answers to open-ended questions are very instructive. For instance, we asked students what reason they change or not their passwords for. It turned out that many students consider their passwords to be safe because of one or two attributes (e.g., because they are long or complex), and due to the associated sense of security they do not feel the need to change their passwords at all or more frequently. Others referred to their own indolence or that their passwords are literally 'at their fingertips' (i.e., they can type them very fast, automatically, from motor memory). In other words, considerations of security were subordinate to considerations of convenience.

In *Group 1*, before the course 12 out of 27 respondents (44.44%), after the course 20 students (74.04%) mentioned security aspects to be a priority (e.g., they take care of security or they consider their passwords to be secure). Even though they knew a lot about security issues, their password habits did not show significant improvement by the end of the academic year. It may be surprising that in *Group 2*, before the course 18 out of 19 respondents (94.74%), after the course 15 students (78.95%) mentioned security to be taken into considerations; the remaining ones referred to laziness (e.g., admittedly, some of them even wrote down they should have changed their password more frequently, still, were lazy to do it). Therefore, it is not enough to be informed, but students should follow appropriate attitude and take responsibility to use their passwords safely and protect their data and systems.

IV. DISCUSSIONS AND CONCLUSIONS

This study provided important lessons from didactic point of view and for the reason of planning further research and development.

Both student groups involved were trained by using multimedia tools during the education. We demonstrated the vulnerability of passwords and called students' attention to the importance of personal password management and information security awareness in various ways. It was demonstrated that the educational method supported by multimedia password retrieval programs, consequently, facilitating students' interactive participation had greater impact on students' information security practices, attitudes, and awareness than the method applying only video demonstration which provides purely a passive reception.

The discussion of the results suggests that the difference between the two groups, i.e., the different effectiveness of the applied educational methods is based on to what extent they can involve students in the learning process as active participants rather than passive recipients.

The research also highlighted the areas that should be paid more attention to during the education, particularly

Received: 07 August 2018
Accepted: 30 September 2018
Published: 15 October 2018

where there was no significant improvement (such as regarding password storage), yet involving other methods could also be useful. (Even if we dealt with security of password storage during the course, the testing of password decrypter programs did not provide new experiences about it, and consequently, could not influence directly the password storage habits.)

This study was conducted involving a small sample from a year of a certain university program therefore our conclusions are limited. However, on the basis of our promising results it would be worthwhile to continue the research and carry out further analysis and development of teaching tools and methods.

The password retrieval programs used during the course could be tested on personal computers and laptops. However, keeping up with the constantly evolving technology and with the continuous change in the students' device usage habits, we aimed at developing new multimedia programs for mobile devices, both iOS and Android mobile operating systems.

The use of multimedia password retrieval programs in education can be characterized by the main features of educational virtual reality (VR): (1) "…[i]t [i.e., VR] creates a simulated environment (…), where the learner can take on the roles of observer, participant and creator"; (2) "[i]t creates complex circumstances and media for the possibility of immersion and (…) experience ..."; (3) it forms a link to situations that are difficult to access; (4) it creates the possibility of protected and safe experiences [16, p. 10]. The use of the program in human–computer interaction creates a simulated space, a kind of VR that supports the students' experiential, situated, observational, and activity-based learning [16, pp. 11–12]; in other words, it creates the possibility of individual experience, action, experimentation, knowledge testing, and encounters in a novel, virtual environment where the consequences of activities are apparent without causing real damages to the physical world.

The analysis of efficiency also highlighted one of the essential features of VR in the field of educational application. Originally, the term referred to "immersive virtual reality", i.e., the user plunges into this artificial world. Regarding the efficiency of training, the point is not that the user is being surrounded by a computer-generated three-dimensional world but rather the personalized student activity itself.

Acknowledgment

We would like to thank András Simon (Semmelweis University, Faculty of Health Sciences) and Dr. Gábor Szász (professor emeritus, Dennis Gabor College) for their valuable comments.

References

[1] G. Kiss and A. Szász, "Analysing of the Information Security Awareness of the Economic Information Technology Students", In *Proceedings of the 17th IEEE International Symposium on Computational Intelligence and Informatics – CINTI 2016*, Szakál, A., ed., Budapest: IEEE Hungary Section, 2016, pp. 213–218. DOI: https://doi.org/10.1109/CINTI.2016.7846406.

[2] G. Kiss and A. Szász, "Level of the Information Security Awareness of the Mechanical Engineering Students", in *Proceedings of the 15th International Conference on Information Technology Based Higher Education and Training (ITHET 2016)*, Kaynak, O. ed., Istanbul: IEEE Computer Society, 2016. DOI: https://doi.org/10.1109/ITHET.2016.7760758.

[3] G. Kiss, Z. Árki, and A. Szász, "Level of the information security awareness of the nursery school students", *TOJET: Turkish Online Journal of Educational Technology*, Special Issue for INTE 2016, pp. 51–60, Dec 2016.

[4] G. Kiss and A. Szász, „A gépészhallgatók információbiztonság-tudatosságának elemzése" [Analysis of the information security awareness of the mechanical engineering students], *GÉP*, Vol. 67. No. 7–8, pp. 5–8, 2016.

[5] A. Ferrari, Y. Punie, ed., and B. N. Brečko, ed., *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*. Luxembourg: Publications Office of the European Union, 2013. DOI: https://doi.org/10.2788/52966.

[6] R. Vuorikari, Y. Punie, S. Carretero, and G. Van Den Brande, *DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model*. Luxembourg: Publications Office of the European Union, 2016. DOI: https://doi.org/10.2791/11517.

[7] S. Carretero, R. Vuorikari, and Y. Punie, *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of us*e. Luxembourg: Publications Office of the European Union, 2017. DOI: https://doi.org/10.2760/38842.

[8] J. Ollé, „Interaktivitás és tevékenység-központúság az oktatásinformatikában" [Interactivity and activity-centered methods in educational informatics], In *Interaktív oktatásinformatika*, Lévai, D. and Papp-Danka, A., eds., Eger: ELTE Eötvös Kiadó – Eszterházy Károly Főiskola, 2015, pp. 9–16.

[9] D. Lévai and A. Papp-Danka, eds., *Interaktív oktatásinformatika* [Interactive educational informatics]. ELTE Eötvös Kiadó – Eszterházy Károly Főiskola, Eger, 2015.

[10] Ollé J., Papp-Danka A., Lévai D., Tóth-Mózer Sz. és Virányi A., *Oktatásinformatikai módszerek. Tanítás és tanulás az információs társadalomban* [Educational informatics methodology. Teaching and learning in the information society]. ELTE Eötvös Kiadó, Budapest, 2013.

[11] A. Keszthelyi, About passwords. *Acta Polytechnica Hungarica*, Vol. 10, No. 6, pp. 99–118, 2013.

[12] A. Keszthelyi and E. Kadëna, "Misunderstanding how Passwords Work", in *Management, Enterprise and Benchmarking in the 21st Century, III*. Michelberger, P. ed., Budapest: Óbuda University, Keleti Faculty of Business and Management, 2016, pp. 83–92.

[13] S. Siegel, *Nonparametric Statistics for the Behavioral Sciences*. New York: McGraw-Hill, 1956.

[14] E. L. Lehmann, *Nonparametrics: Statistical Methods Based on Ranks*. Revised edition. New York: Springer-Verlag, 2006.

[15] J. B. Kruskal and M. Wish, *Multidimensional Scaling*. London: Sage Publications, 1978.

[16] P. Aczél, "Virtual reality and education – world of teachcraft?" *Perspectives of Innovations, Economics and Business*, Vol. 17, No. 1, pp. 6–22, 2017. DOI: http://doi.org/10.15208/pieb.2017.02.