Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam

Phuong Thao Mai[1], **Andrea Tick**[2]

[1] Doctoral School on Safety and Security Sciences, Óbuda University
Népszínház u. 8, 1081 Budapest, Hungary, thao.mai@stud.uni-obuda.hu

[2] Keleti Károly Faculty of Business and Management, Óbuda University,
Népszínház u. 8, 1081 Budapest, Hungary, tick.andrea@uni-obuda.hu

Abstract: Within the digital culture, the increasing internet consumption and the constant development of technology, especially smartphones have made cyber awareness turn to be increasingly urgent. This study focuses on comparing the level of cyber security awareness, knowledge and behavior among university students in general and between Hungary and Vietnam in particular. Research data was collected, using a set of questionnaires and the 313 responses from University Students, in different school years and fields of study, in Hungary and Vietnam. Quantitative analysis was conducted using SPSS. Results show that all respondents possess a lack of knowledge of cyber security, leading to a low level of cyber threat awareness, beyond the differences in respondent countries. However, there are minor differences in the behavior, between respondents in Hungary and Vietnam, which were measured through four dimensions of cyber security: malware items, password usage issues, social engineering and online scam issues. This research helps to raise awareness of differences in cyber security mindfulness, due to cultural characteristics, that can be considered, when developing global mega-systems, such as, social platforms.

Keywords: Cyber security; internet security; online threats; smartphone usage; student awareness; student behavior; Hungary, Vietnam

1 Introduction

The rapid and dramatic development of information technology, over the recent decade, cannot be denied. Especially in the current context of the Industry 4.0, the massive global rates of internet consumption by individuals and organizations in all of governmental, industrial and also academic sectors, together with the diverse development of smartphone and digital applications have significantly transformed the society as well as daily life [1, 2]. Regarding education sector, the

information and knowledge society in the "digital society" has generated enormous challenges to universities and academic institutions regarding the digitalization in education system such as the comprehensive integration of digital, online, e-learning educational forms, the exploration of industrial and business academic programs, and the possibility of their complex integration into higher education at all levels. Across the globe, the spread of novel coronavirus COVID-19 since early 2020 has led to profound challenges in social interaction, organization as well as the education sector. When the policies on lockdown and social distancing are taken place in most of the countries in the world, one of the most urgent responses to the pandemic applied to maintain educational activities in any higher education institutions is switching all face-to-face forms of education to e-learning/digital learning forms. With the emergent current situation due to the pandemic, the digital competences, skills and practices are indispensable. Along with immediate getting used with the new form of study, students' security awareness in the digital learning environment has been raised as one of the most concerned issues that need to be addressed recently.

Based on distinctions in economic, cultural and social aspects, Vietnam is currently a developing country which has been strongly stimulated to become a high-income economy by 2045 [3]; meanwhile, Hungary is a high-income economy, which was transformed from a developing to developed country. The paper aims to compile a comparative study on the cyber security behavior of students in Hungary and Vietnam. It raises the questions whether in the virtual society created by social networks, the internet where global mega-systems can be used by anyone all over the world, the differences of nations, cultures and educations should be considered at all in relation with cyber security on smart phone. The question arises whether there are peculiarities regarding cyber security on smart phone in the various cultures and countries among students in higher education that must be kept in mind. This paper initially focuses on two different cultures, Hungary and Vietnam and makes an effort to show the differences, linked to the cyber security on smart phone, between these two cultures, among the higher educated students. As a first step, two countries were chosen from a developing and transition economy, on purpose, aiming to reveal the differences. The research findings would help to compare these countries to countries of similar economic and cultural backgrounds. Furthermore, it is expected that the research results of this study would provide the input to future research, in which, the research scale of countries could be expanded. With this goal, more countries with different economic and cultural backgrounds will be compared.

2 Literature Review

2.1 Digital Society in 2020 - the Comparative Context between Hungary and Vietnam

Digital, mobile, and social media have played a vital role in people's everyday life all over the world. Digitalization together with information technology has revolutionized both products and services [4]. It is emphasized that human lives have entered a whole new global age in which countless unfolded opportunities would touch every aspect of life. According to the international official report on digital world in 2020 [5], over 4.5 billion people have been using the internet which account for 59% of total population in the world, meanwhile social media users have passed the 3.8 billion mark. As stated in statistics from January 2020 [6], the total number of people around the world using the internet have increased by 7% with 298 million compared to the corresponding period last year that make the total internet users reach to 4.54 billion. In particular country scale regarding this study, compared to the total population of Hungary in 2020 (9.67 million), there have been 7.64 million internet users until January 2020 which account for 79% [7]. In Vietnam, there have been 68.17 million internet users in 2020 which make up 70% of total population of the country; Compared to January 2019, the number increased by 6.2 million (10.0%) [8]. Thanks to the huge number, Vietnam is ranked as the top 9^{th} worldwide for the internet growth. It is claimed that mobile phone has accounted for over half of total time that people spent on when being online using the internet of people [6]. Specifically, nearly 246 million mobile connections in Vietnam in January 2020 (equivalent to 150% of the total population) in which up to 93% of the total internet users aged from 16 to 64 using smartphone. It is noticed that the daily time accessed the internet via smartphone by internet users aged from 16 to 64 in Vietnam is 3 hours 8 minutes which is considered as a half of the worldwide average time per day spent using the internet by the same age range of respondents. Regarding the mobile connections in Hungary in 2020, there have been more than 11.6 million mobile connections until January that increased by 2.2% compared to the corresponding period last year (equivalent to 120% of the total population) [7] [8]. According to Figure 1, there is a big difference in the rate of smartphone owners, the average download speed for fixed internet connections (MBps/100), and in mobile connections between Hungary and Vietnam.

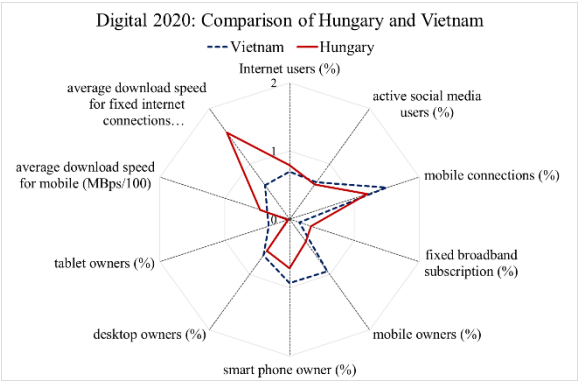

Figure 1
Digital 2020: Comparison of Hungary and Vietnam [5-10]

2.2 The Impact of Internet and Cyber Risk on Society and Individuals

An evolution of the internet, followed by a booming of digital media has brought about drastic changes in learning, information access and knowledge construction. Particularly, cyberspace has facilitated the way people communicate and socialize. Because of the increasing connection with high technology, people use internet for more social connecting in both personal and professional environments such as daily conversation, business work, online services (banking, education and virtual healthcare, etc.). In this line, even operation manner of businesses has been changed thanks to the emergence of the internet and high technologies. It is certain that internet became the fastest-growing communications medium in the last decades [11]. This means that the internet consumption buttressed by information technology improvements has been increasing dramatically. However, being continuously connected, also causes more cyber security risks, which could be cyber threats against a critical infrastructure and economy. To individual internet users, cyber security risks can result in threats to confidential identity, identity as well as privacy [12]. Furthermore, the existence of cyber risks also emerges which are explicitly cybersex, pornography, personal information exposure, cyber addiction, online fraud, addiction towards gaming and gambling, which have negative effects on adults and children [13]. The authors of the study [14] emphasized the effect of the cyberspace toward the daily life: "In our technology and information-infused world, cyberspace is an integral part of the modern-day society. In both personal and professional contexts, cyberspace is a highly effective tool in, and enabler of, most people's daily digitally transposed activities." In the meantime, another study [2] has emphasized that the majority of internet users still lack sufficient awareness of various internet threats/ cyber hazards.

Online study has become an integral part of higher education thanks to the availability of internet resources and constantly has been critical for the future of higher education [15, 16]. At the same time, it is emphasized that internet access together with information technology provide a great extent of flexibility and autonomy for the students [17]. Thus, attitude and perception of the students to cyber security would play a vital role in their self-protection from online threats to their daily online activities. It is noticed that people are recently more dependent on the internet technologies for their daily tasks which have facilitated the extending scale of the involvement in cyber-related activities; whilst the fundamental knowledge needed for preventing from cyber threats correspondingly is lagging [18]. Furthermore, it is also argued that even the basic level cyber security awareness is not sufficient enough for mitigating cyber risks and threats [2, 18]. A study [19] found out that cyber security in mobile phone using has been largely studied in technical aspect while the role of the human aspect who interact with technology is overlooked. As such, further studies cause concern regarding more insights and practices would be critical, to not only individuals, but also the educational sector and other related organizations.

Regarding research topics on cyber security and individual cyber engagement, individual attitudes and behaviors concerning cyber threats have attracted the attention of both academic scholars and practitioners [20, 21]. There have been also a number of studies about cyber security awareness of individual and organization, and the effect of cyber-attacks to internet users. To be more specific, studies on information security awareness in both governmental organizations and private sectors on the level of individual resilience with cyber security awareness as a cause of job stress [22, 23]. Similarly, studies [24, 25] provided more insights about understanding of how employee awareness and attitudes contribute to a company or organization's cyber security, as well as focusing on cyber regulations and the establishment of security policies. Regarding studies on cyber security awareness in education sector, authors of the research [26] have measured the influence of a cyber-security awareness campaign for school youth. After conducting their study based on carrying on the campaign, they found a great impact on cyber security awareness of the targeted school youth when compared with their existing knowledge related to cyber security hazards. However, authors in the study [2] strongly emphasizes that lack of cyber awareness is still a serious global problem while there is still little attention to research on the relationships between individual cyber security awareness, knowledge and behavior which is based on comparative analysis between countries; especially, in smartphone using. In fact, the comparative approach for studies in this area plays a crucial role for the creation of intervention programs [27]. Furthermore, the new milestone in the development of smartphone thanks to the endless innovation in its technology and convenience could not be denied. Simultaneously, the number of internet users who access the internet via smartphone has been constantly increased with up to 91% until January 2020 [6]. This implies that more potential cyber threats could attack not only individuals, but also organizations, education institutions as well as

governments at any time and this could be the most concerned topic than ever. Therefore, further research on cyber security in smartphone use, particularly as a comparative evaluation of the level of awareness across different countries, is crucial, not only for individuals, but, also, the educational sector and other related organizations and governments.

3 Research Methodology and Research Questions

This study was conducted, seeking to answer the following research questions:

1) What is the different state of cyber security awareness of higher education students between Hungarian and Vietnamese students?
2) What are the main factors impacting on the difference level of cyber security awareness of students between Hungary and Vietnam?
3) How similarly do university students behave between the two countries regarding using smartphone through cyber security dimensions?
4) What segments of students regarding cyber security awareness can be found and which are the most influential factors in creating the segments?

Quantitative research method is applied in this study which uses both primary and secondary data for the analysis. Specifically, the statistics analysis is chosen for this study to collect primary data through online questionnaire surveys. The respondents are selected using samples of target population and the purpose. The research population for this research comprised university students in the two countries: Hungary and Vietnam. Because of the large population sizes, researcher was unable to test every person in the total population due to some contrasts in time and budget, especially under the current circumstances of Covid-19. Therefore, this research relied on sampling and applied non-probability, convenience sample. The research data was collected using a set of online questionnaires answered by 313 university students in different school years and different field of study in Hungary and Vietnam in which 191 respondents are students in Hungary (61%) and 122 respondents are from Vietnam (39%).

The targeted respondents received the survey via social media and e-mail, and they were asked to spend from 5 to 7 minutes on this questionnaire. The questionnaire included three parts, (a) personal demographic information, (b) a set of 15 questions on the awareness of cyber security on smartphone – both parts comprise both types of Yes/No and multiple choices questions – (c) respondents were requested to indicate their rate of agreement with statements on cyber security dimensions. The instrument in part three was structured in the Likert fashion, on a 5–point scale, ranging from:

1 - Totally disagree

2 - Partly disagree

3 - Neutral

4 - Partly agree

5 - Strongly agree

A pilot testing for confirming the validation of the questionnaire was done by a number of random students at university level in different countries such as Australia, Hungary, the USA, the United Kingdom and Vietnam excluded from the targeted audience group who actually participated in the study's result contribution.

For the purpose of the study Pearson's Chi-squares test of independence, independent samples t-tests and the decision tree method were applied to reveal the similarities and differences in the cyber security behavior of students in Hungary and Vietnam when using smartphones.

4 Results and Analysis

4.1 Demographic Profile

The study respondents were university students of Óbuda University in Hungary and the University of Danang in Vietnam. In the total 313 respondents of the survey, up to 99.7% of respondents are using smartphone. Table 1 displays the respondents' demographic information. Regarding gender, it is shown that in general, female students make up the highest percentage which is 53.7%, followed by male student with 45.4% and others with 0.9%. In both Hungary and Vietnam, the majority of respondents are in the age between 19-22 years old which account for 63.6% of total number of respondents. The second highest percentage in age range of the respondents in both countries is 24.9% which represents for students in the age of 22-25 years old. This number has illustrated that the survey has approached well to the targeted respondents who are the most suitable research objectives for this study. Regarding the fields of study, up to 70.9% of total respondent percentage are studying in the field of Economics or Business Management. In addition, Engineering, Mathematics or Natural Sciences is the field of study that is second most studied by total respondents (13.7%), followed by other fields (11.8%), Medicine (3.2%) and Laws fields (0.3%). Due to the fact that the majority of the respondents study economics, not engineering or informatics, the behavioral attitude is expected to give valuable results. Further studies will be conducted to extend the sample to make it representative.

The duration of time using smartphone taken into account in this study could be an important factor affecting the experience of cyber security issues. Accordingly, there are up to 101 students using smartphone in 7-10 years in Hungary which account for the highest rate in all four periods of time with 32.3%. Meanwhile, the majority of respondents in Vietnam have been using smartphone in 3-6 years and 7-10 years, which account for 37.7% and 35.2% respectively. It is to be noted that up to 24% of total respondents in Hungary and 21% of total respondents in Vietnam who are in the range age of under young adults have experienced smartphone for over 10 years.

Table 1
Respondent's demographic information (in %)

Country	**Hungary**	**Vietnam**	**Total**
Gender: Male	50.0%	38.1%	45.4%
Female	49.0%	61.9%	53.7%
Others	1.0%	0.0%	0.9%
Age: Under 19	2.1%	5.9%	3.5%
19 - 22	63.4%	63.9%	63.6%
23 - 25	25.8%	23.5%	24.9%
Over 25	8.8%	6.7%	8.0%
Smartphone Usage: Yes	100.0%	99.2%	99.7%
No	0.0%	0.8%	0.3%
Fields of Study: Economics or Business Administration	82.0%	52.9%	70.9%
Engineering, Mathematics or Natural Sciences	10.3%	19.3%	13.7%
Medicine	0.5%	7.6%	3.2%
Law	0.0%	0.8%	0.3%
Other fields	7.2%	19.3%	11.8%
Duration of using smartphone: Under 3 years	2.1%	6.1%	3.5%
3-6 years	21.1%	37.7%	27.5%
7-10 years	52.8%	35.2%	46.0%
Over 10 years	24.0%	21.0%	23.0%

Based on the responses of the question about online activities, all the respondents claimed that they spent most of the online time via their smartphone. The respondents were asked to choose at least three activities that they spend time the most daily. As shown in Figure 2, accessing social networking sites is the activity that most of respondents in both Hungary and Vietnam choose, which means they are heavy social networking users.

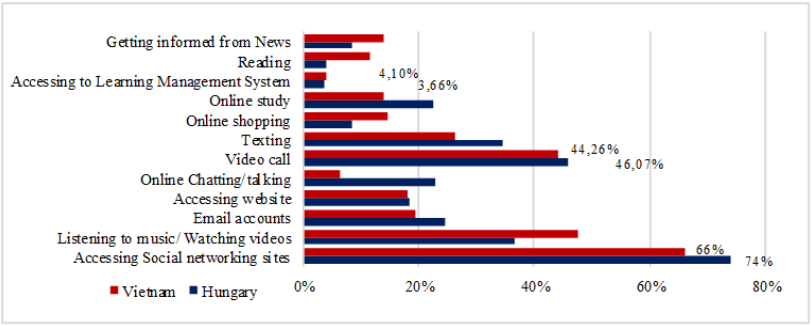

Figure 2

Online activities participated by the respondents in Hungary and Vietnam (in %) (Source: edited by authors)

Specifically, over 70% of total respondents in Hungary use smartphone to access social networking sites such as Facebook, Instagram, etc., and up to 66% of total respondents from Vietnam chose the same activities. In Vietnam, there have been up to 67% of total population using social media [8]. According to a research on Vietnamese students using social-internet-network [28], 100% of respondents ascertained that they got more than one social network accounts and the majority of students spend time on social networking from 1-3 hours per day. Furthermore, Figure 1, also shows that University Students in both Hungary and Vietnam, use their smartphones for mostly, entertainment activities (listening to music/watching videos) and communication (texting, chatting, video calls); instead of, for study purposes (emailing, reading book, online study, accessing websites).

Together with Figure 3, it is stated, that up to 70.2% of total respondents in Hungary and 61.5% of total respondents in Vietnam, are not willing to use a smartphone for accessing online study systems/applications or even getting online materials for their study. Preferences of students in Hungary and Vietnam are similar regarding the access of online learning management system via smartphone, as justified by the CHI^2 test supposing relationship between the preference and the country of origin (CHI^2=2.529, p=0.112).

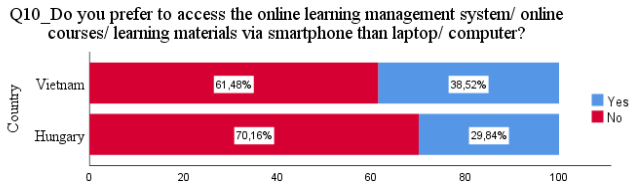

Figure 3

The intention of students to use smartphone for only study activities (Source: edited by authors)

The difference between online activities pursued by students in Hungary and Vietnam proved to be significant, despite the close percentages and some individual similarities, regarding certain activities (CHI^2=39.222, p=0.000).

4.2 Findings on Awareness of Cyber Security on Smartphone

The general awareness of cyber security of all respondents was analyzed with the question "Have you ever heard/ known about the term of cyber security?". Figure 3 shows the results of this question for comparing the knowledge of respondents in Hungary and Vietnam combined with the responses on the question of "desire to learn more on cyber security". Accordingly, it could be clearly seen, that the number of respondents in Hungary who know about cyber security is higher than in Vietnam, accounting for 84.8% of total respondents in Hungary; while the percentage of university students knowing about this term is 73.8%. When asked about their willingness to learn more about cyber security, 89.3% of respondents in Vietnam answered "Yes" while only 69% of respondents in Hungary gave the same answer. It is to be noticed that up to the nearly 40% of the "No" answers for this question to all respondents in Hungary is a relatively high ratio, which ought to be taken into account when 100% of them use smartphone daily and can face unexpected cyber threats from their phone at any time. Testing and comparing the difference of student behavior in Hungary and Vietnam on the above two questions a significant difference was detected between student behavior (CHI^2=26.963, p=0.000), which is due to the difference in the wish to learn more on cyber security being either aware of the term or not. The difference can be captured in Figure 4 illustrating how knowledge of cyber security leads to the desire to learn more on cyber security in Hungary, Vietnam and in total. The difference is well manifest in the "No" groups. In total, a larger proportion of students who answered "No" for the knowledge of the term Cyber security wishes to learn more about it, while the path is the opposite in Vietnam but similar in Hungary. It has to be highlighted that students who learnt about the term cyber security wish to learn more on it in both countries. The balance swings based on student awareness of the importance of cyber security. There is a higher awareness, in the case of Hungary, since student behavior shows that those who already knew about cyber security and might have realized the importance of being prepared for unpredictable cyber threats, are willing to study more about cyber security.

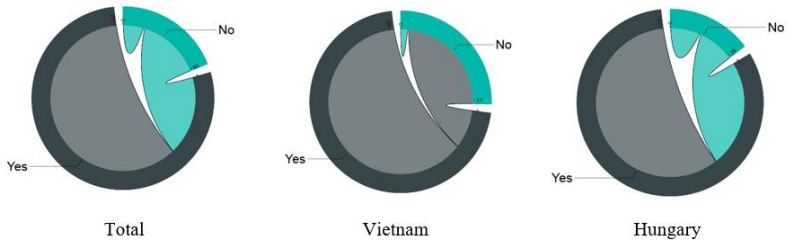

Figure 4

Knowledge of cyber security leads to desire to learn more on cyber security (Source: edited by authors)

The source of difference is shown in Table 2, stating that balance is turned to Hungary for the knowledge while it is turned to Vietnam for desire to learn.

Table 2
The significant difference in student behavior on the knowledge of the term Cyber security (Source: edited by authors)

Comparisons of Column Proportions		Country	
		Hungary (A)	Vietnam (B)
Cyber security knowledge	Q14_Have you ever heard or known about the term of "Cyber security"?	B (0.000)	
	Q16_Do you desire to learn more on security?		A (0.000)
Results are based on two-sided tests. For each significant pair, the key of the category with the smaller column proportion appears in the category with the larger column proportion. Significance level for upper case letters (A, B, C): .05			
a. Tests are adjusted for all pairwise comparisons within a row of each innermost sub-table using the Bonferroni correction.			

Furthermore, the awareness of respondents to cyber security while using smartphone and the difference between respondents in the two counties are also presented by analyzing the answers to specific questions. Accordingly, even though respondents are with their phone every day and spend time on them with many purposes (Figure 1), about half of all the respondents, in both countries, are not sure about their smartphone being virus infected, when their phone is not responding correctly, while 32% and 21% of respondents in Hungary and Vietnam, respectively, have no idea about this issue. For the aim of comparing the behavior of students in Hungary and Vietnam a significant difference was detected in case of the belief of the need of protection on smartphone (CHI^2=11.713, p=0.003) as shown in Table 3. The percentage of respondents in Vietnam is higher for "Yes" (76.2%) which implies that they are more skeptical about security protection while students in Hungary trust more their smartphones and care less about security protection with up to more than 40% of respondents are unsure and deny the necessity of security applications in their smartphone.

Table 3
Awareness of respondents on the need of smartphone security

Q18_Do you think that your smartphone needs security protection? (e.g.: antivirus application) * Country Crosstabulation				
	Country	**Hungary**	**Vietnam**	**Total**
Do you think that your smartphone needs security protection? (e.g.: antivirus application)	Yes	113_a	93_b	206
	No	58_a	17_b	75
	Not sure	20_a	12_a	32
Total		191	122	313
Each subscript letter denotes a subset of Country categories whose column proportions do not differ significantly from each other at the .05 level.				

Regarding the questions on the "possibility of a virus affected device in case of no response of smartphone" and "auto saving login information in smartphone", in both countries students behave similarly and approximately half of the students do not believe saving auto login information in smartphone as a good action from a security perspective (CHI^2=4.298, p=0.117 and CHI^2=5.797, p=0.055, respectively). With a significance level smaller than 5.5% there is a difference in auto login behavior of respondents between the two countries. A larger proportion of students in Vietnam compared to Hungary is not sure about the relation of security breach and auto login data savings meanwhile 54.5% and 48.4% in Hungary and Vietnam respectively are sure about the security concerns. What affirms the need of cyber security education is the relatively high percentage of students (28.3% and 23% in Hungary and Vietnam respectively) trusting saving auto login information. On contrary to the similar behaviors in case of the two questions above, students' approach to the need of smartphone security protection (e.g. antivirus app) in these two countries differ significantly (CHI^2=11.713, p=0.003). This significant difference makes the behavior different in the combination of the three concerns (CHI^2=8.232, p=0.041) as shown in Table 4.

Table 4

Students approach to security protection on smart phone (Column N %)

Country	Hungary	Vietnam	Total
Q17_Have you noticed that when your smartphone is not responding, it is most probably considered as a virus infected device?	27.7%	29.7%	28.6%
Q18_Do you think that your smartphone needs security protection? (e.g., antivirus application)	82.5%	92.1%	86.6%
Q19_Do you think that saving auto login information in your smartphone is good from a security perspective?	39.4%	27.7%	34.5%
The table contains a multiple response set with "Yes" answers as percentage of group totals exclusively.			

Together with the improvement of smartphone, mobile banking has developed by the diffusion of mobile communication technology to become an innovative and essential service to people around the world. Mobile banking is defined as "the financial services delivered via mobile networks and performed on a mobile phone" which is the recent trend in banking transition [29]. The era of mobile banking has arrived; applications can be downloaded for the simplest mobile banking facilities onto mobile phones. Pop-up windows often induce one to save credit card information for future online services without calling attention to its dangers. Students in Hungary and Vietnam behave similarly in the use of mobile banking and submission of credit card information (country comparison: CHI^2=2.831, p=0.304) i.e. the more students use mobile banking the more they save their credit card information (Hungary: CHI^2=34.392, p=0.000; Vietnam CHI^2=9.923, p=0.000 and Cramer's V equals 0.421 and 0.289 respectively).

4.3 Cyber Security Dimension Items

Table 5 describes the summative descriptive analysis of the variables in the four dimensions applied for evaluating the cyber security behavior of respondents. The present analysis shows the Mean, Median, Mode and the Interquartile Range (IQR) in descending order. The dimension on password and online scam issues were the most relevant while in the other two dimensions, there were some constant items. It could be seen that all the respondents in general show their highest awareness in the case of not considering any amount of money for services offered by an online site. Due to the number of constant responses, university students in both countries have shown the least aware behavior in the dimension of social engineering issues.

This study applied the Cronbach's alpha to assess the reliability of the instrument. The statistical validation was performed for each item as well as for the overall model as shown in Table 5. The Cronbach's alpha values were in the range from 0.782 to 0.791 (Table 5) in which each item had a Cronbach's alpha coefficient over 0.78. The overall Cronbach's alpha value, of all four dimensions in Hungary, was 0.79 while the value, when texting all respondents in Vietnam, only was 0.804. Reliability is considered acceptable when this score exceeds 0.70 (Hair et al, 1998). The overall reliability is 0.794 with all the items included.

Table 5
Descriptive analytics and reliability of Cyber security dimension items

Item	***Mean***	***Median***	***Mode***	***IQR***	***Cronbach's Alpha if Item Deleted***
Dimension 1. Cyber security behavior on malware items					
29. I prefer to update information on my study via computer	3.78	4	5	2	Deleted
27. I trust any information sent from my university online learning management system	3.59	4	4	1	0.786
24. I can sense something is wrong if my smartphone runs extremely slow.	3.55	4	3	2	0.788
26. I will apply security patches to my phone as soon as possible.	3.38	3	3	1	0.791
28. I prefer to update information on my study via my smartphone	3.03	3	3	2	0.789
23. An interesting subject line makes me open an email attachment.	2.42	2	1	2	0.790
25. I'm willing to download materials from unsecure sites.	2.30	2	1	2	0.790
22. I'm willing to open email or message attachments from strangers.	2.18	2	1	2	0.786

Dimension 2. Cyber security behavior on password usage issues					
30. My password consists of lowercase, uppercase, numbers, special characters.	3.87	4	5	2	0.789
30. My password doesn't follow keyboard pattern.	3.35	3	5	3	0.790
36. I do use the "Remember my password" option in my phone.	3.15	3	4	2	0.785
32. I use a similar password for different applications.	3.12	3	4	2	0.782
34. My passwords are based on my personal information.	2.71	3	1	3	0.786
35. I never change passwords.	2.55	3	3	2	0.784
37. I keep my password somewhere in my phone.	2.41	2	1	3	0.789
31. I can share passwords with other people.	1.86	1	1	2	0.790
Dimension 3. Cyber security behavior on social engineering issues					
44. I wouldn't reveal any confidential information under any circumstances.	3.73	4	5	2	0.787
42. I check the authorization or identity of someone before talking on any issues.	3.55	4	3	1	0.788
43. I wouldn't communicate with a stranger although his/her looks warrant sympathy.	3.35	3	3	1	0.787
41. I'm not willing to respond to calls, SMS, or email messages to friendly/ non-threatening strangers.	3.28	3	3	2	0.785
40. I think I'm not a target of social engineering attacks due to student status.	2.78	3	3	1	0.785
39. I'm not interested in reading social engineering issues.	2.76	3	3	2	0.785
Dimension 4. Cyber security behavior on online scam issues					
47. I never trust strangers identity information given on the Internet.	3.45	3	3	2	0.791
49. I'm aware of and able to identify the latest online scams.	3.38	3	3	1	0.785
48. I never consider any amount of money for services offered by an online site.	3.19	3	3	3	0.786
50. I wouldn't hesitate to meet internet friends in person.	2.75	3	3	2	0.788
45. I established trusted online relationship with strangers.	2.36	2	1	1	0.786
46. I respond to SMS announcing contests involving huge sums of money.	1.96	1	1	2	0.794

The visual representation of the mean responses (Figure 5) shows a slight or weak difference between the responses of the students in the countries separately (the numbers represent the index of the statements in the Table 6). The correlation of mean responses for the items between Hungary and Vietnam, is r=0.985, which also suggests similar behavior, so further tools – independent samples t-test and the CHAID decision tree method for segmentation of categorical data – helped to find similarities and differences between the countries.

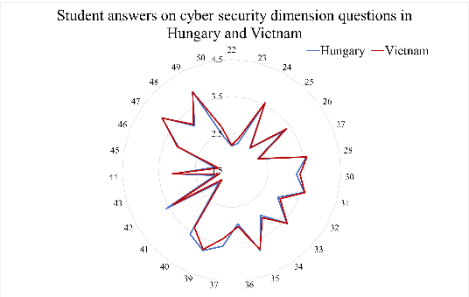

Figure 5

Student responses on cyber security dimension questions (source: edited by authors)

4.1.1 Significance of Cyber Security Dimension Items

The comprehensive reliability of the items in the dimensions of cyber security on smartphone for the two countries in question and the reliability of the individual items allow a comparative analysis between the students in these countries. In order to find the significant items in the dimension's independent samples t-tests were conducted on the items to compare the behavior in Hungary and in Vietnam (Table 6).

Table 6

Significant differences between Hungary and Vietnam

Independent Samples t-test	Levene's Test for Equality of Variances		t-test for Equality of Means		
	F	Sig.	t	df	Sig. (2-tailed)
23. An interesting subject line makes me open an email attachment.	1.030	0.311	-3.022	311	0.003
26. I will apply security patches to my phone as soon as possible.	0.091	0.763	-1.965	311	0.050
30. My password doesn't follow keyboard pattern.	3.608	0.058	3.515	311	0.001
31. I can share passwords with other people.	3.379	0.067	2.271	311	0.024

34. My passwords are based on my personal information.	0.491	0.484	-4.715	311	0.000
42. I check the authorization or identity of someone before talking on any issues.	0.481	0.488	-2.060	311	0.040

Out of the 27 items the behavior of students showed significant difference in case of 6 questions. Two items came from behavior on malware items, three from password usage and one from social engineering. Regarding the individual online scam issue items students behave similarly in these countries. In each case the variances proved to be equal in the population and in each case the p value for the independent t-test was below 5%, thus the test was significant. Most of the statements were on private and very personal aspect of cyber security like curiosity, personal password practices and trust in unknown individuals, which statements rather belong to cyber safety and there was only one statement specifically belonging to cyber security. The significant difference was confirmed with CHI^2 analysis due to the ordinal scale nature of responses in which process item 23, 30 and 34 also showed significant difference in the behavior.

5 Discussion on Behavior toward Cyber Security on Smartphone

The next step in the comparative analysis was to confirm these significant dimension items and to reveal further ones along which the behavior of the students is different in these two countries. For the specific analysis the CHAID (CHI-squared Automatic Interaction Detector) decision tree method was applied, which is a multivariable recursive classification process that can be used for categorical variable and can also be a segmentation process [30, 31, 32]. The categorical variable in this case is the country while the independent variables are the dimension items. The decision tree is applied because it provides a visual representation of the significant dimension items and represents the relationships between the dependent and the independent variables in a tree structure and makes the interpretation easier. The advantage of the CHAID method is that there are no restrictions on the measuring scale of the variables and their distribution, categorical variables can be used, as well as numerical variables for dependent and independent variables. Splitting is based on CHI^2 tests, and the algorithm first unifies the categories that are the least different concerning the categorical variable then splits according to the strength of the dependent variable. It stops when it finds an optimal tree depth and no relevant changes would happen in the segments. The Exhaustive CHAID method differs from CHAID by not having a stopping criterion. The decision tree method is used in the research to reveal the significant differences between Hungary and Vietnam. The splitting variables will be used to characterize the different behavior of students and identify the areas.

The SPSS program was used for growing the tree. All the statements were used as independent variables and the target variable was set to Hungary (Vietnam was set as target variable for a second running and resulted in the same decision tree), with the following criteria: the splitting node significance level was set to α=0.05, the minimum number of cases in the parent node was set to 30 while that of the child note to 10 due to the fact that the number of students from Vietnam was 124 and the goal was to gain a decision tree with sufficient depth. The maximum tree depth was set to 5 in order to gain as many significant splitting variables as possible. Even though, the decision tree grew 3 levels (Figure 6).

The decision tree levels show the significant items and also gives a priority order of significant items in the cyber security behaviors of students on smart phones. The 0 level presents the percentage and the numeric distribution of the students. The algorithm step by step selects the most significant items and creates segments in which the distribution of students from the two countries can be found. It can be concluded that students are split into three groups by item 34, then 2 items (24 and 30) with the same impact became the splitting items.

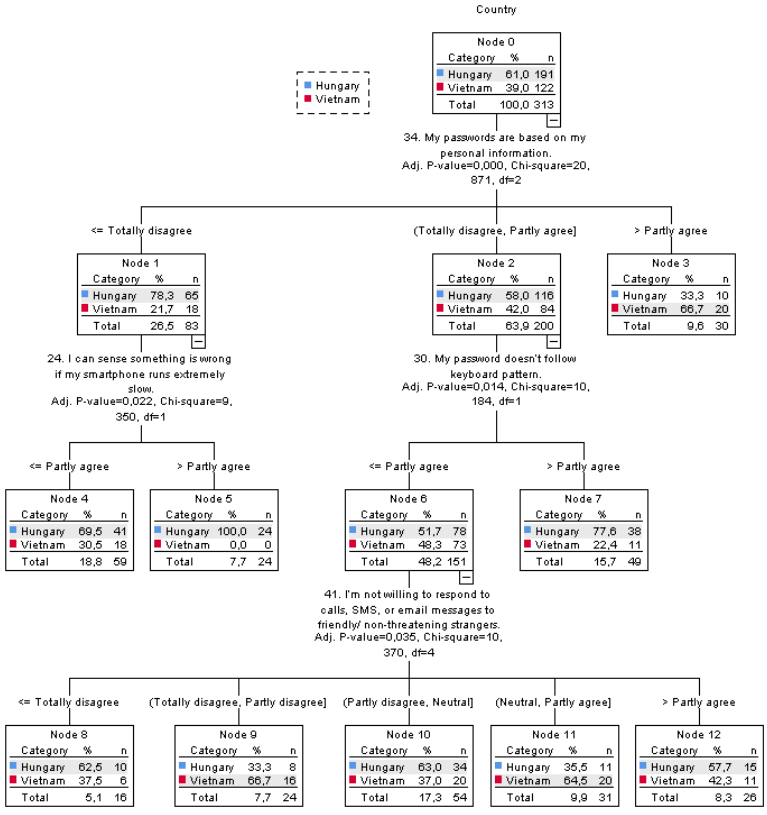

Figure 6
Splitting statements concerning behavior of students in Hungary and Vietnam

The level 1 splitting (34) put only 10 students from Hungary in the group more characteristic to the Vietnamese group. The *leftmost group* at level 1 is dominated by the students in **Hungary** which group is characterized by *high awareness of non-personal data for passwords* and *skeptical behavior with slow running of smart phones.* The *rightmost leaf* is *the least aware of password usage*, which group is assigned to **Vietnamese students**. The *second group*, which *pays attention to password usage on smart phones, avoids using keyboard patterns* (a second splitting item at level 2) but still *uses personal information* is also assigned to students in **Hungary**, in which case the less careful are further split into 5 groups by the item 41 linked to *social engineering*. At level 3 two groups are assigned to students in Vietnam and three groups to students in Hungary, and their behavior does not follow a consistent pattern. The behavior of students in this particular branch calls for the highest degree of education and awareness raising. It has to be noted that with the application of CHAID instead of exhaustive CHAID algorithm, the *rightmost group* at level 1 is further split by item 35 (I never change password) which further confirms *this group's lower level of awareness of password usage.* (The tree is not presented in the paper due to its length). At the same time in case of the most unsure group being either from Hungary or from Vietnam at level 3 (item 30 <= Partly agree) a new variable has become influential (item 31 – I can share passwords with other people.) and segments two groups one assigned to Vietnam (<= Neutral) and one to Hungary (>=Neutral).

Most of the students belong to the uncertain branch. The Exclusive CHAID algorithm reduces the decision uncertainty from 39% to 17.89% by level 4 ([6+8+20+11+11]/313=0.1789) which is a 21% reduction in uncertainty (i.e. error) compared to level 0. Table 7 gives the representation of the decision tree.

Table 7

The representation of the decision tree

Node	Hungary		Vietnam		Predicted Category		
	N	Percent	N	Percent		Sig.[a]	Split Values
0	191	61.0%	122	39.0%	Hungary		
1	65	78.3%	18	21.7%	Hungary	0.000	<= Totally disagree
2	116	58.0%	84	42.0%	Hungary	0.000	(Totally disagree, partly agree]
3	10	33.3%	20	66.7%	**Vietnam**	0.000	> Partly agree
4	41	69.5%	18	30.5%	Hungary	0.022	<= Partly agree
5	24	100.0%	0	0.0%	Hungary	0.022	> Partly agree
6	78	51.7%	73	48.3%	Hungary	0.014	<= Partly agree
7	38	77.6%	11	22.4%	Hungary	0.014	> Partly agree
8	10	62.5%	6	37.5%	Hungary	0.035	<= Totally disagree
9	8	33.3%	16	66.7%	**Vietnam**	0.035	(Totally disagree, partly disagree]

10	34	63.0%	20	37.0%	Hungary	0.035	(Partly disagree, Neutral]
11	11	35.5%	20	64.5%	**Vietnam**	0.035	(Neutral, partly agree]
12	15	57.7%	11	42.3%	Hungary	0.035	> Partly agree
a. Bonferroni adjusted							

Table 8 gives information about the leaves in the decision tree. The "node" information is the number of students in the segmented group and the proportion to the total number of students. The "Gain" shows the number of students segmented to the target group by the algorithm and the proportion to the total number of students in Hungary. The "response" is the proportion of students segmented by the target within the group and the "Index" is the ratio of the response % and the root target %. The higher the index the impact of the rule leading to that group is larger.

The model used to find extra significant variables that cause a different behavior of students in Vietnam and Hungary related to cyber security on smart phone is 69.6% accurate so there is a 30.4% probability of misclassification.

Table 8

Final segmentation by the decision tree

Node	Node		Gain		Response	Index
	N	Percent	N	Percent		
5	24	7.7%	24	12.6%	100.0%	163.9%
7	49	15.7%	38	19.9%	77.6%	127.1%
4	59	18.8%	41	21.5%	69.5%	113.9%
10	54	17.3%	34	17.8%	63.0%	103.2%
8	16	5.1%	10	5.2%	62.5%	102.4%
12	26	8.3%	15	7.9%	57.7%	94.5%
11	31	9.9%	11	5.8%	35.5%	58.1%
3	30	9.6%	10	5.2%	33.3%	54.6%
9	24	7.7%	8	4.2%	33.3%	54.6%

The decision tree method used allowed the researchers to identify two-two (item 24 and 41, and item 31 and 35) extra significant variables by the CHAID and the exhaustive CHAID methods while the significance of three variables that make the behavior of the students different were confirmed. Most of these variables belong to *password usage* while one belongs to *smart phone security* and *protection* and one to *social engineering*.

To answer the hypotheses questions, concerning the comparison of cyber security behavior of students in Hungary and Vietnam on smart phones, three methods were used and certain similarities and differences were found. Student behave *similarly concerning the use of LMS on smartphone* as well as *using mobile*

banking services and *saving credit card information* or *auto saving login information*. Analyzing the four dimensions of cyber security, student behavior proved to be relatively similar in the dimension of online scam, the *differences* cropped up regarding *password usage* – students in Vietnam tend to be less aware of cyber secure password usage than students in Hungary, on *smartphone security* issues and their *knowledge of cyber security and intention to learn more* on it (Figure 7).

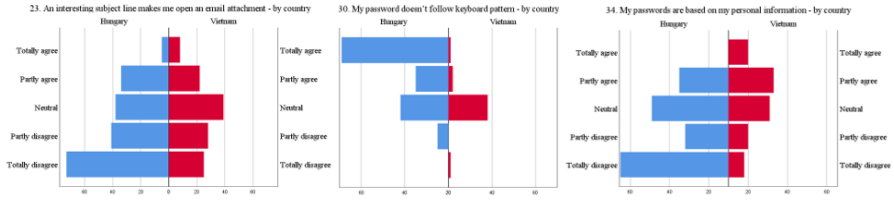

Figure 7

Differences in overall student behavior in three questions (item 23, 30, 34)

At the same time, the more uncertain students, tend to behave similarly both in Hungary and Vietnam and their behavior on certain social engineering issues proved to be significantly different. The exhaustive CHAID decision tree enables student segmentation identifying **highly aware students (Hungary), the least aware students (Vietnam)** and the **uncertain group** (partly Hungary and partly Vietnam) mainly *segmented by password issues and social engineering*.

The results confirm the need of education and training, at an early age, and also confirms that there are cultural differences in cyber security practices, in these two countries.

Conclusions

This study has targeted University Students' self-evaluating issues, in relation to cyber security dimensions, through survey for the purpose to investigate the level of awareness and behavior in cyber security via using smartphone. By choosing Hungary and Vietnam as the two countries for comparative analysis, the similarity and differences in the level of existing knowledge of cyber security, the level of awareness and behavior in cyber security, using smartphones were discovered and discussed. The findings of this study have shown results in all aspects, chosen for evaluating the current level of awareness and behavior in cyber security of respondents in both countries. It should be noted, that without any barriers of the different countries, the majority of all respondents, who are currently University Students, in different fields of study, are lacking not only a fundamental knowledge of cyber security, but also, good practices in their daily experiences while using their smartphones, beyond the differences in respondent's country. Importantly, the respondents have also shown their neglect of self-protection from threats of cyber security, by ignoring minor potential risks, while using their smartphone while connected to the Internet. Based on the research results, as

discussed herein, the study emphasizes the importance of a cyber-security formal education, that could directly support young users with a fundamental knowledge of this global issue, for self-prevention, from cyber threats. Through a comparative analysis between Hungary and Vietnam, it is shown that the findings of this research, contribute to the International Academic scheme, especially in the field of cyber-security for smartphones, using a different lens. Finally, the information in this study, can also provide basic data, for further relevant research, particularly in any comparative research for this emerging global issue.

References

[1] Jalali, M. S., Siegel, M., and Madnick, S.: "Decision-making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment". *Journal of Strategic Information System*, 28(1) 2019, pp. 66-82

[2] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., and Basim, H. N.: "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", *Journal of Computer Information Systems*, 2020, pp. 1-16

[3] World Bank Group.: "Vibrant Vietnam, Forging the Foundation of a High-Income Economy", The World Bank, Washington, 2020, World Bank Document

[4] Pieskä, S., Luimula, M., and Suominen, T.: "Fast Experimentations with Virtual Technologies Pave the Way for Experience Economy". *Acta Polytechnica Hungarica*, 16 (6), 2020, pp. 9-26

[5] Digital in 2020//We are social, 2020 [Online] URL: https://wearesocial.com/digital-2020

[6] Digital 2020: Global Digital Overview // Datareportal, 2020 [Online] URL: https://datareportal.com/reports/digital-2020-global-digital-overview

[7] Digital 2020: Hungary//Datareportal, 2020 [Online] URL: https://datareportal.com/reports/digital-2020-hungary

[8] Digital 2020: Vietnam//Datareportal, 2020 [Online] URL: https://datareportal.com/reports/digital-2020-vietnam

[9] The World Bank Open Data,: 2021 [Online] URL: World Bank Open Data | Data

[10] O'Dea, S.: "Forecast of smartphone user numbers in Hungary from 2015 to 2025", Statista, 2020 [Online] URL: https://www.statista.com/statistics/566122/predicted-number-of-smartphone-users-in-hungary/

[11] Karabasevic, D., Stanujkic, D., Maksimović, M., Popovic, G., and Momcilovic, O.: "An Approach to Evaluating the Quality of Websites Based on the Weighted Sum Preferred Levels of Performances Method". *Acta Polytechnica Hungarica*, 16 (5), 2019, pp. 195-215

[12] Senthilkumar, K., Sathishkumar, E.: "*A Survey on Cyber Security awareness among college students in Tamil Nadu*". IOP Conference Series: Materials Science and Engineering, 2017, 263, pp. 1-10

[13] Khalid, F., Daud, M. Y., Rahman, M. J. A., and Nasir, M. K. M.: "An Investigation of University Students' Awareness on Cyber Security". *International Journal of Engineering & Technology*, 7(4), 2017, pp. 11-14

[14] Reid, R., and Niekerk, J.: "*A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory*". In Proceedings of the nineth International Symposium on Human Aspects of Information Security & Assurance, 2015, pp. 34-44

[15] Allen, I. E., and Seaman, J.: "*Learning on demand: Online education in the United States*". Sloan Consortium, Newburyport, 2010

[16] Luyt, I.: "Bridging spaces: Cross-cultural perspectives on promoting positive online learning experiences". *Journal of Educational Technology Systems*, 42, 2013, pp. 3-20

[17] Ivanova, M.: "ELearning Informatics: From Automation of Educational Activities to Intelligent Solutions Building". *Informatics in Education*, 19(2), 2020, pp. 257-282

[18] Abawajy J.: "User Preference of Cyber Security Awareness Delivery Methods". *Behavior Information Technology*, 33(3), 2014, pp. 237-48

[19] Chin, A. G., Etudo, U., and Harris, M. A.: "On Mobile Device Security Practices and Training Efficacy: An Empirical Study". *Informatics in Education*, 15(2), 2016, pp. 235-25

[20] Lehto, M.: "*Cyber security competencies: cyber security education and research in Finnish universities*". ECCWS2015-Proceedings of the 14th European Conference on CyberWarfare & Security: ECCWS 2015, University of Hertfordshire, Academic Conferences and Publishing International Limited, 2015, pp. 179-88

[21] Shropshire, J., Warkentin, M., Johnston, A., and Schmidt, M.: "*Personality and IT security: an application of the five-factor model*". AMCIS 2006 Proceedings, Acapulco, Mexico, 2006

[22] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., and Jerram, C.: "A study of information security awareness in Australian government organizations". *Information Management & Computer Security*, 22 (4), 2014, pp. 334-345

[23] McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, and M., Lillie, M.: "The effect of resilience and job stress on information security awareness". *Information Computer Security*, 26(3), 2018, pp. 277-289

[24] Hadlington, L.: "Employees Attitudes Towards Cyber Security and Risky Online Behaviours: An Empirical Assessment In The United Kingdom". *International Journal of Cyber Criminology*, 12(1), 2018, pp. 269-81

[25] Pendley, J. A.: "Finance and accounting professionals and cybersecurity awareness". *Journal of Corporate Accounting Finance*, 29(1), 2018, pp. 53-58

[26] Reid, R., and Van Niekerk, J.: "Decoding audience interpretations of awareness campaign messages". *Information Computer Security*, 24(2), 2016, pp. 177-93

[27] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M.: "Individual differences and information security awareness". *Comput Human Behav*, 69, 2017, pp. 151-56

[28] Xu, T. D. T., Polyakova, N., and Shipilova, S. S.: "*Social Internet-networks in the life of Vietnamese students*". HS Web of Conferences, 28 (01101), 2016

[29] Alampay, E. A., and Moshi, G. C.: "Impact of mobile financial services in low-and lower-middle-income countries: A systematic review". *Information Technologies & International Development*, 14, 2018, pp. 164-181

[30] Dudás, P.: "Segmentation using a decision tree", *Economica New* 9(2), 2018, pp. 49-54

[31] Kass, G.: "An exploratory technique for investigating large quantities of categorical data", *Applied Statistics*, 29(2), 1980, pp. 119-127

[32] Hámori, G.: "Characteristics of CHAID-based decision trees (A CHAID alapú döntési fák jellemzői)", *Hungarian Statistical Review* (*Statisztikai Szemle)* 79(8), 2001, pp. 703-710