Cyber Security Awareness and the Behaviors of Higher Education Students, using Smartphones in Vietnam

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

[1]Keleti Károly Faculty of Business and Management, Óbuda University, Tavaszmező u. 17, 1084 Budapest, Hungary, Tick.Andrea@kgk.uni-obuda.hu

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

Abstract: This study investigates the level of cyber security awareness and behaviors of university students in Vietnam, through their experience of using smartphones. It is expected to determine the importance of cyber security awareness and the formal education to young generation in developing countries in the booming of information technology. Research data was collected using a set of questionnaires to 114 university students in different school years and fields of study, in Danang city, Vietnam. Descriptive data analysis was done by using the SPSS software. The research results showed that the majority of respondents are lacking fundamental knowledge of cyber security and good practices, for daily experiences, in using their smartphones. It was also noticed that the respondents presented their neglect of self-protection, from threats of cyber security, due to ignoring minor risks, while using smartphones connected to the internet.

Keywords: Cyber education; internet security; online threats; student awareness; student behavior; Vietnam

1 Introduction

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, digital media has facilitated the way people communicate and socialize. However, along with the development of the internet, there is also existence of cyber risks like cybersex, pornography, personal information exposure, cyber addiction, online fraud, addiction towards gaming and gambling, which have negative effects on adults and children [1]. According to Fischer [2], cyber security is sometimes publicly discussed under other common concepts such as information privacy, information sharing, intelligence gathering, and surveillance. Yet, the concept of cyber security refers to three main areas: activities or means to protect computers or smartphones from attack and threats from computer's, internet's networks relating to all hardware, devices software, data and also other elements of cyberspace; the quality of preventing or being protected from cyber threats; and the attempts of the broad field in order to implement or improve those activities or means. One of the most serious impacts of a successful cyber-attack is the exfiltration of the internet users' financial, proprietary or personal information, by attackers who can benefit, often without the knowledge of the victims. Furthermore, system access by legitimate users could be slowed or prevented by denial-of-service attacks which result in the destruction or disruption of their equipment [3].

Regarding digital media, the idea of transforming the smartphone to a pocket desktop has increased the number of users accessing the internet via their phone. Thus, it cannot be deniable that this essential portable technology device plays vital role in people’s lives. According to İnce and Kilic [4]**,** given an unprecedented increasing rate of smartphone users, it is necessary to research about an impact of these devices on human life. In the same spirit, Reid and Niekerk emphasized the huge impact of the internet on 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’ [5, p. 34]. The global spread of novel coronavirus COVID–19 since early 2020 has resulted in critical impacts on not only the global economy society, but also many other aspects of human society [6]. Social interaction has become more challenging ever when people have to implement social distancing in all activities including working, studying and doing services. Because of this, using computer or smartphone has become more priority when the lockdown is taken place due to COVID–19 pandemic. Instead of face-to-face forms of work or education, working from home via internet has been applied as of the most urgent responses to the pandemic. Therefore, not only getting used with the new form of working/study, increasing cyber security awareness is critical to internet users [7, 8]. According to research on cyber security behavior of smartphone users in India, it is claimed that for a variety of Indian, smartphone is their first digital device with the internet connection. Hence, they are less experienced in dealing with the Internet-enabled devices, as well as handling cyber threats which has led to a fact that inexperienced Indian smartphone users confront more risks of internet-related security breaches together with uncontrolled consequences relating to security issues [9]. Understanding the nature of such cyber-attacks on smartphone as well as the importance of young generation's awareness of cyber security is critical to not only individuals, but also to society, this paper aims to investigate the level of cyber security awareness and behavior of university students in Vietnam in using smartphone through their habit of phone using and the knowledge of information security. With a case study of students at the university level in Vietnam, it is expected to determine the importance of cybersecurity awareness and training, to younger generations, in developing countries, in the current booming of information technology. This study is conducted to answer the research questions in this statement:

What is the current state of cyber security behavior in the aspects of malware, password usage, social engineering, and online scam among higher education students in Vietnam?

The next section presents the literature review and followed by the sections of research aims and research method. The section after that provides the expecting research results and recommendation based on the results. Then, to bring the research to a close, the final section provides conclusions and directions for further research.

2 Literature Review

In recent years, the constant increase of internet usage in any parts of the world unavoidably lead to the exponential rise of cybercrime which could generate uncontrolled criminal threats to individuals as well as to organizations [10]. In a study by Yadav et al. [11], it was emphasized that there has been increasing apprehensions about the internet users' awareness, especially regarding the cyber culture and cybercrime while it has received very little research attention. The research has contributed to claim the important role of the internet users' habits and cyber awareness. According to Cranfield et al. [12], smartphones are mostly privately owned, and obviously higher education institutions allow their student to use them within the university. Simultaneously, another study conducted by McGill and Thompson [13] has proven that people have higher level of awareness of protecting their personal computer or laptop than their smartphone or tablet. This led to a fact that the lack of security awareness of smartphone users has become a critical factor influencing the mobile security behaviors of the users [12].

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 [14, 15]. This means that accessing to the internet for studying would be an important purpose for students at higher education level and prolong their daily internet usage. 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 also argued that even the basic level cyber security awareness is not sufficient enough for mitigating cyber risks and threats [16, 17]. As such, further studies about this concern for more insights and practices would be critical to not only individuals, but also educational sector and other relating organizations.

In Vietnam, smartphones have become an indispensable item in life, for not only communication purposes, but also for expressing one’s image and status in society. According to Viet Nam News, in 2017, up to 84% of the people use smartphones, compared to 78% a year ago, and has been experiencing an upward trend. In addition, at the same time, the article mentioned that 95% of Key Cities’ citizens use mobile phones, among which 84% are smartphone users, up six percentage points from 2016. More remarkably, there are more than 88% of people aged 18 to 36 years old own a smartphone while only 38% of the 37 and older age groups are smartphone users [18]. These numbers illustrate that smartphone plays an important role in lives of young generation who have expansive network and are hungry of expressing their personal values through the objects they are using, especially university students. This influence has been documented in some cyber security related work, including demand for cyber security solutions, e-government systems, national information systems and technical standards for locally made security products in Vietnam. Nevertheless, there is little attention in the degree of cybersecurity awareness, among youngsters and young adults on the trend of Internet sources, security risks of online working and self-protection mechanism toward being a cyber victim.

The Fletcher School has classified Vietnam as a breakout economy as defined according to the Digital Intelligence Index, signifying a low current level of digitalization (46.79) but rapid progress (62.37) [19]. Despite significant advancements in the development of information and communication technology (ICT) infrastructure, as highlighted by the Network Readiness Index [20], challenges remain to be addressed in Vietnam. While Vietnam has experienced substantial growth in information technology and prioritized digitalizing the administrative system for public service innovation (51.01), the average IT skills development among its population remains low (41.63), together with concerns over cybersecurity, data privacy, pose more potential and higher risks of IT hazards in this country [21].

As for internet and social media usage, 70.3% and 73.7% of the population are internet and social media users [22], respectively, while the penetration of mobile connections stands at 157.9%. The number of mobile connections and active social media users grew by 0.9% and 10.8% in 2021 compared to 2020, respectively. 96.9% of the population owned smart phone in 2020 and the daily time spent on social media equaled 2 hours and 21 minutes, twice as much as listening to music streaming services (1 hour 9 Minutes). Around one third of the population (31.8%) expressed concern about how companies use personal data and 34.7% of the population used some form of ad-blocking tool in the month preceding the survey time [22].

As young adults are those university students classified who are within the age range from 18 to 29 years old. They are known as the most active internet users in terms of information seeking and social network. It is generally known that spending long time online would put these young adults in high-risk state in which they can be exposed to such cyber risks mentioned earlier. Several studies have shown the young adults' high dependence on smartphone useage for seeking information via the internet, using social media as well as gaming [23]. A long duration of time online, via smartphone, could put this range of citizens in a vulnerable position, that can attack them with unanticipated consequences.

3 Research Methodology

In order to obtain the research aim, quantitative method was chosen for this study to collect primary data through questionnaire surveys. Data analysis was done by using the SPSS software. The research population comprised of university students staying in Danang city, Vietnam. Currently, Danang has more than 15 universities with over 80,000 students, 8 universities are currently running under the scope of the University of Danang. Because of the large population sizes, researcher was unable to test every person in the population due to some contrasts in time and budget, especially under the current circumstances of Covid–19. Therefore, this research relied on non-probability convenience sampling.

Accordingly, the research data was collected from 114 university students in different school years and different field of study in Danang city, Vietnam. The respondents received the survey via E-mail or Facebook Messenger and were asked to spend from 3 to 5 minutes on this survey. Survey responses were voluntary, no credit was given to complete the questions, students were assured of anonymity, and that their responses would only be used to analyze data for this research. The survey questionnaire utilized in the research was self-developed by the authors, drawing upon references from previous studies conducted by Muniandy et al. [24] and Bain et al. [25].The questionnaire included 3 sections: demography, a set of 15 questions on the awareness of cyber security on smartphone, and a section on behavior toward cyber security on smartphone consisting of four issues for giving personal evaluation which are *malware items*, *password usage*, *social engineering* and *online scam*. Sections 1 and 2 comprise both type of Yes/No and multiple choices questions, attempted to examine the current practice of using smartphone and their general knowledge of cyber security. In section 3, the instrument is structured in the Likert fashion, on a 5–point scale, ranging from 'Totally disagree' (1), through 'partly disagree' (2), 'neutral' (3), 'partly agree' (4) to 'strongly agree' (5), respondents were requested to indicate their agreement or disagreement with the statements based on this scale.

In order to confirm the validation of the questionnaire, a pilot testing was carried out to confirm whether the questionnaire was clear enough to understand, to see how participants will react to the questionnaire, or if there is the need to modify or include more items in certain areas. Mostly Vietnamese students from different institutes in different countries such as Australia, the USA, United Kingdom and Vietnam formed the pilot group. This research has applied the Cronbach's alpha to assess the reliability of the instrument, which values were in the range from 0.645–0.820. According to Cohen [26], these values surpassed the minimal consistency guidelines for an instrument to be judged acceptable.

The research used descriptive statistics for demographic profile and the analysis of the dimensions separately, while contingency analysis, namely CHI^2 test, Analysis of Variance (ANOVA) for the analysis of the related question items and comparison of student behavior was used. Furthermore, Cluster analysis based on preliminary factor analysis using Principal Component Analysis (PCA) for student segmentation and identifying groups based on cyber security awareness was applied. The classification of students based on the dimensions applied reliability and validity analysis, using Cronbach's alpha. Ward and K-Means classification processes were conducted and finally a confirmatory discriminant analysis was run to visually present the clusters found.

The following sections deal with the findings and results and analyses the cyber security awareness behavior of students in the survey.

4 Findings and Discussion

4.1 Demographic Profile

The sample compiled of university students in Vietnam, up to 99.1 per cent of whom use smartphone frequently. The total of 114 respondents are divided as 62.3% of them are female while 37.7% of them are male. The majority of respondents are between 19-22 years old (64%), 24.6% of them are between 23 and 25. This has shown that respondents' age range is positive with the group of students that this research has targeted to. In addition, the highest number of participants are studying Economics or Business Management (52.6%), followed by other fields (20.2%), Engineering, Mathematics or Natural Sciences (29.3%), Medicine (7%) and Laws field (0.9%). Considering the experience in smartphone usage, up to 38.6% of the respondents have been using smartphone for 3–6 years, 35.1% have experience between 7 and 10 years. Surprisingly, 20.2% of the respondents – young adults – have experience in smartphone usage for over 10 years (some starting at the age of 9 or earlier!).

Regarding online activities pursued via smartphone, all the respondents use smartphone to access social networking sites such as Facebook, Instagram, etc., which mean they are heavy social networking users (Figure 1). A previous relevant study on Vietnamese students using social-internet-network also ascertained that 100% of the research's respondents got more than one social network accounts and the majority of students spend time on social networking from 1 to 3 hours per day [27]. Figure 1 depicts, that students at higher levels, use their smartphone for most of essential activities such as entertainment (listening to music, watching videos), communication (texting, chatting, video calling) and even study purposes (emailing, reading book, online study, accessing websites).

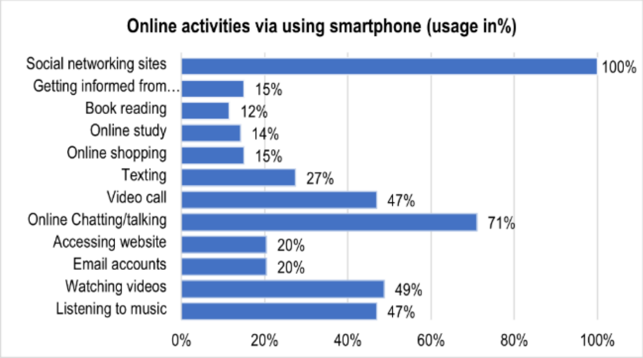

Figure 1
Online activities participated by the respondents (developed by authors)

However, using smartphone for entertainment and communication has presented as the main using purposes admitted by university students in Vietnam. This figure is relevant to a study about mobile learning trend among higher education students in Vietnam which claimed that up to 83% of the student's using smartphone for communicating and social networking purposes [28]. Familiarly, it is statistically reported by the University World News that an average Vietnamese person has spent up to 11 hours per day on the Internet and social media [29].

4.2 Awareness of Cyber Security on Smartphone Findings

The term of 'Cyber security' has not been new to young people around the world. However, to the surveyed young adults in Vietnam, there are up to 28% who have not heard or known about this term. This could be a concerning issue while 100% of them use smartphone and internet daily. Furthermore, when asked about their willingness to learn more about cyber security, 89.5% of them agreed, even so, no relationships were found between the two questions ($CHI^2=0.864$, $p=0.353$). Although, 63.2% of the surveyed have heard about the term cyber security and would desire to learn more on the issue, only 1.8% of the questioned have not heard about the term cyber security and would not like to learn more about it.

Regarding the responsibility for information security in university environment, Vietnamese students were asked about who should take this responsibility. The responses of this question resulted in over 90% of total respondents think that ensuring information security in university environment should be responsible by all students (92%), academic staff (93%) and the university board (94%) (the higher management level at the university).

As Figure 2 shows, although respondents use their smartphone most of the time in a day for a diverse range of purposes (Figure 1), over 50% of them are not sure if their smartphone is virus infected when not responding well, and about 20% of them have no idea about this problem. The majority of Vietnamese students using a smartphone believe that it needs to be security protected by antivirus application (78.1%) while 14% of them have the opposite point of view. In the meanwhile, 47.4% of these students disagree with saving auto-login information in the smartphone as a good perspective from cyber security. For the remaining half of the total respondents, up to nearly 29% represent the "not sure" response.

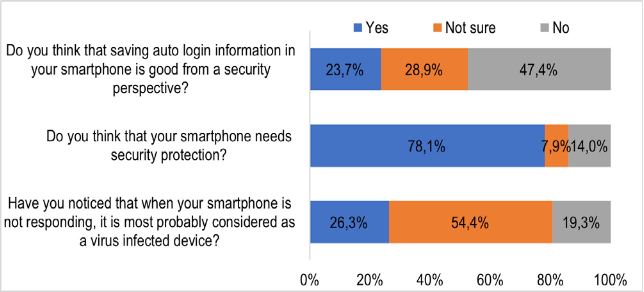

Figure 2
Participants' response to cyber security (developed by authors)

Mobile banking is known as an innovative service, which has been developed by the diffusion of mobile communication technology. According to Alampay and Moshi [30, p. 165, 31, p. 14], 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. With all the significant benefits of mobile banking, it is yet to gain larger-scale adoption, especially in developing countries. Nevertheless, in recent years, a number of commercial banks in Vietnam have introduced and diffused some mobile banking systems, which has received positive support from banking customers, especially the younger generation [32].

The distribution of this study associated with the online banking aspects, have shared the same expecting result with 84% of total respondents currently using mobile banking services as shown in Figure 3. In addition, more than half of all participants trust submitting their bank card's information, for online services, such as online shopping, online service payments through their smartphone (62%). Student behavior considering submitting credit card information and mobile banking services shows a significant relationship i.e., the more students use mobile banking the more they trust submitting their credit card information for online services and shopping (CHI^2=7.106, p=0.008) and vice versa. Based on the distribution of the answers more students trust the security level of mobile banking, online service and shopping while (56.14%) there are some who do not trust the systems and do not use online banking services (10.53%).

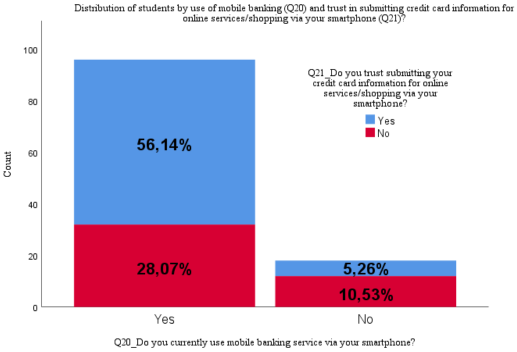

Figure 3

Respondents' trust in providing credit card information through mobile banking (developed by authors)

4.3 Behavior toward Cyber Security on Smartphone

Table 1 presents the descriptive measures of the variables in the four dimensions applied concerning cyber security. The dimension on password issues were the most relevant while in the other three dimensions some items were quite constant. In the case of the dimension on online scam the negative sentiment resulted in a reverse order of Mean and IQR. In case of the malware issue dimension, the perception of security issues, the belief in university responsibility and the awareness of security installation were the most constant items, while in the case of the password issue dimension students showed the highest awareness in the case of password sharing. Based on the constant reply to social engineering concerns students and finally, students showed the least aware behavior for the case of social scam issues.

Table 1

Descriptive analytics of Cyber security dimension items (developed by authors)

Dimension	Item	Mean	Me	Mo	IQR
Cyber security behavior on malware items	I prefer to update information on my study via computer	3.68	4	5	2
	I trust any information sent from my university online learning management system	3.59	4	4	1
	I can sense something is wrong if my smartphone runs extremely slow.	3.58	4	3	1
	I will apply security patches to my phone as soon as possible.	3.56	4	3	1
	I prefer to update information on my study via my smartphone	3.17	3	3	1
	An interesting subject line makes me open an email attachment.	2.69	3	3	2
	I'm willing to download materials from unsecure sites.	2.28	2	1[a]	2
	I'm willing to open email or message attachments from strangers.	2.21	2	1	2
Cyber Security behavior on password	My password consists of lowercase, uppercase, numbers, special characters.	3.83	4	5	2
	I do use the "Remember my password" option in my phone.	3.14	3	4	2
	I use a similar password for different applications.	3.13	3	4	2
	My passwords are based on my personal information.	3.05	3	3	2
	My password doesn't follow keyboard pattern.	3.01	3	3	2

usage issues	I keep my password somewhere in my phone.	2.42	2	1	2
	I never change passwords.	2.39	2	3	2
	I can share passwords with other people.	1.65	1	1	1
Cyber security behavior on social engineering issues	I check the authorization or identity of someone before talking on any issues.	3.68	4	3	2
	I wouldn't reveal any confidential information under any circumstances.	3.68	4	5	2
	I wouldn't communicate with a stranger although his/her looks warrant sympathy.	3.42	3	3	1
	I'm not willing to respond to calls, SMS, or email messages to friendly/ non-threatening strangers.	3.33	3	3	2
	I'm not interested in reading social engineering issues.	2.77	3	3	1
	I think I'm not a target of social engineering attacks due to student status.	2.70	3	3	1
Cyber security behavior on online scam issues	I'm aware of and able to identify the latest online scams.	3.44	3	3	1
	I never trust strangers' identity information given on the Internet.	3.43	3	3	1.25
	I never consider any amount of money for services offered by an online site.	3.04	3	3	2
	I wouldn't hesitate to meet internet friends in person.	2.79	3	3	1.25
	I established trusted online relationship with strangers.	2.30	2	3	2
	I respond to SMS announcing contests involving huge sums of money.	2.00	2	1	2

The relatively high number of constant replies support the reduction of the number of items in the dimensions to find typical cyber security behavior patterns in case of Vietnamese students. The following subchapters describe students' cyber security behaviors in the four dimensions separately, then classification is done based on the revealed hidden factors.

4.4 Cyber Security Behavior Dimensions

Figure 4 shows the findings for respondents' cyber security behavior in relation to malware items. Amongst the six malware-related statements, the statements number 2, 3, 5 and 6 indicate the potential weak or harmful cyber security practices to the respondents.

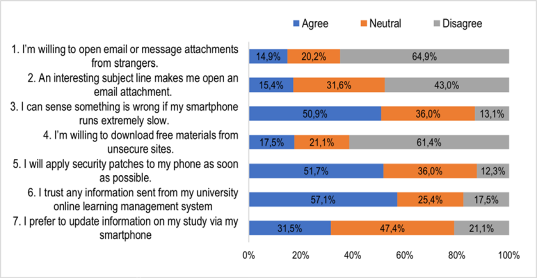

Figure 4
Respondents' Cyber security behavior on malware items (developed by authors)

Figure 5 presents the study findings for Vietnamese students' behavior toward dealing with using password issues. Beginning with the positive results, nearly 80% of smartphone users do not share passwords with others and approximately 70% of them set complicated passwords for their information security. Nevertheless, statement numbers 2, 4, 5, 6 and 7, do not result in satisfactory responses. Accordingly, up to 43% of the survey participants use a same password for different application and 27.2% of them give the neutral point of view on this issue. Furthermore, nearly 40% of the total respondents claim that their passwords are based on their personal information while more than a quarter of the total percentage are unsure about their password details. Although over 50% of the participants claim that they change their password frequently, up to 31.6% of them are not aware of the importance of changing passwords. Probably for the convenience, 43% of the students admits that they do use the 'Remember my password' option in using smartphone and over a quarter of them do not have the certain answer for this issue. Last but not least, a half of the total number of respondents agree that keeping passwords in smartphone is not a good way for ensuring their information security. It could be seen that even though survey participants provide some good practices in protecting passwords when using their smartphone, their low level of awareness and behavior at some points proves the high risk of threats to their information security.

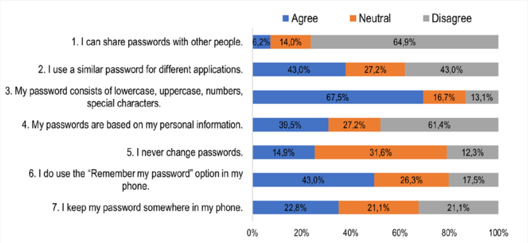

Figure 5

Respondents' Cyber security behavior on password usage issues (developed by authors)

Regarding respondents' cyber security behavior on social engineering issues, Figure 6 probably illustrates the ambiguous evaluation, by survey participants among six statements. Specifically, approximately one third of the total number of respondents give neutral point of view in all the statements while each of them is clear and in detailed enough for understanding.

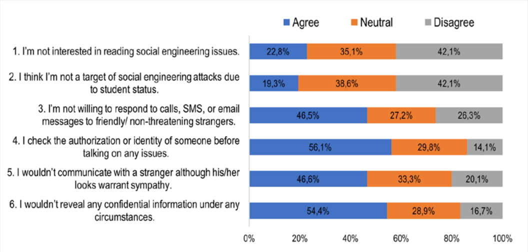

Figure 6

Respondents' Cyber security behavior on social engineering issues (developed by authors)

This results in obstacles for analyzing their awareness level of social engineering problems. In addition, the responses of participants in this section do not show their best practices on cyber security issues related to social engineering aspect. Evidently, more than a quarter of total respondents claim their willingness to respond to calls, SMS or email to strangers (26.3%). Simultaneously, almost a quarter of survey participants are not interested in reading social engineering while 35.1% of them cannot decide their interest, which mean that the low awareness level in this aspect could expose them to the unpredictable social engineering threats.

The last aspect of cyber security to consider respondents' behavior is online scam. All of six statements do not produce satisfactory results, particularly the statement numbers 3, 4, 5 and 6 (Figure 7).

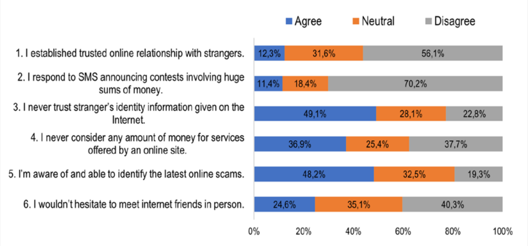

Figure 7

Respondents' Cyber security behavior on online scam issues (developed by authors)

Accordingly, 49% of respondents agree to not trust stranger's identity information given on the Internet while 22.8% of them have the opposite opinion and up to a quarter shows the neutral point of view. In the meanwhile, 56% of disagreement on establishing trusted online relationship with strangers is not the expecting number to this target survey respondent and up to 31.6% do not know to deal with the situation. Furthermore, 24.6% of the respondents admit their willingness to meet internet friends in person while up to 35.1% express the "neutral/ unsure" to the statement (Figure 7).

Difference in the behavior of respondents in cyber security based on the different experience of the duration using smartphone (four different groups of time) was also tested. In this line, all the statements that belong to the four dimensions of cyber security behavior on smartphone using were tested and two statements (Q44: 'I would not reveal any confidential information under any circumstances' and Q45: 'I established trust online relationship with strangers') were found significant for the analysis (F=3.669, p=0.045 and F=3.457, p=0.032, respectively).

It can be seen in Figure 8a, regarding the level of agreement to the statement in Q44, respondents having under 3 years of smartphone usage have strongly agreed with the highest rate (4.7/ 5.0) while the level of agreement of the groups of 3-6 years and over 10 years are nearly the same with about 3.7/5.0. The group of 7-10 years of using smartphone mostly provided neutral point of view (approximately 3.0/5.0).

This unexpected illustration could be explained by that the group of users with the shortest period of using smartphone probably have not had enough experience with smartphone; hence they might be more aware of any potential risks of online threats for their security. Additionally, being accessed to the knowledge of cyber security at the earlier ages than other groups of respondents could be the main factor contributing to their higher awareness and behavior in cyber security issues in this statement.

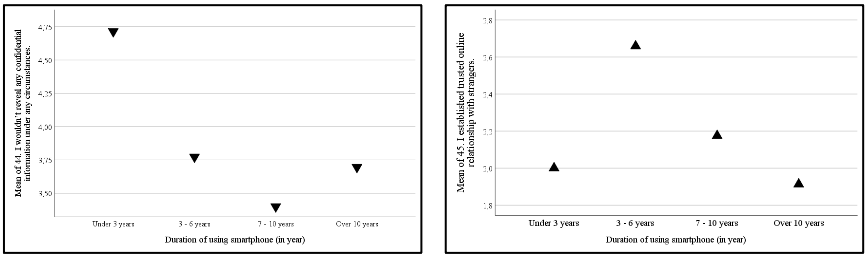

Figure 8a

Figure 8b

Figure 8

The average values of not revealing confidential information and establishing trusted online relationship by strangers grouped by years of experience (developed by authors)

According to Figure 8b, the two groups that having the shortest and longest experience with using smartphone showed stronger disagreement with this statement 'I established trust online relationship with strangers'; whilst the other two groups provided that to some extent, they trusted to establish online relationships. Combined with Figure 8a, it could recognize the importance of education on cyber security to the group of users who are in the ages between 19 to 25 years old. This is because their current level of behavior certainly shows that they could be the most vulnerable groups of smartphone users while they are heavy smartphone users.

4.5 Classification of Vietnamese Students by Cyber Security Dimensions

The four dimensions of cybersecurity behavior (on malware items, on password usages, on social engineering and on online scam issues) of Vietnamese students supported the classification of these students. The overall reliability of the items equaled 0.809 using Cronbach's alpha, which means a rate of good reliability [33]. Each item had a Cronbach's alpha coefficient over 0.79, ranging from 0.795 to 0.811, which enabled the consideration of each item in the classification procedure.

Each dimension of cyber security behavior consisted of about 7-8 questions out of which the questions related to desktops and single sign on were excluded since these questions were not directly related to smartphone usage. The strength of correlations of items within a dimension showed a two-pole variation that demanded the disclosure of hidden factors within the dimension. The factors were revealed using the Principal Component Analysis (CPA) with Equamax rotation for each dimension. Two important factors have been identified in case of Dimension 1, 3 and 4 while three have been revealed for Dimension 2. In this case the password following keyboard pattern proved to be such a strong factor that it stood by itself. For each dimension more than 50% of the information was kept (52.527%, 59.773%, 67.837% and 60.714%, respectively). Concerning cybersecurity threats, one of the most vulnerable points of keyboard patterns is a keylogger malware so the item was left for inclusion in classification. The dimension reduction has proved to be adequate and mediocre in the cybersecurity dimensions, resulting in a KMO test value of over 0.56 in each case ($KMO_{malware}$=0.568, $KMO_{password}$=0.626, KMO_{social}=0.670, KMO_{scam}=0.580 respectively) [34]. On the other hand, the Bartlett's test of sphericity is significant (p=0.000), which implies that the variables are related and therefore suitable for structure detection. Factor score were calculated using Bartlett factor score method [35]. The factors in Table 2 were revealed and used for classifying Vietnamese students on cyber security behavior in smartphone usage. The variables dominating the factor served for naming the factor. The weights of the variables i.e., the correlation value of the variables in the factor were over 0.566 and the highest being 0.904.

Table 2

Dimension reduction using PCA and Structure Matrix in Discriminant analysis (developed by authors)

Cyber security Dimensions	**Factors in Cyber Security Dimensions**	**Structure Matrix Function (Discriminant analysis)**	
		1	**2**
Malware	IT security trust		0.307
	Unknown message download		0.543
Password issues	Password changing habits	0.268	
	Password pattern		0.465
	Password negligence		0.272
Social engineering	Authorization and identity precautions		0.280
	Beliefs in social engineering		0.366
Online scam issues	Light-mindedness	0.313	
	Online scam awareness		0.405

Pooled within-groups correlations between discriminating variables and standardized canonical discriminant functions.

The factors in all four dimensions were used as input items to cluster the Vietnamese respondents. Ward and K-Means clustering methods have been applied, both of which were confirmed with discriminant analysis. No serious normality and no heteroscedasticity problems were detected. The linear relationship among the factors proved to be significant (F-test, p=0.000). Three clusters were formed running along two functions (Figure 9).

'*Light-mindedness*' (horizontal dimension) and '*Security concerns'* (vertical dimension) were assigned to the two functions. The clusters show that Vietnamese students in the survey have different awareness of and attitude to cyber security aspects. Group 1 and 2 are more careless regarding online scam issues and password changing habits when using smartphones (the statement had negative sentiment and the group centroid coordinates are 0.958 and 0.549 along function 1, respectively) while group 3 does not show such strong trust in these issues (group centroid coordinate is −2.424 along function 1). On the other hand, groups 1 and 3 are more conscious about security issues like malware, password patterns or authorization and identification precautions when using smartphones (group centroid coordinates are 0.604 and 0.18 along function 2 respectively, while group 2 performed worse at this dimension (group centroid coordinate is −2.351 along function 1). Group 1 proved to show a more conscious behavior along both dimensions while students belonging to the other two groups lack training in one of the aspects, which justifies the students need of more education on cyber security in higher education.

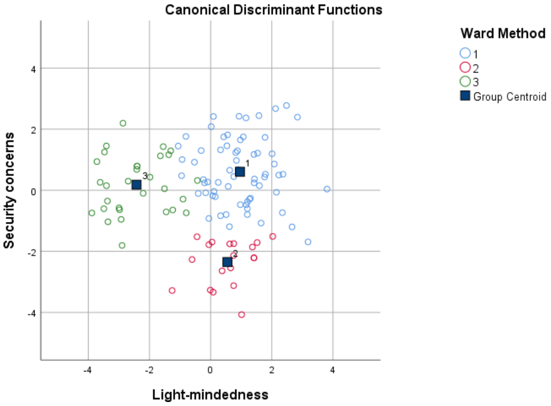

Figure 9

Clusters determined by “light-mindedness” and “security concerns” (developed by authors)

The discriminant functions well separate the three groups. Table 3 presents the eigenvalues and the importance of the functions, while Table 2 includes the structure matrix. The eigenvalues larger than 1 represent that they bear more information content than the original dimensions and the Wilks’ Lambda being small for function 1 (Wilks’ Lambda=0.145) and relatively small for function 2 (Wilks’ Lambda=0.465) depict that the differences between the groups are significant (Chi^2 tests are significant at p=0.000).

Table 3

The separating dimensions’ eigenvalues (developed by authors)

Function	Eigenvalue	% of Variance	Cumulative %	Canonical Corr.
1	2.178^a	65.1	65.1	0.828
2	1.169^a	34.9	100.0	0.734

a. First 2 canonical discriminant functions were used in the analysis.

The structure matrix enabled the naming of the horizontal and the vertical functions and shows which factor belongs to which function. The difference in the behavior of Vietnamese students regarding cyber security awareness and behavior can be determined on the one hand by their personal attitude to password patterns and online relationships and by their attitude to security issues on malware.

5 Discussion

Due to the COVID situation in 2020, the study was constrained to an online format, resulting in limited access and direct contact with respondents. As a result, the research sample size and diversity were both restricted. Regarding the students' awareness of cyber security at the higher education level, the study has examined their general knowledge of this term and provided simple questions involving to their daily activities via using smartphone. It could be realized that among the participating university students a large number of them have not known about the term of 'Cyber security' which means that knowing about protecting themselves from online threats/attacks is still new to them. This should be an important issue that must be given due consideration as they are the heavy smartphone users who have been always with smartphone every time of the day and use smartphone as the must-have item for all essential online activities.

This study has applied four types of cyber security threats including malware, password, social engineering and online scam in order to evaluate respondents' cyber security behavior. As evidently shown in the findings, it could be claimed that the participants' behavior toward all four aspects is considered as vulnerable since the findings are more unsatisfactory and these weakness in behavior would expose them to potential cyber security threats. It was also noticed that research findings conform with related previous studies, which were led in other Asian countries.

A comparative study on cyber security awareness and behavior via using smartphone conducted by Mai and Tick [7] has shared the homologous findings. It is emphasized that the majority of respondents — students at university level in different fields of study — are lacking essential knowledge of cyber security as well as good practices in their daily phone usage regardless the difference in nationalities. Similarly, a research study on cyber security behavior of smartphone users in India in 2020 has claimed that the study respondents did not well perform their cybersecurity behavior through not adopting basic security features or using smartphone without knowledge of technical security controls when using smartphone. There is also significant difference between independent variables such as gender, age indicated in the study [9]. Compared to other relevant studies, the research by Breitinger et al. [36] show interesting findings, claiming that despite of respondents with advanced knowledge of cyber security, they still follow weak practices. Hence, it is concluded that simplifying approaches for phone security setting, ruling secure default setting and changing public mindset of the importance of cyber security would greatly contribute to enhance the awareness and behavior of users toward cyber security.

A study by Muniandy et al. [24] on cyber security behavior among higher education students in Malaysia showed that their respondents generally lack the best practices which could protect them from cyber security threats. They assessed five aspects of cyber security threats (malware, password, phishing, social engineering and online scam) to prove the awareness level of their respondents and concluded that students' behavior is unsatisfactory concerning all these five types of threats. The study highly recommended that all education about cyber security must be seriously considered as the importance of the best practices on the Internet. Another recent study by Khalid et al. [1] on university students' awareness of cyber security in Malaysia demonstrated that although their respondents showed a high awareness level in chosen aspects of cyber security such as cyber bully, personal information, and internet banking, there were still limited knowledge of cyber-sex and self-protection regarding cyber security.

There have been also many other relevant studies on students' awareness and behavior in computer security in the last decades that showed interesting research results. As reported by Bain et al. [25], their respondents were focused on college students who showed the lacking awareness of protecting their personal information when using computer, especially passwords. For example, using the same password for different applications, not keeping password secret and not changing it frequently which share the same findings with this study resulted by a large number of total respondents. The similar study findings are claimed by Jones and Heinrichs [37] that research findings in students' security behaviors in using smartphones at undergraduate level did not show satisfactory outcomes. Hence, it could be concluded that the findings of this research do not notice any surprising results and certainly conform to previous studies' conclusions. Furthermore, this research is therefore significant in determining the popular similarity in cyber security issues that lead to the high risk of cyber threats to young generation in developing countries, particularly higher education students. As such, the study also claims that the increasing emergence of cyber security incidents could certainly drive from user's awareness and behavior.

Conclusions

This study has focused on Vietnamese university students' awareness and behavior, in cyber security, via using a smartphone. The findings of this study have shown unsatisfactory results in all aspects examined, for evaluating the current level of awareness and behavior for cyber security of respondents. Repeatedly, the majority of respondents are lacking not only fundamental knowledge of cyber security, but also good practices in their daily experiences with using their smartphone. It has been noticed that the respondents also present their neglect of self-protection from threats of cyber security due to ignoring minor risk while using smartphone connected to the internet. The research results to some extent, showed compatible results to relevant previous and recent studies, especially studies in developing countries.

Based on the clarified research results, the study emphasizes the importance of cyber security education that could directly support smartphone users to protect themselves with fundamental knowledge and good practices on this global issue. This would be very important to educate young generation about cyber security, particularly students at higher education levels as they account for the largest of population using smartphone and internet, simultaneously, they would become the main forming of the future workforce. Therefore, this study highly emphasizes the vital role of formal education concerning cyber security, that has not been common in Vietnam for students. It is also expected that the findings of this research would contribute to the International Academic Scheme, especially in the field of cyber security by providing useful information on smartphone users' awareness and behavior in cyber security. In addition, it is expected that the results of this study will provide basic data for further relevant research in the future, particularly in comparative research in developing countries, on this emerging global issue.

References

[1] F. Khalid, M. Y. Daud, M. J. A. R. Rahman and M. K. M. Nasir, “An Investigation of University Students’ Awareness on Cyber Security,” *International Journal of Engineering & Technology,* vol. 7, no. 4.21, p. 11–14, 2018

[2] E. A. Fischer, “Cybersecurity Issues and Challenges: In Brief,” 2016

[3] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese and D. Upton, “A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate,” *Journal of Cybersecurity,* vol. 4, no. 1, 2018. DOI: 10.1093/cybsec/tyy006

[4] Z. Ince and V. A. Kilic, “The smartphone usage habits of high school students and their addiction to smart phones,” *The Journal of International Education Science,* vol. 3, no. 6, pp. 104-123, 2016

[5] R. Reid and J. van Niekerk, "A Cyber Security Culture Fostering Campaign through the Lens of Active Audience Theory," in *In Proceedings of the ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).*, 2015

[6] M. Garai-Fodor, “The Impact of the Coronavirus on Competence, from a Generation-Specific Perspective,” *ACTA POLYTECHNICA HUNGARICA,* vol. 19, no. 8, pp. 11-125, 2022. DOI: 10.12700/APH.19.8.2022.8.7

[7] P. T. Mai and A. Tick, “Cyber Security Awareness and Behaviour of Youth in Smartphone Usage: A comparative study between university students in Hungary and Vietnam.,” *Acta Polytechnica Hungarica,* vol. 18, no. 8, pp. 67-89, 2021. DOI: 10.12700/APH.18.8.2021.8.4

[8] M. Garai-Fodor, “Digitalisation trends based on consumer research,” in *IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023: Proceedings*, Budapest, 2023. DOI: 10.1109/SACI58269.2023.10158614

[9] P. Shah and A. Agarwal, “Cybersecurity behaviour of smartphone users in India: an empirical analysis,” *Information and Computer Security,* vol. 28, no. 2, pp. 293-318, 2020. DOI: 10.1108/ICS-04-2019-0041

[10] M. J. Miller, G. E. Higgins and K. M. Lopez, “Considering the role of e-government in cybercrime awareness and prevention: Toward a theoretical research program for the 21st century,” in *Citizens and E-Government: Evaluating Policy and Management*, C. Reddick, Ed., 2010, pp. 221-233. DOI: 10.4018/978-1-61520-931-6.ch012

[11] D. Yadav, G. Singh, K. Dave and R. S. Rai, “Internet Users' Habits and Cyber Awareness: A Cross Sectional Study,” *Pacific Business Review International,* vol. 10, no. 11, pp. 56-66, 2019

[12] D. J. Cranfield, I. M. Venter, R. J. Blignaut and K. Renaud, “Smartphone Security Awareness. Perceptions and Practices: A Welsh Higher Education Case Study.,” in *In Proceedings of INTED2020 Conference*, Valencia. Spain, 2020 2-4 March. DOI: 10.21125/inted.2020.0891

[13] T. McGill and N. Thompson, “Old risks. new challenges: exploring differences in security between home computer and mobile device use.,” *Behaviour and Information Technology,* vol. 36, no. 11, pp. 1111-1124, 2017. DOI: 10.1080/0144929X.2017.1352028

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

[15] I. Luyit, “Bridging spaces: Cross-cultural perspectives on promoting positive online learning experiences,” *Journal of Educational Technology Systems,* vol. 42, no. 1, p. 3–20, 2013. DOI: 10.2190/ET.42.1.b

[16] J. Abawajy, “User preference of cyber security awareness delivery methods,” *Behaviour and Information Technology,* vol. 33, no. 3, pp. 237-248, 2014. DOI: 10.1080/0144929X.2012.708787

[17] M. Zwilling, G. Klien, D. Lesjak, L. Wiechetek, F. Cetin and H. N. Basim, “Cyber Security Awareness. Knowledge and Behavior: A Comparative Study,” *Journal of Computer Information Systems,* vol. 62, no. 1, pp. 82-97, 2022. DOI: 10.1080/08874417.2020.1712269

[18] Saigoneer, “In 2017. 53% of Vietnamese Owned at Least a Smartphone. Compared to 35% in 2015: Report.,” 2018. [Online]. Available: https://saigoneer.com/vietnam-news/13774-in-2017.-53-of-vietnamese-own-at-least-a-smartphone.-compared-to-35-in-2015-report. [Accessed 10 November 2021]

[19] C. Bhaskar, R. Chaturvedi, C. Filipovic and G. Brewer, “Digital Intelligence Index,” 2020 [Online] Available: https://sites.tufts.edu/digitalplanet/files/2021/03/digital-intelligence-index.pdf. [Accessed 15 November 2020]

[20] Portulans Institute, “Network Readiness Index 2020,” 2020. [Online]. Available: https://networkreadinessindex.org/wp-content/uploads/2020/10/NRI-2020-Final-Report-October2020.pdf. [Accessed 15 November 2021]

[21] Portulans Institute, “Network Readiness Index 2020 Viet Nam,” 2020. [Online]. Available: https://networkreadinessindex.org/wp-content/uploads/2020/12/Viet%20Nam.pdf. [Accessed 2021 November 15]

[22] S. Kemp, “Digital 2021: Vietnam,” 21 February 2021. [Online]. Available: https://datareportal.com/reports/digital-2021-vietnam. [Accessed 15 November 2021]

[23] M. Daud and F. Khalid, “Nurturing the 21st Century Skills among Undergraduate Students through the Application and Development of Weblog,” *International Education Studies,* vol. 7, no. 13, pp. 123-129, 2014. DOI:10.5539/ies.v7n13p123

[24] L. Muniandy, B. Muniandy and Z. Samsudin, “Cyber Security Behaviour among Higher Education Students in Malaysia,” *Journal of Information Assurance & Cyber security.,* vol. 2017, pp. 1-13, 2017. DOI: 10.5171/2017.800299

[25] L. Z. Bain, M. Hayden and s. Sneeby, “An empirical study of user authentication: The perceptions versus practice of strong passwords,” *Issues in information systems,* vol. XI, no. 1, pp. 256-265, 2010. DOI:10.48009/1_iis_2010_256-265

[26] J. Cohen, Statistical power analysis for the behavioral sciences, Hillsdale: Lawrence Earlbaum Associates, 1988

[27] T. D. T. Xu, N. S. Polyakova and S. S. Shipilova, “Social Internet-networks in the life of Vietnamese students.,” in *SHS Web of Conferences*, 2016

[28] A. Murphy, W. Midgley and H. Farley, “Mobile Learning Trends Among Students in Vietnam,” in *Communications in Computer and Information Science*, 2014

[29] M. A. Ashwill, “Vietnam: An Outlier in the Coronavirus Epidemic and HE?,” 2020

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

[31] L. Bängens and B. Söderberg, “Mobile banking - Financial services for the unbanked?,” Spider, Uppsala, 2008

[32] B. N. Vuong, V. T. Hieu and N. T. T. Trang, “An empirical analysis of mobile banking adoption in Vietnam,” *Gestão & Sociedade,* vol. 37, no. 14, pp. 3365-3393, 2019. DOI: 10.21171/ges.v14i37.3078

[33] P. R. Hinton, I. McMurray and C. Brownlow, SPSS Explained, London and New York: Routledge, 2014

[34] N. U. Hadi, N. Abdullah and I. Sentosa, “An Easy Approach to Exploratory Factor Analysis: Marketing Perspective,” *Journal of Educational and Social Research,* vol. 6, no. 1, pp. 215-223, 2016. DOI: 10.5901/jesr.2016.v6n1p215

[35] C. DiStefano, M. Zhu and D. Mîndrilã, “Understanding and Using Factor Scores: Considerations for the Applied Researcher,” *Practical Assessment. Research. and Evaluation,* vol. 14, no. 20, pp. 1-11, 2009. DOI: https://doi.org/10.7275/da8t-4g52

[36] F. Breitinger, R. Tully-Doyle and C. Hassenfeldt, “A survey on smartphone user’s security choices. awareness and education,” *Computers & Security,* Vol. 88, 2019. DOI: 10.1016/j.cose.2019.101647

[37] B. H. Jones and L. Heinrichs, “Do business students practice smartphone security?,” *Journal of Computer Information Systems. 53(2),* Vol. 53, No. 2, pp. 22-30, 2012. DOI: 10.1080/08874417.2012.11645611