Information security behaviour of smartphone users: An empirical study on the students of University of Dhaka, Bangladesh.

Shohana Nowrin and David Bawden
Department of Library and Information Science
City, University of London

To be published in *Information and Learning Science*
Accepted for publication 19 May 2018
DOI 10.1108/ILS-04-2018-0029

Abstract

Purpose: The purpose of this study is to understand the information security behaviour of the students of the University of Dhaka, Bangladesh in the use of smartphones. Bangladesh is well known as one of the largest and fastest growing mobile phone market of the world, and the University of Dhaka is also the largest student's assembly in the country in terms of using smartphones. Besides, the rising use of smartphones are also likely to be typical of other sub-continent countries.

Design/methodology/approach: To gain an understanding of the information security behaviours of the students of University of Dhaka, Bangladesh, a quantitative survey method was deployed in revealing the approaches of the students towards avoidance of various security risks. A total of 356 students participated in the study, although eight of the participants did not carry out the full survey because they do not use smartphones. The collected data was analyzed with suitable statistical methods.

Findings: The findings of the study reveal that students of University of Dhaka possess a moderately secure behaviour in terms of avoiding harmful behaviours, utilizing useful phone settings and add-on utilities and disaster recovery. This study also shows that the students do not behave securely in all aspects of using different security features in the same way, and it also varies somewhat according to gender, and between Faculties and Institutions. The university library is recommended as the focus for instruction and guidance on best practice in smartphone use by students.

Research limitations/implications: The study does not include any other universities of Bangladesh except University of Dhaka due to the shortage of time. A further study can be conducted to gain an understanding in a greater extent by including students of the other universities and perhaps also other countries.

Originality/value – This is the first paper in Bangladesh relating the study of information security behavior regarding the use of smartphone among the student of University of Dhaka. This study will help to raise information security awareness among the students and encourage the authorities to adopt appropriate strategies and policies to resolve information security risks in the use of smartphones. Specially, the university library can take some initiatives in this case, like providing advice, seminars, workshops, lectures etc. in order to make the students aware about security issues.

Keywords: Information behaviour, information security behaviour, smartphone, Bangladesh.

Paper type: Research paper.

Introduction

The smartphone is considered a very useful instrument for communication in this digital age. Apart from mere call or text facilities, smartphones offer a wide range of computing capabilities and connectivity options through usage of various form of mobile applications. The usage of these applications has a great impact on the behaviour of smartphone users (Alfawareh and Jusoh, 2014). Currently students use smartphone applications for a diverse range of academic purposes (Woodcock et al., 2012), using various social networking sites, online shopping and banking, accessing email and many more. Because of the dramatic increase in number of smartphones, providing information security has become a great challenge for information security specialists and researchers (Esmaeili, 2014). Furthermore, ensuring overall smartphone network security is largely dependent upon individual information security behaviors of the users. This paper aims to conduct an empirical study on the information security behaviours of the students of University of Dhaka, Bangladesh in the proper use of smartphones, to protect the information security of the students. This study focuses on information security behaviour in the context of smartphones because Bangladesh is well known as one of the largest and fastest growing mobile phone market of the world. Furthermore, the smartphone sales in the capital city of Dhaka are much higher compared to the global average sales of smartphones which represent at least 20 percent of the total mobile handset sales of the country (Rahman, 2015). It is believed that the University of Dhaka, Bangladesh is the largest students assembly in the country in terms of using smartphones (Hossain and Ahmed, 2016) where over 31,955 students are studying (UGC, 2016). Besides, the uses of smartphones are also likely to be increasing in other sub-continent countries, and perhaps more widely. The objectives of this study are summed up in the following four research questions.

RQ1. Do the students avoid harmful behaviours in the use of smartphone?
RQ2. Are the students aware of useful phone settings or add-on utilities to maintain securities?
RQ3. Are they well prepared for disaster recovery?
RQ4. Do the information security behaviours differ among students who use smartphones?

Literature review

In the process of searching and collecting relevant literature, a range of databases were explored namely Web of Science, Emerald Insight, and ProQuest; also web resources, relevant blog posts, and online newspapers. Smartphones are used for range of activities like making phone calls, taking photos, text messaging, browsing internet, updating social media statuses, banking, sending/receiving emails, and many more. Such diverse usage of smartphones may not only cause unintentional leak of personal information but also can threaten the users with criminal blackmail attempts out of their embarrassments (Muslukhov et al., 2013). Another concerning factor is their tendency to download apps provided by the third parties without carrying out proper scrutiny (Mylonas et al., 2013). Another security issue can be raised because of the loss or theft of smartphones, in which case the personal information of the users can be acquired by the third parties (Imgraben et al., 2014). It is generally recognized that adopting appropriate security technologies has a great role to play in ensuring information security of the smartphone user (Ng et al., 2009; Esmaeili, 2014). However, the security technology alone cannot protect the information of the users completely (Imgraben et al., 2014). Moreover, it is well established that the

information security behaviour of the individual users has a direct effect on security aspects of smartphone (Rhee et al., 2009).

Several surveys have been carried out on the area of information security behaviours of smartphone users. In a recent study Das and Khan (2016) examined the information security behaviours of smartphone users in the Middle East. The authors tested a model which is based on existing research with survey data from 500 smartphone users. The authors aimed to determine the relationship between the information security behaviours with users' evaluation of security threats and responses to it as well as to gain an understanding about their concerns about particular threats. In a different study, Ngoqo and Flowerday (2015) investigated the low level of information security awareness of the students, who use mobile phones, with an aim of increasing the security awareness among the students and ensuring safer security behaviours thereby. This study proposed a framework named The Information Security Behaviour Profiling Framework (ISBPF) which can be used to estimate the profiles of information security behaviour of the student mobile phone users. Chandramohan and Tan (2012) conducted research to investigate smartphone security risks happening because of downloading the unsafe applications by the users. The authors evaluated how these unsafe applications mislead the users by pretending to be authentic and offer amusement, and then sell users confidential information to third parties.

Bangladesh is well known as one of the largest and fastest growing mobile phone markets of the world. It is reported by the Bangladesh Telecom Regulatory Commission (BTRC, 2017) that, by the end of the February 2017, mobile phone subscriptions have reached 129.584 million. Though there have been many research works conducted on the area of information security behaviour of the smartphone user, very few researches have been conducted on this field in Bangladesh. A review of relevant literature in Bangladesh reveals that the researches highlighted the field of information needs and seeking behaviour (Mostofa 2013; Hossain et al., 2017; Islam and Ahmed, 2012) and the use of smartphones from academic prospective (Hossain and Ahmed, 2016). There is a massive gap of research work in information security behaviour on smartphone use in Bangladesh. This research aims to address this, by conducting an empirical study on the information security behaviours of the students of University of Dhaka, Bangladesh.

Methodology

This exploratory research followed the survey method where a structured questionnaire was developed to conduct the online survey. The questionnaire was pilot-tested before going for the actual survey, by sending the link of the online questionnaire to 20 students through personal email, with the aim of redesigning the final survey if necessary. Google Forms was used to collect the responses from the students. A range of platforms and modes were used during online survey to reach the maximum number of respondents, including personal email and social media outlets such as Facebook, Twitter and Google Plus. Among these social networking sites, the researcher gave the priority to Facebook as it is the most popular social networking site in Bangladesh (Islam and Mostofa, 2015). 356 respondents participated in the survey initially, but subsequently 8 of the participants discontinued the survey after answering the questions in the demographic information section, as they do not use smartphones. Therefore, the sample size for the subsequent sections was 348.

The responses received from the students are presented in the form of tables and figures after analysis through usage of appropriate statistical methods. IBM SPSS and Microsoft Excel were used for analysis of data. Pearson' Chi-square test was used to test the significance of the differences between students' information security behaviours by gender and by Faculties/Institutions. In the test, the null hypothesis indicates that there is no difference between the groups. If the p value is less than 0.05 ($p < 0.05$), the null

hypothesis is rejected and concludes that there is significant difference between the groups. Otherwise, the null hypothesis is accepted to conclude that there is no difference between the groups.

Analysis of the study

The findings of this study are described in the following according to the research questions.

Academic and demographic information of the students

This section was designed to collect the academic and demographic information namely gender, age group and Faculty/Institution affiliation of the respondents.

Table 1*. Participating students (n=356), by Gender and Age*

Demographics	Frequency	Percent
Gender		
Male	251	70.5
Female	105	29.5
Age		
Under 18	5	1.4
18-24	298	83.7
25-34	52	14.6
35-44	1	0.3

The demographics of the participants are shown in Table 1, and their level of education attainments in Figure 1.

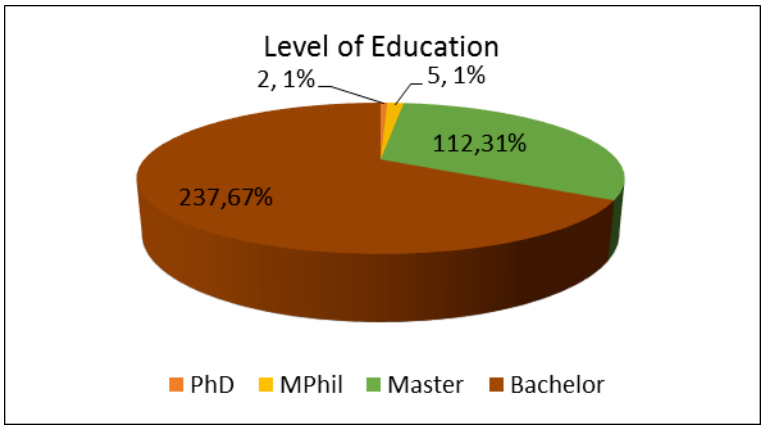

Figure 1. *Participating students (n=356), according to their level of education*

As will be discussed below, the nature of the study is reasonably in accord with the overall student population.

***Table 2**. Participating students (n=356), by Faculties/ Institutions*

Faculties/Institutions	Frequency	Percent
Arts	141	39.6
Social Sciences	38	10.7
Business Studies	70	19.7
Biological Sciences	29	8.1
Pharmacy	37	10.4
Engineering and Technology	9	2.5
Earth and Environmental Sciences	1	0.3
Fine Arts	4	1.1
Nutrition and Food Science	1	0.3
Disaster Management and Vulnerability Studies	2	0.6
Modern Languages	2	0.6
Leather Engineering and Technology	3	0.8
Statistical Research and Training	10	2.8
Education and Research	2	0.6
IIT	7	2.0
Total	356	100.0

A majority of participants were from the larger faculties within the university, particularly Arts and Business Studies. However, all parts of the university, including the smaller institutes, were represented, and so again the study may claim to be representative.

Smartphone information security behaviour of students

This section focuses on the information security behaviour of the students of University of Dhaka to establish their attitudes towards information security issues in the use of smartphones.

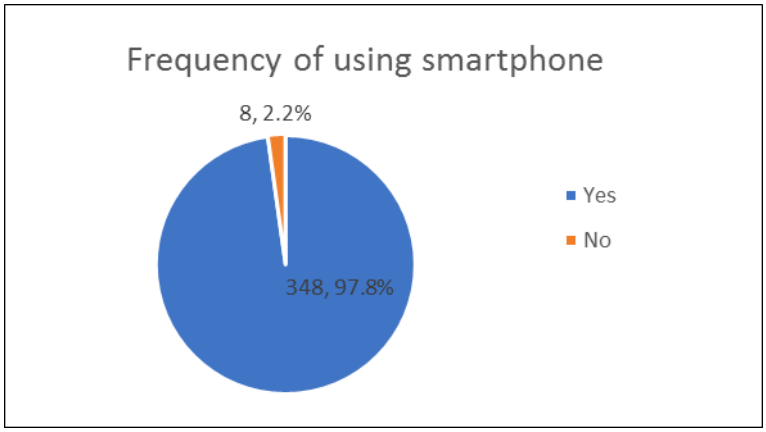

***Figure 2.** Participating students (n=356), by frequency of using smartphones*

It is clear from Figure 2, that virtually all students made use of smartphones.

***Table 3.** Participating students (n=348), by approaches towards avoidance of harmful behaviours*

Behaviours	Always	Sometimes	Never

Switch off all data connection	(74) 21.3%	(220) 63.2%	(54) 15.5%
Check permission/Access authorization to applications	(194) 55.7%	(99) 28.4%	(55) 15.8%
Avoid downloading apps from unknown sources	(199) 57.2%	(93) 26.7%	(56) 16.1%
Configure automatic locking	(168) 48.3%	(114) 32.7%	(66) 19.0%
Updates to smartphone systems and applications	(220) 63.2%	(104) 29.9%	(24) 6.9%
Use remote management apps	(55) 15.8%	(165) 47.4%	(128) 36.8%

Table 3 demonstrates the students' approaches regarding avoidance of harmful behaviours in the use of smartphones. It shows that a majority of students switched off all data connections 'sometimes' to reduce security risks. However, only 21% did so 'always', and nearly as many 'never' did so, a rather alarming pattern.

A positive sign is that the largest number, over half of students always checked the permission before authorizing any third-party applications, with only 16% never doing so. A similar good pattern of behaviour was observed for the downloading of applications, while the largest number, though not a majority, always kept a screen lock configured to avoid unauthorized access. However, a concerning proportion of students never practices these security precautions.

A majority of students kept updated with the latest versions of operating systems and applications, but - perhaps of concern - only 16% always considered security features of remote management apps.

Table 4. *Participating students (n=348), by approaches towards adopting useful phone settings and add-on utilities*

Behaviours	Always	Sometimes	Never
Deploy updates	(124) 35.6%	(150) 43.1%	(74) 21.3%
Installation of anti-virus software or application	(157) 45.1%	(92) 26.4%	(99) 28.4%
Modify privacy settings of the device	(152) 43.7%	(127) 36.5%	(69) 19.8%
Use apps for privacy protection management	(131) 37.6%	(117) 33.6%	(100) 28.7%
Reduce online "data traces"	(71) 20.4%	(168) 48.3%	(109) 31.3%

Table 4 gives a summary of the students' approaches in utilizing the useful phone settings and add-on utilities.

Although a majority 'always' or 'sometimes' used these features, it is concerning that substantial numbers 'never' did so, with nearly a third making no use of anti-virus or privacy protection software, or reducing data traces.

Table 5. *Participating students (n=348), by approaches for disaster recovery*

Behaviours	Always	Sometimes	Never
Data backup	(199) 57.2%	(85) 24.4%	(64) 18.4%
Data wiping out upon disposal	(51) 14.7%	(142) 40.8%	(155) 44.5%
Take out insurance	(44) 12.7%	(68) 19.5%	(236) 67.8%

The data in Table 5 shows that while less than a fifth of students never backed up information on their devices, the same proportion did not always permanently erase their data, and only 13% took our insurance for their device; again a mixed picture of security behaviour.

Comparison of student's information security behaviours

Table 6. *Participating students (n=348), by comparison of students' information security behaviours by gender and Faculties/Institutions in terms of avoiding harmful behaviours*

Behaviours	Gender			Faculties/Institutions		
	χ^2	df	Asymp. Sig.	χ^2	df	Asymp. Sig.
Switch off all data connections (e.g. by flight-mode)	3.998	2	.135	51.415	28	.004*
Check permission/Access authorization to applications	1.100	2	.577	35.144	28	.166
Avoid downloading apps from unknown sources	3.314	2	.191	43.496	28	.031*
Configure automatic locking	6.209	2	.045*	55.591	28	.001*
Updates to smartphone systems and applications	2.134	2	.344	49.412	28	.008*
Use remote management apps	7.367	2	.025*	47.891	28	.011*

The results of Chi-Square tests comparing the student's attitudes by *gender* suggested that there were significant differences in two out of six cases (Table- 6). Since the p-values for two items were less than the significance level of 0.05, therefore, the null hypothesis was rejected, and a conclusion was made that there were significant differences among the student's attitudes or behaviours by gender in terms of configuring automatic locking and using remote management apps. However, the percentages of 'never' in the use of remote management apps for both the male (38.6%) and female (32.4%) students were also alarming.

Analysis of student's attitudes by *faculties/institutions* in terms of avoiding harmful behaviours suggested that there were significant differences in almost all the cases excepts in checking permission/Accessing authorization to applications. Since the p-value ($p > 0.166$) of this item was greater than the significance level of 0.05. So, the null hypothesis was rejected in rest of the cases and a conclusion was made that there was significant difference in terms all those cases by faculties/institutions. For example, students from the Faculty of Arts were most concerned, and those from the Faculty of Business least concerned, about switching off data connection features.

On the other hand, commonalities were seen. For example, the largest proportion of students from all parts of the institution 'always' avoided downloading apps from unknown sources and the lowest proportion 'never' did so. The same is true of the updating of operating systems.

Table 7. *Participating students (n=348), by comparison of students' information security behaviours by Gender and Faculties/Institutions in terms of useful phone settings or add-on utilities*

Behaviours	Gender			Faculties/Institutions		
	χ^2	df	Asymp. Sig.	χ^2	df	Asymp. Sig.

Deploy updates	3.236	2	.198	41.949	28	.044*
Installation of anti-virus software or application	1.831	2	.400	71.086	28	.000*
Modify privacy settings of the device	.474	2	.789	45.851	28	.018*
Use apps for privacy protection/ permission management	5.450	2	.066	58.129	28	.001*
Reduce online "data traces"	12.939	2	.002*	38.244	28	.094

Table 7 shows the comparison of students' information security behaviours by gender and faculties/institutions in terms of useful phone settings or add-on utilities. The results of Chi-Square test comparing among the students' behaviours by *gender* suggested that there was significant difference between gender and in reducing online data traces, female students being much concerned than male students. Moreover, comparing students' information security behaviours by *faculties/institutions* suggested that there were significant differences in all the cases excepts in reducing online data trace.

The same pattern of some variation in behaviour between students from different parts of the university, with commonalities in the extreme 'always' and 'never' responses, was seen for use of anti-virus software and modification of privacy settings.

Table 8. *Participating students (n=348), by comparison of students' information security behaviours by Gender and Faculties/Institutions in terms of disaster recovery*

Behaviours	**Gender**			**Faculties/Institutions**		
	χ^2	Df	Asymp. Sig.	χ^2	df	Asymp. Sig.
Data backup	8.179	2	.017*	78.389	28	.000*
Data wiping out upon disposal	.755	2	.686	73.360	28	.000*
Take out insurance	6.146	2	.046*	35.364	28	0.160

Table 8 compares the students' information security behaviours by gender and faculties/institutions in terms of disaster recovery. The results of Chi-Square test showed that, there were significant differences between *gender* groups in terms of data backup and taking out insurance.

The percentage of 'always' for male students was higher than female students in the case of data backup. Male students were comparatively more aware than female students in terms of utilizing this feature. In the case of taking out insurance the students of the all faculties/institutions irrespective to their gender were very reluctant to adopt that and it was found that the 'never' had got the highest percentage of response for both genders.

On the other hand, students' attitudes by *faculties/institutions* in terms of disaster recovery suggested that there were significant differences in almost all the cases except in taking out insurance. So, the null hypothesis was rejected in rest of the cases and a conclusion was made that there were significant differences in terms all those cases of disaster recovery by faculties/institutions.

The same variation between students of different faculties and institutes was seen as for other aspects of security behaviour noted above.

Findings and discussions

The study shows that among the participants, the majority of students belong to the age group of 18-24 where there were more male participants than the female. Notably, such ratio is also apparent in the UGC report where the total number of students in the University of Dhaka is recorded with 31,955 where the male and female students proportion are 20,681 and 11,274 respectively. Meanwhile, 25,564 of students belong to the undergraduate programme who falls under the age group of 18 to 24 (UGC, 2016). The study population is therefore reasonably representative of the student body. Furthermore, other studies have suggested that demographic factors do not have any great influence on smart phone use and security concerns; see, for recent examples, Aharony (2017) and Johnson and Radhakrishnan (2017).

In this study, the first objective (RQ.1) is to investigate the students' approaches towards the features regarding avoidance of harmful behaviours in the use of smartphones. The findings of this survey suggest that over half of the features were responded positively by a majority of students where they answered with 'always' to utilize these security features. The second objective (RQ.2) of this study is to find out the students' behaviours in using phone settings and add-on utilities. It is revealed that about half of the features are utilized by the majority number of students 'sometimes'. Among these features, the largest number of the students exercise disabling reduce online data traces feature. Meanwhile, the features like 'installation of anti-virus software' and 'modify privacy settings' are utilized 'always' by about half of the students. Though the students do not utilize the security features accurately at all time, it is apparent that overall the students are not so vulnerable to information security breach in this case. Under the third objective (RQ.3), the approaches of the students in disaster recovery present very concerning results. In the case of data wiping out upon disposal and taking out insurance, a largest number of students never adopt these important disaster recovery features. The outcome of this study in this case very concerning because these features play a crucial role in securing information from the access of the third party. To achieve the fourth research objective (RQ.4), a chi-square test was conducted to find out the differences between students' information security behaviours by gender and Faculties/Institutions. During making comparison by gender, it is observed that in respect of avoiding harmful behaviour, and useful phone settings or add-on utilities section, female students are less vulnerable than male students in the case of 'configuring automatic locking' and 'reducing online data traces' accordingly. On the other hand, under the section of disaster recovery the male students are comparatively more concerned than female students in using 'data backup'. However, in using the feature of 'taking out insurance', both genders seem very vulnerable to security breaches. This might have happened because separate insurance policies only for smartphones are not very popular in Bangladesh.

After analyzing cross tab of Chi-square test, it can be observed that in terms of avoiding harmful behaviours, utilizing useful phone settings and add-on utilities, and maintaining disaster recovery by Faculties/Institutions, mixed approaches were found among the students. None of the Faculty/Institution possesses secured attitudes towards all the features of smartphone information securities. A Faculty which seemed secured in using one feature is found vulnerable to other features. For instance, in the case of 'avoid downloading applications from unknown sources', students from the Faculty of Arts possess a secured behaviour. Meanwhile, the Faculty of Business Studies shows that the students are much aware about utilization of 'data backup' whereas in the case of 'data wiping out upon

disposal' feature, the students of that Faculty look very unaware. These differences may occur because individual students of different faculties possess independent perception about various security features, perhaps because of instruction given locally, or awareness of particular examples of problems arising locally. The recommendation below that university libraries may be well-placed to offer advice on smartphone security to students addresses this point, since librarians will be well-placed to appreciate differences between parts of their institutions.

Overall, it is found from the study that, in some cases the students utilise the security protocols of certain features sometimes where they remain vulnerable to security threat on rest of the times and those other times cannot be ignored under any circumstances because that may cause risk to the students as well as other users of the smartphone network. The reasons behind that the students do not make better use of security features in their use of smartphones is likely to be a combination of lack of understanding of the importance of such issues, combined with a disinclination to take the time and effort necessary to take appropriate measures. In a survey of smartphone security among Chinese users of all kinds, Zhang, Li and Deng (2017) found that students were more likely to take security measures than the general population, and emphasised the need for instruction in these matters. However, one positive aspect is that the level of knowledge about the smartphone security issues has been improved among the students after participating to this research survey. Although this study was focused on the students of University of Dhaka, Bangladesh but the results are not just of interest to that university or to Bangladesh, because the behaviours of smartphone users are likely to be typical of students (and perhaps other people) in other countries as well. The poor information security behaviours of the students observed in our study against some of the security threats go along the research outcome acquired in Das and Khan (2016).

Recommendations

Based on the data analysis, findings and suggestions from the students, a detailed set of measures can be identified to reduce the information security risks. The major recommendations are as follows:

i. Configure the automatic locking system in the smartphone so that after a fixed time it locks automatically.

ii. Check access authorization before installing the application in the smartphone. It will make aware about what types of personal information can be accessed by the application developers.

iii. Disable the Bluetooth and GPS of the smartphone to protect unauthorized access to the device and be aware when using public Wi-Fi or unknown internet connection.

iv. Install proper antivirus software or firewall protection to make the smartphone free from viruses, malware or spyware.

v. Be cautious in clicking on unknown sources or links which may cause security breaches. Smart phones can be affected by spyware, malware or other viruses for clicking on the unknown sources.

vi. Perform regular software and system updates in the smartphone so that new features of information security can be available in the device.

vii. Educate users in the above points by organizing seminars, workshops, and also train the users about handling confidential information to minimize the problem of information security. This may best be done within the context of the university library, as noted below.

Conclusion

Smartphones provide a range of new facilities for the users, at the same time the use of smartphone also increases the risk of information security breaches. Therefore, it is important to understand the information security behaviours to design the solutions and increase awareness among the users. Information security awareness may contribute in changing information behaviours of the smartphone users which will help to minimizing the information security risks as well in the use of smartphone. However, the outcome of this study will contribute with some important information which will be useful in gaining better understanding about information security behaviours in the use of smartphones. Such understanding may help to develop suitable strategies and policies as well as introduction of necessary training programmes for the improvement of information security in the use of smartphones. Specially, the university library would be well-placed take some initiatives to make students aware about security issues through advices, seminars, workshops, lectures besides other information issues. This fits well with the trend for university libraries to encourage use of smartphones for accessing library services among other academic purposes, both in the developing world (see, for example, Elahi, Islam and Begum 2018, and Sharma and Madhusudhan, 2016) as well as in Europe and North America (see, for example, Abbas, MacFarlane and Robinson 2017). It also fits well with the mission of university libraries to improve the information and digital literacy capabilities of their students, with privacy and security being increasingly important issues; see, for example, Wissinger (2017) and CILIP (2018). Besides, students' views regarding which methods or approach would be helpful for them can be taken into consideration in providing appropriate awareness programme by the university libraries. Further studies can be carried out with larger sample size by including students from other universities, as well as exploring other dimensions of smartphone information security behaviours of students.

References

Abbas, Z., MacFarlane, A. and Robinson, L. (2017), "Use of mobile technology by law students in the law library: an exploratory study", *Legal Information Management*, Vol.17 No.3, pp.180-189.

Aharony, N. (2017), "Factors affecting LIS Israeli students' mobile phone use: an exploratory study", *The Electronic Library*, Vol. 35 No.6, pp.1098-1121.

Alfawareh, H.M. and Jusoh, S. (2014), "Smart phones usage among university students: Najran University case", *International Journal of Academic Research*, Vol. 6 No. 2, pp. 321-326.

Bangladesh Telecom Regulatory Commission (BTRC) (2017), "*Mobile Subscribers".* (Online) Available at: http://www.btrc.gov.bd/content/mobile-phone-subscribers-bangladesh-february-2017 (Accessed 3 May 2017).

Chandramohan, M. & Tan, H.B.K. (2012), "Detection of mobile malware in the wild". *Computer*, Vol. 45 No. 9, pp.65-71.

CILIP (2018), *"What is information literacy? CILIP Information Literacy Group",* (Online) Available at http://www.cilip.org.uk/default.asp?page=informationliteracy, (Accessed 7 May 2018).

Das, A. & Khan, H.U. (2016), "Security behaviors of smartphone users". *Information & Computer Security*. Vol.24 No. 1, pp. 116 – 134.

Elahi, H., Islam, S. and Begum, D. (2018), "Perception on the use of mobile phones in retrieving information from academic libraries - a developing country perspective," *International Journal of Knowledge Content Development and Technology*, Vol. 8 No.1, pp.37-50.

Esmaeili, M. (2014*), "*Assessment of users' information security behavior in smartphone networks". *Master's Theses and Doctoral Dissertations.* Eastern Michigan University. Paper 581.

Hossain, M. U, Hossain, M. A & Islam, M. S. (2017), "An assessment of the information needs and information-seeking behaviour of Members of Parliament (MPs) in Bangladesh". *Information and Learning Science,* Vol. 118 No. 1/2, pp.48-66.

Hossain, M.E. & Ahmed, Z. (2016), "Academic use of smartphones by university students: a developing country perspective". *The Electronic Library*, Vol.34 No.4, pp. 651-665.

Imgraben, J., Engelbrecht, A. & Choo, K.K.R. (2014), "Always connected, but are smart mobile users getting more security savvy? a survey of smart mobile device users". *Behaviou r & Information Technology*, Vol.33 No. 12, pp. 1347-1360.

Islam, M. M. and Mostofa, S. M. (2015), "Usage pattern of Facebook among the students of Dhaka University: a study". *Annals of Library and Information Studies,* Vol. 62 No. 3, pp. 133-137.

Islam, M.S. & Ahmed, S.Z. (2012), "The information needs and information-seeking behaviour of rural dwellers: A review of research". *IFLA journal*, Vol. 38 No. 2, pp.137-147.

Johnson, S. and Radhakrishnan, N. (2017), "Academic use of smart phones among the students of business schools in the UAE: a study", KIIT Journal of Library and Information Management, Vol 4 No.1, pp.32-36.

Mostofa, Sk. M. (2013), "A study of information needs and seeking behavior of faculty members of Darul Ihsan University in Bangladesh". *Library Philosophy and Practice* (e-journal). pp. 983

Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2013), "Know your enemy: The risk of unauthorized access in smartphones by insiders". *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 271-280). Munich: ACM.

Mylonas, A., Gritzalis, D., Tsoumas, B. and Apostolopoulos, T., (2013), "A qualitative metrics vector for the awareness of smartphone security users". *In International Conference on Trust, Privacy and Security in Digital Business* (pp. 173-184). Berlin, Heidelberg: Springer.

Ng, B. Y., Kankanhalli, A. & Xu, Y. (2009), "Studying users' computer security behavior: a health belief perspective". *Decision Support Systems*, Vol.46 No.4, pp. 815–825.

Ngoqo, B. & Flowerday, S.V. (2015), "Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users". *Computers & Security*, Vol. 53, pp.132-142.

Rahman, M.F. (2015), "*Smart Phone Sales Soar on Low-Cost Brands: Symphony, a Local Vendor, Is the Leader in Mobile Handset Market.*" (Online) Available at: http://www.thedailystar.net/smartphone-sales-soar-on-low-cost-brands-55910 (Accessed 7 May 2017).

Rhee, H.S., Kim, C. & Ryu, Y.U. (2009), "Self-efficacy in information security: its influence on end users' information security practice behaviour". *Computers & Security,* Vol.28 No.8, pp. 816-826.

Sharma, R. and Madhusudhan, M. (2016), "Use of mobile devices by library and information science students in central universities of Uttar Pradesh", *DESIDOC Journal of Library and Information Technology,* Vol. 37 No. 3, pp.293-302.

UGC (2016), "42th Annual Report: 2015". Dhaka: Bangladesh University Grant Commission. pp. 302.

Wissinger, C.L. (2017), "Privacy literacy: from theory to practice, Communications in Information Literacy", Vol. 11 No. 2, pp. 378-389.

Woodcock, B., Middleton, A. and Nortcliffe, A. (2012), "Considering the smart phone learner: an investigation into student interest in the use of personal technology to enhance their learning", *Student Engagement and Experience Journal*, Vol. 1 No. 1, pp. 1-15.

Zhang, X.J., Li, Z. and Deng, H. (2017), "Information security behaviors of smartphone users in China: an empirical analysis", *Electronic Library*, Vol. 35 No.6, pp.1177-1190.