CITY, UNIVERSITY OF LONDON

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

SHOHANA NOWRIN

September 2017

Submitted in partial fulfilment of the requirements for the degree of
MSc in Library Science

Supervisor: Professor David Bawden

1. Abstract

Smartphone is the most popular electronic device in the present world. Along with the use of internet, smartphone has made revolution in the information communication technology sector. The current operating systems of smartphones allow to download mobile applications providing diverse types of features and functions. At the present days, the use of smartphone increases to a large extent that it is impossible to think a single day without using the smartphones. The widespread use of smartphones has introduced new types of information security threats, risks and vulnerabilities. The risky user behaviours, non-implementation of security counter measures and storage, and transmission of the vast amount of sensitive information in the smartphones are causing massive information security problems. Security of information is greatly depending on the information security behaviour of the users. Moreover, Information security behaviour has a direct impact to secure the information in the use of smartphone. In this study, the information security behaviour of the students of university of Dhaka, Bangladesh in the use of smartphone has been explored. This study had followed the survey method where a structured questionnaire was developed after exploring relevant literature to conduct the online survey for achieving research objectives. A total of 356 students had participated to the study where eight of the participants did not carry out the full survey because they do not use smartphones. The collected data was analyzed with suitable descriptive statistical methods. Students' information security behaviours have been explored through observing their attitudes towards adapting or avoiding certain security features in terms avoidance of harmful behaviours, useful phone settings and add-on utilities and disaster recovery in the use of smartphone. The chi-square test was carried out to find the differences between students' information security behaviours by Gender and Faculties/Institutions. It has been explored from this study that 100% of the students who use smartphones also use internet. Accordingly, most of the students are aware about security issues in the use of smartphones. Unlike many other studies, in this study the students seem to be cautious in a moderate level in using the smartphone security features. However, a significant percentage of students been found in the case of using every security features, who either 'sometimes' or 'never' utilize those features in the use of smartphones. These students are in very vulnerable situation to security risks and they are also dangerous for the other users of the network. It has been observed that some students behave with awareness in using certain features but the same group appear to be unaware in using other features. Therefore, unless overall security behaviours of the students get collectively improved, the vulnerability to security risks cannot be cured properly. This study will help to raise information security awareness among the students and encourage the authority to adopt appropriate strategy, policy and develop necessary training program to resolve information security risks in the use of smartphones. However, further research can be conducted by inclusion of a large sample size out of the students of other universities also. Moreover, other dimensions of the security issues can be explored in further research. Accordingly, there can be a topic of interest that the students are knowingly ignoring to take into account the security countermeasures even after knowing about the risk of vulnerability to security breaches rather than being cautious to those security issues.

2. Table of contents

3. List of Tables

4. List of Figures

5. Acknowledgement

At first, I wish to acknowledge the immeasurable grace and profound kindness of Almighty, the supreme Ruler of the Universe, who enabled to make my dream a reality.

I am grateful to my supervisor professor David Bawden for his kind supports, valuable suggestions and providing necessary information to complete the dissertation perfectly. Without his direction, guidance, instruction, suggestion, inspiration, stimulation and constant encouragement, the accomplishment of this work would have not been possible.

Most importantly, I would like to thank the students of the university of Dhaka, Bangladesh who took part in this research. Without their generous and willing cooperation and support this study would not have been possible. For completing this study, I had to depend upon different international and national publications. I am really grateful to all the authors whose works I have used in this dissertation.

There are many people to whom I am grateful for the professional and personal support in the completion of my thesis. I must give my heartily thanks to my husband Rashedul Hasan for the regard and affection he has always shown to me. At last, I would like to express my deepest gratitude to my father and my mother for their kind cooperation and constant inspiration that helped me to bring out this study.

Shohana Nowrin

6. Introduction

6.1 Background and context

Mobile phone or smartphone is considered as a very useful instrument for communication in this age of information communication technology and it becomes an integral part of our daily life. Basically, the introduction of smartphone devices has upgraded the mobile phone communication to a different level. Apart from mere call or text facilities, those were provided by the traditional mobile phones, smartphone offers a wide range of computing capabilities and connectivity options as like as traditional computers through usage of various form of mobile applications. The usage of these applications has great impact towards the behaviour of smartphone users (Alfawareh and Jusoh, 2014). Along with other group of users, students are also great fond of using smartphones. Currently students do use smartphone applications for diverse range of academic purposes (Woodcock et al., 2012), using various social networking sites, online shopping and banking, accessing to email and many more. Therefore, the smartphones are becoming very popular day by day among the students. Moreover, Because of the dramatic increase in number of smartphones, providing information security has become a great challenge to consider for the information security specialists and the researchers. (Esmaeili, 2014).

Since the internet facilities are available in smartphones, various mobile applications are used in it which inevitably increases a range of information security risks. Because of the diverse use of these mobile applications, personal information gets collected and stored in the smartphones which can easily be aggregated to draw a complete information and be used maliciously (Jones and Chin, 2015). In such circumstances, protecting personal information through adaptation of security measures are very crucial. However, it is critical to understand the information security behaviour in the use of smartphones. Furthermore, ensuring overall smartphone network security is largely dependent upon individual information security behaviors of the users because inappropriate practices like weak passwords, opening emails from unknown sources, downloading applications from unauthorized websites, not keeping up to date with security patches and so on may make the network vulnerable to security breaches (Esmaeili, 2014). This study investigates the information security behaviours of the students of University of Dhaka, Bangladesh in the use of smartphones. This exploratory research had followed the survey method where a comprehensive review of relevant literature was conducted to gain an understanding about the given topic clearly, which helped to set up structured questionnaire for data collection accordingly. The collected data have been analyzed to gain an understanding about the information security behaviours of the students in consideration of various aspects like their attitudes towards avoidance of harmful behaviours, useful phone settings and add-on utilities, disaster recovery and finally a comparison has been made in terms of information security behaviour among the students of University of Dhaka, Bangladesh.

6.2 Aims and objectives

The aim of this research is to explore the students' information security behaviour in the use of smartphone of University of Dhaka, Bangladesh and assisting relevant department or institutions in adopting necessary steps as well as developing strategies and policies for the students regarding smartphone information securities.

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?

6.3 Scope and definition

This study investigates students' attitudes towards the information security behaviour in the use of smartphone of University of Dhaka, Bangladesh. The University of Dhaka, Bangladesh has been chosen carefully because it is one of the best public universities of Bangladesh with huge resources, large number of students, great reputation, strong faculties as well as the researcher has got the direct contact with the institution. The study does not include any other universities of Bangladesh except University of Dhaka due to the shortage of time. upon considering the result of this study, further studies can be carried out with large sample size by including students from other universities of Bangladesh as well as other dimensions of the smartphone information security behaviours of the students might be explored thereby. This study intends to raise information security awareness among the students and encourage the authority to take necessary initiatives to resolve information security risks in the use of smartphone.

Smartphones are expected to contain the minimum efficiency of using mobile applications through internet. On the other hand, smartphone can be defined as mobile device which can perform the function of a computer usually with touch screen interface and where it is also possible to download or install applications through operating system by using internet connections. According to Jeon et al. (2011) the smartphones can be defined as a device which provides advanced computing ability and connectivity on the top of the basic features of the mobile phones.

Information Security demonstrates securing the information from unauthorized access or disclosure as well as protecting the information. The authors, Mattord and Whitman (2012) defined the information security in the book of *Principles of Information Security* as "the protection of information and the systems and hardware that use, store, and transmit that information." In contrast, Anderson (2003) defined the information security as "a well-informed sense of assurance that information risks and controls are in balance". Accordingly, the information security demonstrates "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide information confidentiality, integrity, and availability" (Kissel, 2013, p.94). Sari (2012) defined information confidentiality as the way of protecting information from intelligible interception and unauthorised disclosure; information integrity as securing the completeness and accuracy of information; and information availability as ensuring vital services and required information are available upon demand. Generally, information security comprises the information confidentiality, authenticity, availability, integrity and accountability (Zissis and Lekhas, 2011). Apart from confidentiality, integrity and availability, some other characteristics of information such as authenticity, non-repudiation, accountability and so on were identified in regard to information security. However, all of these characteristics will be discussed in the following accordingly.

Confidentiality of information demonstrates that only authorized person to the certain information will be eligible for accessing rights to that information. On the other hand, Mattord and Whitman (2012) pointed that the confidentiality of information can be breached if any unauthorized body or personnel gets access to the protected information.

The integrity of information refers to the situation where users become able to trust the information they use as of genuine and in authentic state. According to Mattord and Whitman (2012) the information can be considered with the quality of integrity only when the information is complete, whole and uncorrupted. Furthermore, under the integrity of information nobody should be able to edit or delete the information without permission from the appropriate authority and the preventing measures against corruptness caused by viruses or others ought to be in place. Nist glossary (2013) found that the integrity of information refers to the fact that the sensitive data ought not to be edited or deleted by following an undetected or unauthorized manner.

In defining the *availability of information* Mattord and Whitman (2012) mentioned that - "Availability enables authorized users—persons or computer systems—for access to the information without interference or obstruction and to receive it in the required format." It is expected in principle that the information system would be able to provide information upon demand and failure to do so would lead to the obstruction of availability as well as security breach.

The *authenticity of information* was defined as per the latest ISO/IEC standard as "property that an entity is what it is claims to be" (ISO/IEC 27000, 2014). In another argument Nist glossary (2013) described the authenticity as confidence in consideration to the fact that the message originator, message or transmission is valid. However, the confidence generally grows when something can be verified and something is trusted. Therefore, it can be said that the authentication maintains close relation with authenticity. So, the confidence of authenticity gets established when authentication verifies the identity of users, devices and processes (Nist glossary, 2013).

In terms of defining the *accountability of information* Mattord and Whitman (2012) said "Accountability, also known as auditability, ensures that all actions on system—authorized or unauthorized—can be attributed to an authenticated identity." The security goal of the accountability is to become able to trace out actions of entities or individuals uniquely and perfectly. However, by the grace of this accountability security factors, a range of issues like intrusion detection, fault detection and conducting legal action becomes convenient (Nist glossary, 2013).

In a study, some smartphone information security risks were identified as Data leakage, Improper decommissioning, Unintentional data disclosure, Phishing, Spyware, Network spoofing attacks, Surveillance, Diallerware, Financial malware and Network congestion (ENISA, 2010). Finally, the information security is a massive concern in the modern world and all these security concerns cannot be limited by drawing specific boundary because latest major and minor concerns are emerging continuously.

It is difficult to define information security behaviour because of its vastness and complexity (Rantonen, 2014). Different people have measured the information security behaviours in different aspects. Information security behaviour is nothing but taking precautions by adaptation of necessary measures to secure one’s information, devices and so on. Due to the wider use of the internet, individual users put the fellow users at risk along with themselves, therefore, recognising the risks and taking necessary precautions are important subject in the present time (Li and Siponen, 2011). Agarwal and Anderson (2010) defined information security behaviour as the understanding of individual willingness in taking recommended security precautions like running and updating antivirus software, securing passwords, utilising a firewall and becoming cautious about emails sent by unknown sources at their own accord to protect themselves. So, it can be said that the information security behaviour in the use of smartphone demonstrates, taking necessary precautions for the safety of individual’s own personal smartphone device as well as others in the internet with an aim to improve information security measures.

7. Research context / literature review

The twenty first century has experienced a large amount of new technologies like social networking, LED lighting, voice over IP, cloud computing, smartphones, e-paper and many more but the smartphone is considered as the fastest growing, most powerful and influential technology of the modern time (Ross, 2011). Smartphones are the advanced form of traditional mobile phone with better connectivity and computing ability. It is no longer focused only to the basic features of mobile phones like making voice calls, texting or video messaging. It brings range of facilities by incorporating various technologies into it like a computer. Among many other diverse usage, smartphones are used for the storing various personal information like contact details, location information, bank details, emails, and so on of an individual (Jeon et al., 2011). Moreover, it facilitates with diverse features of various kinds. Some of the most significant smartphone features are internet facilities, radio, telephone, television, GPS navigation system, camera, personal hotspot, gaming console, projector, music player, Wi-Fi hot spot and many more (Ross, 2011; Pitt et al., 2011). The popularity of Smartphones is getting higher day by day because of their portability, computing power and relatively cheaper price range and, therefore, they are about to supersede the traditional computer devices (Chin et al., 2012; Brenner, 2013).

Among many others, nowadays, the smartphones are capable of creating, sharing and consuming contents, provide location services like global positioning system (GPS), navigation, maps and location-aware search, performing financial transactions through online banking and electronic payments. Basically, the operating systems provided by a few number of corporations are run on these smartphones to perform its activities (IDC, 2016). Using these operating systems millions of applications (apps) both free and paid, created by the third parties, provide all sort of services performed by the traditional computers on top of the various additional services of smartphones (TechCrunch, 2014). The rapid growth of smartphones has made the mobile computing available to the large number of people. Statistic shows that there are larger number of smartphones in use compare to the personal computers (PC) (Business Insider, 2013).

It is apparent that the smartphones have deep impact on the personal life of the users and they have been using it as personal device. It enables the users to stay connected to the information at any location and time. Since the web facilities can be carried in the pocket with the smartphones, it facilitates with convenient and wide range of online service connectivity on top of it, like social networking, online shopping, online learning and many others. Users generally share their personal information, preferences and track records along the way of conducting various online activities like online banking, playing games, searching product information, doing online transactions and many more (Chang et al., 2009; Pitt et al., 2011). Smartphone provides most of these facilities through mobile applications which are downloaded by using internet facilities and currently there are more than one million mobile applications available in the web. The mobile applications are basically a type of application software which are run mostly in the smartphone or tablets for providing particular services. These applications are generally circulated by using the internet as a platform. Users can download the applications from online stores according to their needs to personalise the smartphones (Pitt et al., 2011). Considering the configurations of smartphones and the diversity of mobile applications used in it, this can be easily observed that the smartphones of the current time, in most cases, are more powerful than the desktop computers of the previous decade and contain more features than personal computers (Pitt et al., 2011).

7.1 Smartphone security issues/concerns

The nature of the information security risks associated with the smartphones are different than the computer. The smartphones were invented and circulated in the market in mid 2000s which created a new area of information security threat and a significantly new set of information security risks and vulnerability were introduced since then. Notably, the information security risks associated with smartphones are increasing continuously due to the rapid large growth of smartphone use (Burns and Johnson, 2015; Landman, 2010). Researchers have been working on the area of computer and information security since 1970s (Saltzer and Schroeder, 1975). This has been observed that the computer and information security practices have failed to cover and cope up with the information security risks associated with smartphones (Bickford et al., 2010).

Due to storing of various personal information in the smartphone, several information security risks are associated with this. It becomes essential to understand the importance of securing this personal information contains in the smartphone. Smartphones are used for range of activities like making phone calls, taking photos, text messaging, browsing internet, updating social media statuses, storing contact information, banking and sending/receiving email and many more. Such diverse uses of smartphones do not only cause unintentional leak of personal information but can also exploit the users with criminal blackmail attempts out of their embarrassments (Muslukhov et al., 2013). In most cases third party applications are used in the smartphones who may sometimes get the automatic access to the personal information without the consent of the users (Das and Khan, 2016). Other concerning factor is their tendency to download apps provided by the third parties without carrying out proper scrutiny (Mylonas et al., 2013 a). Generally, the smartphone users download and use the applications without being aware about security measures of those applications which may lead to the serious security risk for them (Gajjar and Parmar, 2015). Furthermore, Lin and Varadharajan (2010) described the fact that the increased use of smartphones has also heightened the information security risks because of the users' inadvertent behaviour on installing mobile applications. Due to such practice, the personal information of the users can easily be passed to the third party. It is also observed that the users also share their sensitive data/personal information without being aware of the security risks associated with it. The reasons behind making decision to disclose sensitive data were identified by Workman (2007) as trust, fear, likability and authoritative standing. Therefore, ensuring the security of mobile networks as well as preventing information security breaches are two of the main current challenges for the information system security specialists of the smartphone networks. It was presented in a news report that the smartphone users do almost nothing to secure their personal information contains in the smartphone device (CNBC, 2014).

Another security issues can be raised because of the loss or steeling of smartphone in which case the personal information of the users can be acquired by the third parties as well as the sensitive information might be destroyed permanently (Imgraben et al., 2014). The likeliness of loss or steeling of smartphones frequency is very high because it is such a small hand-held computing device which can be carried everywhere very easily (Ballagas et al., 2006). Similarly, Lazou and Weir (2011) observed that the mobile devices are more likely to face accidental loss and theft compare to large systems fixed in the particular location (p. 183). Sometimes the users do forget to pick the smartphones after laying it down and mistakenly leave the phones behind by walking away. In addition to the prospect of losing the smartphone device, operating it by using the public network either in the coffee shops, airports or any other places raises the risk to information security (ENISA, 2010).

Malware attack is another kind of security issues in the use of smartphones. The malicious software applications which intercept the smartphone users' actions and transmit information to the third party fraudulent site are known as smartphone malware. The malwares are still active threat and well known for their malicious behaviours. As the smartphones are used as the “social” device, it is likely that the malware placed in the network will be spread out rapidly and have far-reaching impacts (Peng et al., 2014). As per the anticipation which was made a decade ago, the smartphones are widely adopted and the processing power of the devices have been developed significantly for which they became “the target of viruses, worms and other malware programs” (Furnell, 2005). In a study Chandramohan and Tan (2012) described about how the software system securities are attacked by the malware and the ways of using malware to gain financial benefits by the fraudsters. In another study Lawton (2008) discussed about the malware InfoJack which functions to send infected smartphones’ serial number and operating system information to the hackers to enable them changing security settings of the smartphones in a way that, they become able to install their required applications in the background of the phone for stealing information. Banking applications are also attacked by the Malware for stealing login details and other financial information (Wang et al., 2012). Apart from this, the smartphones which are connected through the Bluetooth or Wi-Fi, may be affected by malwares where the unauthorized access might be gained to collect and damage sensitive information by performing meaningless operations (Wang et al., 2012; Jeon et al., 2011). In a study, it was also said that, this is probable that the smartphones may be infected by the MPV and in such case, those are likely to spread malicious programs rapidly using the internet connections and exchanging of executable files (La Polla et al., 2013). However, the information security risks of the smartphones have been increased to a great extent because a large number of populations are adopting smartphones due to its popularity but not taking into account the security measures properly. In a study, some other smartphone information security risks were identified as Data leakage, Improper decommissioning, unintentional data disclosure, phishing, spyware, network spoofing attacks, surveillance, diallerware, financial malware and network congestion (ENISA, 2010).

Besides the fact of easily obtainability of sensitive data, the information contained in the smartphone devices also get lost largely because of the psychological influences by the users (Okenyi and Owens, 2007; Luo et al.,2011). It is observed that, in most of the cases the users are not even aware of their vulnerability to attack in their smartphone devices (Furnell et al., 2008). It was argued by the Burns and Johnson (2015) and Nurse et al. (2015) that irrespective to legitimate or illegitimate reason, the sensitive data are always easily obtainable. Such absence of information security awareness and the lack of security conscious behaviour enable the attacker to put less effort to break the security hurdle for gaining access to the stored information (Anderson et al., 2008; Furnell et al., 2008).

Typically, the users have been argued as the weakest link in information system security in several studies, who continuously do harmful internet behaviour and put themselves at risk thereby (Anderson et al., 2008; Ramim and Levy, 2006; Stanton et al., 2005). According to Furnell et al., (2008, p. 235) “Users have significant issues with their online behaviour, carrying out risky online practices”. Furthermore, risky information security practices of the users have been noted as one of the vital reasons of disclosure of their sensitive data (Anderson et al., 2008; Chin et al., 2012). Accordingly, the users who are not exhibiting security conscious behaviour, nor utilising security tools are of extreme risk and should be treated with particular importance (Furnell et al., 2007; Husted et al., 2011; Mylonas et al., 2013 b). For one reason or another, sometimes the users are unwilling to safeguard themselves from information insecurity, which make them primary target for attack (Chipperfield and Furnell, 2010). Despite an increased publicity can be observed regarding information security risks, associated risks and consequential security breaches, there were very little efforts given to improve the security behaviours and practices of the smartphone users. So it can be said that the interest to learn and adopt the robust security technologies like antivirus, strong password, firewall, encryption and anti-spyware by the users, could minimize the risk of smartphone network related security breaches. On the other hand, not practicing the security behaviour by the users may make the networks unsecured and vulnerable to security breaches (Esmaeili, 2014).

7.2 Resolving the security and privacy problems

Information security risks in the use of smartphone is the most concerning issue of the current age. Although the advanced technological development brings many facilities in the use of smartphones but those facilities also brings security threats to the smartphone users. So it is important to take necessary measures or raise awareness among the users to mitigate the security threats. users may minimise the risk of breaching information security by adopting latest technologies like strong passwords, antivirus, anti-spyware, encryption, firewalls and others (Esmaeili, 2014).

One of the technologies for smartphone security measures can be considered as using appropriate password. In a study Park et al. (2014) said that unauthorised access to personal information by others may be prevented by using security password. In another study Hogben and Dekker (2010) observed that deploying the authentication methods like PIN or password together with screen lock system can be considered as an effective method of protecting smartphones from unauthorized access as well as privacy intrusion. An alternative method to this knowledge based authentication system is the use of biometric methods like Touch ID or face unlock system (Bhagavatula et al., 2015), although it was argued by different authors that the deployment of authentication mechanism in the smartphones is time consuming (Harbach et al., 2014 a). However, a study conducted on 2011 had revealed that only a quarter number of users believe that the PIN can be helpful in protecting mobile phone (Ben-Asher et al., 2011).

Another useful security mechanism, in protecting the information of the smartphone users, is use of the antivirus applications in the mobile phone. Sometimes antivirus software helps to prevent attacks from unsafe links, viruses, phishing, and malwares accordingly (Jeon et al., 2011). The device-level authentication may also deliver the frontline protection for the smartphone users in terms of regulating the access to individual applications as well as other information contained in the smartphones (Botha et al., 2009).

Performing necessary scrutiny before providing permission to the third-party application is also identified as an important act to assure the security of private information in the use of smartphone (Hogben and Dekker, 2010). Different operating systems of the smartphones offer different permission mechanisms (Kraus et al., 2016). Besides, in order to promote the better understanding and attention of the apps permission among the users, a range of solutions have been recommended by different authors, that may include the risk communication and importance of the improvement of information presentation (Kelley et al., 2013; Harbach et al., 2014 b; Kraus et al., 2014 and Benton et al., 2013).

Smartphone security risks initiated by the malwares can be mitigated by keeping the devices up to date. Though keeping smartphone devices up to date is an important security measures but this measure is highly dependent upon the smartphone users' information security behaviour because evidently, they are reluctant to keep their devices up to date all the time (M¨oller et al., 2012). Apart from these, smartphone security awareness and security education is also required to ensure information security. The smartphone education and the awareness generally demonstrates the knowledge about existing security controls available to the users for protecting information (Keys, 2013). According to the Larkin (2009), the available existing controls to the users are mainly device password protection, installing security software including remote access software and applications to alert for abnormal transaction. As confidential information like credit card numbers, details of bank transactions, social security information and other electronic records stored in the smartphones are likely to causes potential dangers to the smartphone users (Dourish et al., 2004); therefore, it is important for the users to be aware of security measures in using of smart phone when they deal with this confidential information in their smartphones.

The data backup option is also one of the significant information security features in the use of smartphones. The backup function may recover the sensitive information. Basically, with the data backup option a copy of the information is kept stored in the smartphone (Li et al., 2014). According to Chin et al. (2012) data backup plays an important role in recovering the data in the case of lost or theft of the devices. Other features that can mitigate the problem of device loss like remote data wipe, device encryption, device locators are sometimes poorly adopted by the users (Mylonas et al., 2013 b). The reasons behind poorly adopting these measures might be the unawareness of the users about the availability of such features (Chin et al., 2012).

In a report of ENISA (2010) on information security and privacy risk a list of opportunities in ensuring smartphone securities were indicated. In that report, the Sandboxing had been identified as mostly used apps and capability-based access control models by which it is possible to control the installation of unsecure apps. 'The controlled software distribution' facilitates the providers to have better control over app security as the submitted apps are passed through vetting process, so that the security flaws can be scrutinized and insecure apps can be removed accordingly in there. Installation of the remote application removal functions to remove the malware from smartphone devices. Backup and recovery function is integrated in most of the smartphone devices which minimize the risk of data loss. Extra authentication options provide additional facility for authentication, such as some smartphones can be used as card reader.

7.3 Information security behaviour

It is highly 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, only the security technologies itself cannot protect the information of the users completely (Imgraben et al., 2014). Alongside, the security of information also dependent in a great extent on the behaviour of individual users in the use of smartphones (Esmaeili, 2014). Moreover, it is well established that the information security behaviour of the individual users has the direct effect on security aspects of smartphone (Rhee et al., 2009).

A wide range of research has been carried out for understanding information security behaviour in the use of smartphone from different aspects. Ngoqo and Flowerday (2015b) conducted a study on information security behaviours of the student mobile phone users, with an aim to levering security awareness as a way of stimulating safer information security behaviours, where they proposed a framework that can be used to profile the students' information security behaviour. It was examined by Harris and Patten (2014) that in downloading mobile applications from the repositories, the smartphone users show over confidence which cause information security risks. In a study Jones et al. (2014) said that it is important to investigate security features of the mobile applications before downloading because the applications from unknown sources are considered as the major risk to information security.

Moreover, utilizing appropriate phone settings and adopting proper add-on utilities can offer a layer of defense in ensuring smartphones information security. It is found that adopting appropriate technologies can empower the users in ensuring information security in the use of smartphone (Jones and Heinrichs, 2012). Furthermore, according to Souppaya and Scarfone (2012) add-on utilities in smartphones can play a significant role in protecting information security. Encryption mechanism can also be used to reduce the information security risks and threats for smart phone users (Park et al., 2014).

In the event of loss, stolen or damage of smartphones, protecting information by adopting data recovery plan can be very crucial. A practice of regular data backup by the smartphone users would minimise the risk of information loss in such case. Accordingly, data wiping out before disposing the devices is also proven as very crucial (ENISA, 2010). It is examined in a study by Botha et al. (2009) that the smartphones are more likely to confront accidental loss or theft than any other electronic devices. So, it is clear that better understanding of the importance of information security aspects and security behaviour of the smartphone users can be helpful to reduce the information security risk and manage the overall security of the information of the smartphone users properly. Harris et al. (2015) argued that the information security risks arise due to the possibility of loss or damage of the smartphones need to be understood by the users appropriately to ensure mitigating such risks.

7.4 Factors affecting the information security behaviour

There has been much researches conducted in identifying the factors of information security behaviours. Among many other cases, a large number of authors have identified the human behaviours as one of the causes of information security breaches (Zhang et al., 2009).

Some of the significant factors like security practices (technology), security practices (care behaviour), intention to IT practice and self-efficacy, have great significance to influence the information security behaviours of the users (Karamizadeh et al., 2013; Rhee et al., 2009; Lee and Kozar, 2005). However, a recent research was conducted by Ngoqo and Flowerday (2015a), to have an understanding about the relevant factors that cause the poor information security behaviour of the student mobile phone users, through analysis of the existing theories in the perspective of social sciences. The authors identified two principle aspects relevant to the information security behaviours of the students namely awareness and behavioural intent. Subsequently, the study suggested that these two aspects might be very significant to reduce the knowing-and-doing gap. Two basic human oriented factors namely knowledge and behaviour towards information security were mentioned by the Van Niekerk and Von Solms (2010). The authors found that the adequate security measures may not work properly when the users lack the proper level of knowledge or cooperation in this regard. For instance, most of the mobile phones offer update installation features which require the users to instigate it; however, if the users do not use this feature, a behaviour, which may cause the security vulnerabilities.

In a study of Yoon et al. (2012), the authors examined the factors of information security behaviours that motivates the college students' information security. They developed a research model by adopting well established Protection Motivation Theory (PMT). The authors integrated social norms and habit factors to the model in identifying the students' behaviour of information security. The study finds out that students' information security behaviour depends on the level of severity, self-efficacy, response efficacy and response cost. Their study suggested that education in security awareness and understanding severity of security issues influences student attitude towards information security. Another study conducted by Bojmaeh (2015) also explained about the main factors that influence the information security behaviours of the users. In this study, the author discussed about four groups of information security factors namely self-efficacy, security practice-care behaviour, intention to IT security practice and security practice-technology that have influence towards information security behaviour. The obtained result from this study demonstrates that all these factors have a noteworthy and positive impact on information security behaviour where security practice-care behaviour gained the highest impact. Esmaeili (2014) formed an information security behaviour model by evaluating the theoretical frameworks of human behaviour. In this model attitude, intention, breaching experience, computing experience and facilitation condition have been identified as important factors that influence smartphone information security behaviour. The objective of this model is to find out the relationship among the factors that affect smartphone security behaviour of the users. Moreover, the model aims to help in understanding the impact of these factors towards practicing information security behaviour as well as utilizing security technologies in the smartphones.

7.5 Related survey findings on smartphone securities

Several surveys have been carried out on the area of information security behaviours of smartphone users. In a most 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 the collected 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 tried to gain an understanding about their concerns against particular threats like data leakage, malware and data theft. The study also revealed that the users are more concerned about malware attack and data leakage than loss of information and users' security behaviours are mainly influenced by the factors like efficacy and cost effectiveness of security measures.

In a different study Ngoqo and Flowerday (2015b) investigated the low level of information security awareness of the students, who use mobile phone, 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. The results of this study revealed a possible relationship between information security awareness and behavioural intension. Accordingly, such relationship helps to exhibit the information security behaviour profiles of students. However, by identifying the link between these (awareness and intension), the framework reveals new method for categorizing and tracking the information security behaviour profiles of the student mobile phone users.

Simpson (2016) showed that there is significant gap in literature on the aspect of smartphone security. The author identified six cognitive factors namely self-efficacy, party trust, institutional trust, awareness on security risks, vulnerability and threats and influence on smartphone security behaviour and practice on the basis of traditional computer security domain which have significant impact on information security behaviours and practice. The study aims to analyse the factors and their persuasive significance which was identified previously on the basis of traditional computer security and tried to find out the implication on the aspect of smartphone security. The findings of the study identified that threats, vulnerability and risk awareness are associated to each other by which it is possible to predict the security practice, self-efficacy and behaviour of the smartphone user. However, knowledge of all three categories of awareness is important for the users for being able to protect themselves against all possible security risks and vulnerabilities. The result of the study will help the smartphone users as well as the organizations to mitigate the inappropriate smart phone user's security behaviour and practice by focusing on the specific areas of concern.

It was found in a study after conducting a survey on students participated from four of the universities in Budapest on February 2010 that, generally the users' view the mobile phone communication as secure which, possibly, make them relaxed in using it. Furthermore, as the students lack the appropriate security education, they are not aware about necessary security measures required to be adopted for protecting unauthorized access to their mobile information. Moreover, the statistical analysis of the survey findings also revealed that there was a big difference among students, in terms of using mobile operating system where the respondents were found to be using either old or new mobile operating systems. However, the students actually failed to secure their phones. Finally, the study came up with the conclusion that in mitigating the danger of information security risks, the students either need to be properly educated or be offered a transparent security features (Androulidakis and Kandus, 2011).

Chandramohan and Tan (2012) conducted a research to investigate smartphone security risks happen because of downloading the unsafe applications by the users. The researchers put focus on the main security risks of the smartphones namely malware, spyware and greware. The authors evaluate how these unsafe applications mislead the users by pretending to be authentic and offer amusement and then sell users confidential information, steal user's credentials, manipulate users browsing input and content delivery. And finally, the study tried to find out some solutions like detecting malware before downloading unknown applications for getting rid of these security risks caused by unsafe applications. This malware detection can be carried out by dynamic analysis, static analysis, application permission analysis and cloud based detection.

Lawton (2008) carried out a study on security threats of malware in the smartphone. The main focusing issues in this study was the security threats that are faced in smartphone during conducting the financial transactions. The authors observed how the malware attacks smartphone through Bluetooth, email, instant messaging and flashcard memory readers. The findings of this study suggested that this malware attacks in smartphone can be controlled by using antivirus software, raising awareness among the users, firewalls and using secured and authentic applications. Waehlisch et al. (2012) did a similar study relating financial transaction where they made an effort to identify the available security options for security risks that the users faced during conducting such financial transaction. The respective risk factors and the probable solutions they highlighted were the malware detection to control stealing data, establishing ad-hoc trust with an aim to build secure trust between two devices, provision of secure data transmission to ensure sending data securely and reporting the level of threats to the security application from all component. Furthermore, Zonouz et al. (2013) carried out a research where the authors proposed cloud computing as a solution for information security threats. It is said that the security support can be provided through this cloud computing which would be located in a trusted location and be operated centrally to make the users aware of malware.

Botha et al. (2009) conducted a research on mobile security where they suggested for some considerations that must be followed by the users when they use smartphone for the first time. In that study, the authors observed the security risk by describing the issues like, user authentication (e.g. using passwords for user authorizations) and security issues relating network connections and harmful contents. In a study Lin and Varadharajan (2010) presented a new technique namely the trust enhanced security for smartphones. This new technique recommends the smartphone security solution to be trust-centric rather than security-centric. Under this solution, the traditional security mechanism gets extended by including the trust based decisions where the trust based relationships can be identified separately and be managed properly. However, the integration of such trust related issues into security decision making proceedings formulate the outcome of the trust enhanced security mechanism. The research indicates to the initial stage, when the built-in apps of the mobile phones are laid for the first time in the device. It further argues that the control for providing trusts on those application through making authorisation to those are exercised by a particular party. Therefore, the research draws a conclusion that the trust towards application by the smartphones, trust from the applications towards smartphones in recognising authentication, and combined effort of the trust and security in the smartphone network can achieve the goal of ensuring smartphone security.

7.6 Bangladesh aspects

Bangladesh is well known as one of the largest and fastest growing mobile phone market of the world. It is reported by the Bangladesh Telecom Regulatory Commission (BTRC, 2017) that, by the end of the February 2017 the mobile phone subscriptions has reached to 129.584 million. Furthermore, the smartphone sales in the capital city of Dhaka are much higher compare to the global average sales of smartphones which represent at least 20 percent of the total mobile handset sales of the country (Rahman, 2015). Though there have been many research works conducted on the area of information security behaviour of the smartphone users but no research has been conducted yet 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 the area of information security behaviour on smartphone use in Bangladesh. However, this research aims to conduct an empirical study on the information security behaviours of the students of University of Dhaka, Bangladesh in the use of smartphone to protect information security of the students.

University of Dhaka, Bangladesh is regarded as one of the best universities in Bangladesh. This is the oldest university of the country. The university is well known for its quality education and research activities. The university was established on 1st July 1921 with 3 Faculties, 12 Departments, 60 teachers, 877 students and 3 dormitories. Sir P. J, Hartog[1] was the first vice chancellor of the university. Currently, there are 13 Faculties, 77 Departments, 11 Institutes, over 51 Research Centres in the university (www.du.ac.bd). The number of teachers and the students has reached to 2306 and about 31,955 accordingly (UGC, 2016). The university offers Ph.D., M.Phil., graduate and undergraduate programs. It includes the Faculty of Arts, Science,

[1] Hartog, Sir Philip Joseph (1864-1947) was the first Vice Chancellor of the University of Dhaka. He was a British national who was born in London on 02 March 1864. Apart from holding the Vice Chancellor position in the University of Dhaka, other important roles he performed were as a member of Indian Public Service Commission, a member of the Calcutta University Commission and the chairman of the Committee on Indian Education. Hartlog was well versed in English, French, German, Urdu, Hindi and Bangla. His most notable publications are *Culture: Its History and Meaning*, *The Marks of Examination* (1936) and *An Examination of Examinations* (1935) This great personality had passed away on 27 June 1947 [Banglapedia]

Business Studies, Biological Sciences, Faculty of Fine Arts, Engineering & Technology, Faculty of Medicine, Pharmacy, Faculty of Education, Faculty of PGMIR and Faculty of Law.

The University of Dhaka had played a vital role in all critical junctures in the national history of Bangladesh. It played a great role in the Language Movement during 1948 to 1952 that eventually culminated in the recognition of Bangla as a National Language of East Pakistan of that time. This great institution also made huge contribution in the liberation war of the nation. A number of students, teachers and employees sacrificed their lives for earning the independence of the country in 1971. The University of Dhaka was declared under the legislation of "The Dhaka University Order 1973" only just after the creation of Bangladesh in 1971 as a democratic and autonomous body.

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). Moreover, this is the most reputed university of the country. The significance of the University of Dhaka is not limited to the academic achievement only but it led from the front in all major civil rights movements of the nation. The university is considered as the lighthouse of the education sector of Bangladesh. Due to the factor of cheap availability of smartphones, a massive number of smart phones are used by the students. These students use their phones for several reasons including social networking, education purposes, entertainment, financial transaction and various other applications. The wi-fi facilities provided by the university covers almost full area of the campus. The students also use internet connection provided by their respective mobile network. However, the diverse use of internet by these massive number of students are, undoubtedly, not free from information security risks. After considering all these relevant factors, the University of Dhaka has been chosen as the sample for conducting this empirical study.

From the above it can be observed that new sets of information security issues related to threats, risks and vulnerabilities have been emerging continuously due to the increased use of smartphones throughout the world. The provided literature seeks to identify functions and features of today's smartphone, different smartphone security issues or risks, possible solutions to overcome these security risks, behaviours which are related to information security in the use of smartphones, factors that affect information securities and relevant survey findings on information security behaviours. After exploring the relevant literatures of these topics in detail, it became convenient to find out that what types of security risks can be arisen, how those issues can be solved and how information behaviours of the users can affect the overall security of the information and also helped to identify the specific security features to determine the information security behaviours of the students in regard to smartphone. Though there have been many research works conducted on the area of information security behaviour in the use of smartphone but no research has been conducted yet on this field in Bangladesh. With due consideration to this issue, this study aims to conduct an empirical study on the information security behaviours of the students of University of Dhaka, Bangladesh in the use of smartphone.

8. Methodology

In order to gain an understanding of the information security behaviours of the students of University of Dhaka, Bangladesh in the use of smartphones an empirical research was conducted as a piece of original work. A quantitative research method was deployed in revealing the approaches of the students towards avoidance of various security risks, phone settings and add-on utility features as well as disaster recovery. However, this chapter discusses the strategy and methodology of conducting this research work. After discussing the research strategy, the study follows through describing the data collection methods, framework of data analysis, limitations and future studies, ethics and confidentiality accordingly.

8.1 Research strategy

This exploratory research had followed the survey method where a structured questionnaire was developed to conduct the online survey to achieve research objectives. Survey method is considered as one of the prominent ways of acquiring relevant information like social characteristics, behaviours, attitudes of the focussed group of people on any given topic (Bird, 2009; Rhee et al., 2009). Therefore, online survey method had been chosen for this research to collect data towards gaining understanding the information security behaviours of the students of University of Dhaka in the use of smartphones.

In the process of searching and collecting relevant literature, a range of databases were explored namely Web of Science, Emerald Insight, ProQuest and many more. In many cases the researcher also took the help of university library guides for searching the relevant journals on the given topic and in some cases also used the Google scholar alert and Zetoc alert services in order to gain updated and relevant literature accordingly.

8.2 Data collection methods

With the view of achieving research objectives properly, the structured questionnaire was developed for collection of data based on the review of literature by keeping in view of the aspects those are relevant to the research objectives. The questionnaire was designed carefully to ensure the maximum responses from the participants. Furthermore, the questionnaire was prepared as free from ambiguity with a plain language without involving any technical words which could require expertise knowledge. Questionnaire was pilot-tested before going for the actual survey accordingly to be assured about the validity of the findings. Necessary modification of the questionnaire had been brought upon considering the feedback of the pilot-testing. However, due consideration for all relevant aspects was given during preparing the questionnaire. In this respect, Oppenheim (1992) suggested that it is important to design the questionnaire appropriately as inadequate design of questionnaire will not only discourage respondents from participating but also increase measurement error. In order to achieve research objectives properly, the survey questionnaire was developed in two parts. In the first part of the questions, the demographic information of the participants like age, gender, level of education and Faculties/ Institutions had been collected. The second part aimed to collect the exploratory information related to information security of the students in the use of smartphones. The students were expected to convey their individual perception through answering the set questionnaire designed to achieve the research objectives.

The target population of this research is the students of the University of Dhaka, Bangladesh. The survey data were collected throughout the months of June and July 2017. The survey was conducted through online. In carrying out the online survey, the Google Forms was used to collect the responses from the students. The researcher used the Google Forms for preparing online survey questionnaire and collecting data due to its nature of being free, mobile friendly, and where virtually unlimited respondents can participate in the survey (Agarwal, 2014). Range of platforms and modes were used during online survey to reach the maximum number of respondents like personal email and social media outlets such as Facebook, Twitter and Google Plus. The social media was chosen because sixty percent of the Dhaka university students use social networking sites (Hossain and Ahmed, 2016). Notably, among these social networking sites, the Researcher gave the priority to Facebook as it is the most popular social networking site in Bangladesh and a vast majority of students of University of Dhaka use it (Islam and Mostofa, 2015). Therefore, the Facebook was given importance in the current study. The link to online survey questionnaire (https://goo.gl/forms/LJ4FoQz6w25JW5mx2) was also shared several times in the respective Facebook group pages of the University of Dhaka to reach out the maximum number of students. Many students were also approached personally through Voice call, E-mail, Facebook messenger as the Researcher has direct contact with the institution. However, a total of 356 completed questionnaire were finally returned by the respondents. Furthermore, though there were 356 respondents participated in the survey initially, but subsequently 08 of the participants discontinued the survey after answering the questions in the demographic information section as they do not use smartphones (they were said to do so in the questionnaire; see *Appendix - C*); therefore, the sample size for the subsequent sections were 348 accordingly.

8.3 Framework for data analysis

The collected data from questionnaire was analysed with suitable descriptive statistical methods. The responses received from the students are presented in the form of tables, figures and analysed using appropriate statistical methods. The IBM SPSS statistics (Statistical Package for Social Sciences) and Microsoft Excel were used for descriptive analysis of data. Pearson' Chi-square test was used to find out the differences between students' information security behaviours by Gender and Faculties/Institutions. The chi-square test generally gets deployed to find out the significant differences between the concerned population being tested (Gravetter and Wallnau, 2009, p. 619). 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.

8.4 Limitations and future study

This study investigated the students' attitudes towards the information security behaviour in the use of smartphone at University of Dhaka, Bangladesh. Dhaka University was chosen carefully because it is one of the best public universities of Bangladesh with huge resources, large number of students, great reputation, strong faculties as well as the Researcher has got the direct contact with the institution. 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 upon considering the result of this study by including students of the other universities. Furthermore, the review of the relevant literature had to be kept in confined due to time constraint. This study may raise information security awareness among the students and the relevant authority may take necessary initiatives to resolve the risks of information security issues regarding the use of smartphones. It is recommended to bear in mind that the research is only exploratory. Moreover, further research work can also be carried out for the exploration of other dimensions of the smartphone information security behaviours of the students as well as other group of users.

8.5 Resources

In conducting this survey, the Google Forms were utilized for preparing the survey questionnaire because it is free and mobile friendly as well as can be used for acquiring huge number of responses. The survey questionnaire was subsequently distributed by using various online platforms. Generally, a link to the online questionnaire was provided to the participants through social networking sites like Facebook, Twitter, Google plus, email and other group posts. After receiving data from the respondents, those collected data were processed and analyzed by using IBM SPSS Statistics and Microsoft Excel.

8.6 Ethics

In any given research, ethical issues are the very important aspects to consider because ethical issues may arise in any stage and out of any consequence of progression of the research. According to Hart (2009, p.296), "... ethical issues can arise during all stages of your research, from the design stage through to the reporting stage ...". In this study, it is expected that no major ethical issues will arise because of the nature of the research. The survey of this research was conducted through online questionnaire and all the prospective participants are the university students who are over 18 years old. Besides, no personal data of the respondents was collected which may raise the ethical issues. Moreover, the participants were neither be called for any face to face interview, nor been attended to any private premises. Copyright issues were taken care of appropriately as the researcher maintained the citations correctly when relevant literature was used. So, overall it can be expected that no ethical issues will arise from this study. Additionally, an ethics check list form provided by the university had been incorporated at the end of the research proposal.

8.7 Confidentiality

In this research, a survey was conducted among students of University of Dhaka, Bangladesh where the students answered the survey questions with fair, open and honest attitude. There are very minor possibilities of coming across sensitive information because the researcher did not collect any personal information of the students. The participants were kept anonymous during collecting their responses and the highest level of personal information included only the faculty/Institution name of the students for enabling the researcher comparing their information security behaviours in the use of smartphones. Besides, the email address of the researcher was provided in the online survey questionnaire, so that the respondents can contact, if they wish to make further query about this research or for any further correspondence or referrals, by making sure that their details remain confidential. However, the information collected from the students were not used in a manner which may be considered as abusive towards the respondents because the respondents were not identifiable and the collected data were kept confidential.

9. Analysis and findings of the study

This empirical study investigates the information security behaviours of the students of University of Dhaka, Bangladesh in the use of smartphones. The survey focused on the students' attitudes in using specific application in terms of avoiding harmful behaviours, their approaches towards useful phone settings and add-on utilities in maintaining securities, their level of preparation for disaster recovery and whether the information security behaviours differ among students who use smartphones. The findings of this study have been described in the following according to the research questions.

In the study, there were 356 respondents who participated initially which were reduced to 348 subsequently due to the non-use of smartphones by eight of the respondents. The questionnaire was divided into two parts namely section- A (academic and demographic information of the students) and section- B (smartphone information security behaviours of the students). In section- A, all 356 participants responded to the questions. In section- B, it was found that eight of the students does not use any smartphones who did not continue to answer the questions in section- B.

Section-A: 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**. University of Dhaka: 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 Table-1 presents that among the respondents, the majority (251, 70.5%) of students were male participants and the rest (105, 29.5%) of the respondents were female. Therefore, it was observed that there were more than double male respondents compare to female participants. However, the number of overall male students were also higher than the female students in the university. According to UGC report, the total number of students in the University of Dhaka is 31,955 where the male and female students proportion are 20,681 and 11,274 accordingly (UGC, 2016). In terms of age, the highest number of participants (298, 83.7%) belonged to the 18-24 age group. This was followed by the age group of 25-34 which represented 52 respondents (14.6%). A small group of respondents (5, 1.4%) belonged to the under 18 age group, and only 1 participant (0.3%) belonged to the age group of 35-44. Notably, the maximum of the overall students in the University of Dhaka belonged to the age group of 18-24 who were either pursuing bachelor or masters level of education.

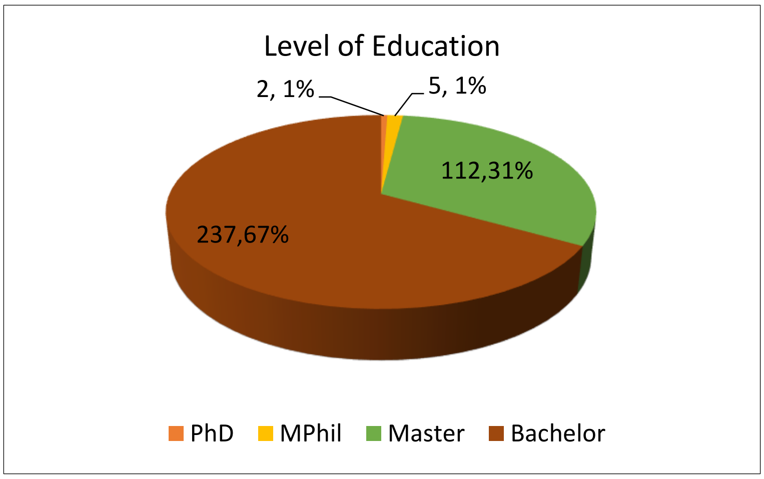

Figure 1. *University of Dhaka: participating students (n=356), according to their level of education*

It is apparent in the Figure-1 that the majority (237, 67%) of students were pursuing bachelor program which was followed by the master's program (112, 31%). Only a very small number of students who participated to the study were pursuing MPhil (5, 1%) and PhD (2, 1%) accordingly. Notably, the frequency reflected real time scenario of the overall students' proportion in the university because it admits less students in the MPhil and PhD program. According to UGC report (2016, p. 308), the aggregate number of students in the University of Dhaka for the MPhil and PhD program is 1153 where the total number of students in the university including all level of education is 31,955.

***Table 2**. University of Dhaka: participating students (n=356), by Faculties/ Institutions*

Faculties/ Institutions	Frequency	Percent
Faculty of Arts	141	39.6
Faculty of Social Sciences	38	10.7
Faculty of Business Studies	70	19.7
Faculty of Biological Sciences	29	8.1
Faculty of Pharmacy	37	10.4
Faculty of Engineering and Technology	09	2.5
Faculty of Earth and Environmental Sciences	01	0.3
Faculty of Fine Arts	04	1.1
Institute of Nutrition and Food Science	01	0.3
Institute of Disaster Management and Vulnerability Studies	02	0.6
Institute of Modern Languages	02	0.6
Institute of Leather Engineering and Technology	03	0.8
Institute of Statistical Research and Training	10	2.8
Institute of Education and Research	02	0.6
IIT	07	2.0
Total	356	100.0

The Table-2 shows that the highest number of respondents (141, 39.6%) were from the Faculty of Arts which was followed by the Faculty of Business Studies (70, 19.7%). Other three faculty's students who represented close number of responses to each other were namely the Faculty of Social Sciences (38, 10.7%), the Faculty of Pharmacy (37, 10.4%) and the Faculty of Biological Sciences (29, 8.1%). The participants from rest of the other Faculties/Institutes individually represented very less percentage each, towards the overall respondents. However, the data collected from these Faculties/Institutions might not be representative due to their low response rate.

Section-B: Smartphone information security behaviour of the students

This section investigates the information security behaviour of the students of University of Dhaka where the Researcher tried to find out students' attitudes towards information security issues in the use of smartphones.

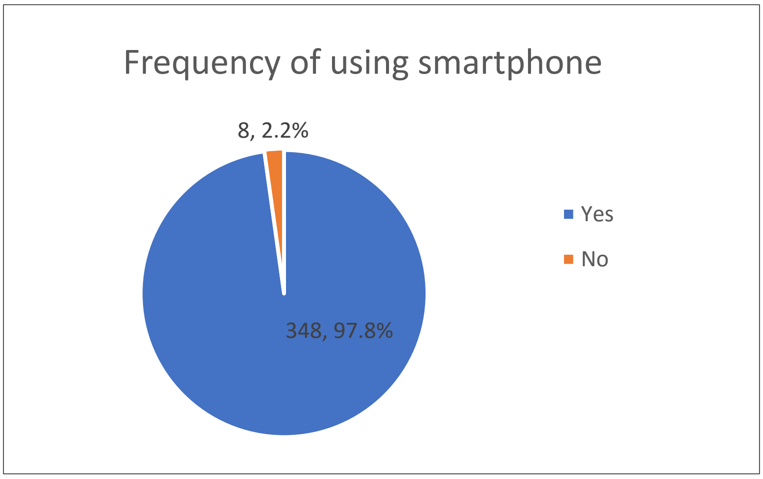

Figure 2. *University of Dhaka: participating students (n=356), by frequency of using smartphones*

The Figure-2, shows the number of respondents who use smartphones. It was observed that the majority of students (348, 97.8%) had been using the smartphones and only a small number (8, 2.2%) of students did not use any smartphones. According to Hossain and Ahmed (2016) smartphones are very popular for academic purposes among the vast majority of students of the University of Dhaka, Bangladesh.

This must be noted in this section that the Researcher aimed to investigate the information security behaviour of the students in the use of smartphones only. In the questionnaire, it was asked to the non-users of the smartphones to discontinue the following survey questions. In that case, the students who did not use the smartphones were not subject to the research and have not been included in the following parts of the study. Therefore, the sample size for the subsequent parts of the research was 348.

Table 3. *University of Dhaka: participating students (n=348), by duration of smartphone use*

Duration of using smartphones	Frequency	Percent
Less than 1 year	19	5.5
1 - 2 years	67	19.3
3 - 4 years	156	44.8
5 - 6 years	66	19.0
More than 6 years	40	11.5
Total	348	100.0

Table-3, demonstrates the duration of using smartphones by the students where it was found that the largest number of the students (156, 44.8%) had been using the smartphones for last 3-4 years. The percentages of students who were using smartphones for 1-2 years (67, 19.3%) and 5-6 years (66, 19.0%) were almost similar. It was observed that 40 (11.5%) students were using smartphones for more than 6 years. Only a small number (19, 5.5%) of students had been using smartphones for less than 1 year.

Table 4. *University of Dhaka: participating students (n=348), by having the internet connection in their smartphone*

Internet connection	Frequency	Percent
Yes	348	100
No	00	00
Total	348	100.0

Interestingly, it was observed that all students (348, 100%) who had been using smartphones were also using the internet in their phone (See Table- 4). It was reasonable to assume that the smartphone users will use internet in their mobile phone because most of the smartphone features do not function properly without internet connection. However, it is important to note here that most of the information security risks are closely related to the use of internet on smartphones.

Table 5. *University of Dhaka: participating students (n=348), by frequency of internet use*

Frequency of internet use	Frequency	Percent
Several times every day	290	83.3
A few times every day	42	12.1
At least once a day	07	2.0
A few times a week	04	1.1
At least once a month	05	1.4
Total	348	100.0

It was found from the questionnaire survey that the frequency of accessing internet using smartphones was very high among the students of University of Dhaka, Bangladesh. Table- 5 reveals that the majority (290, 83.3%) of students were using internet several times a day in their smartphones where only a small number (42, 12.1%) of students had been accessing to the internet a few times every day. The huge differences of the numbers give an idea about the tendency of using internet in smartphones among the students were very high.

Table 6. *University of Dhaka: participating students (n=348), by mode of internet access*

Internet connection used	Frequency	Percent
Mobile network	25	7.2
Wi-Fi	122	35.1
Both	199	57.2
Total	346	99.4
Unanswered	02	0.6
Total	348	100.0

It is shown in Table-6 that a large number (199, 57.2%) of students accessed to internet using both Wi-Fi and mobile network. The second largest group (122, 35.1%) of students used the Wi-Fi mode only, which was followed by the remaining (25, 7.2%) students who used mobile network only to connect into the internet. This should be noted that two (0.6%) students did not answer to this question.

Table 7. *University of Dhaka: participating students (n=348), by reason for using smartphones*

Reason for using smartphones	Frequency*	Percent
Communicating with family, friends and teachers	291	13.8
Academic purpose	264	12.5
Browsing online	210	10.0
Accessing to social networking sites	284	13.5
Entertainment	229	10.9
Listening to music	151	7.2
Taking pictures	149	7.1
Taking videos	88	4.2
Use as a clock	101	4.8
Use as an alarm clock	131	6.2
Sending and receiving emails	201	9.5
Other	06	0.3
Total		100.0

***Multiple answers were permitted**

It is found from Table- 7 that the students had been using their smartphones to conduct a range of activities by using diverse features in it. The majority number of students were using their smartphones for communicating with their family, friends and teachers (291, 13.8%); accessing social networking sites (284, 13.5%); and for academic purposes (264, 12.5%). The subsequent three major groups were almost similar in size who had been using their phones for entertainment (229, 10.9%), browsing online (210, 10%) and sending and receiving emails (201, 9.5%) respectively. The following two groups also possessed almost similar number of percentages who were using their smartphones for listening to music (151, 7.2%) and taking pictures (149, 7.1%) consequently. A significant number of students (131, 6.2%) used the smartphones as an alarm clock. 101 (4.8%) students used their smartphones as a clock and and 88 (4.2%) students for taking videos accordingly. Other uses of smartphone (6, 0.3%) included playing games, watching news, learning new things, knowing word meanings and so on.

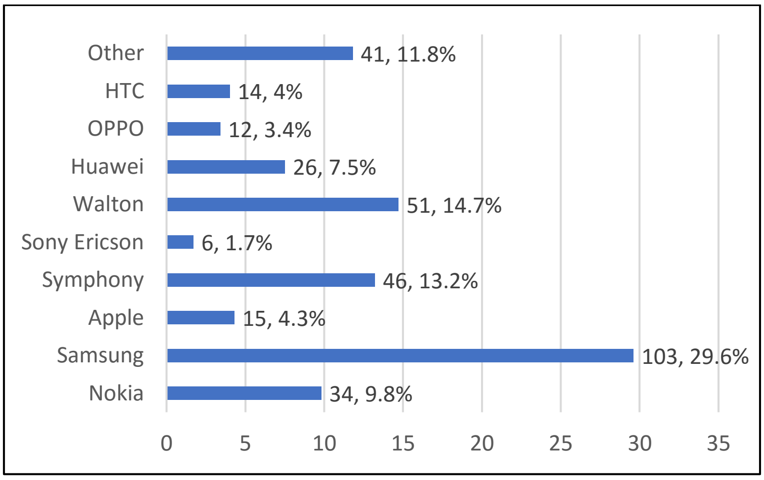

Figure 3. *University of Dhaka: participating students (n=348), by brand of smartphones used*

In Bangladesh, a range of smartphone brands are available in the market including foreign and local brands. Some local brands of smartphones offer very cheap rate phone ranging from BDT 3,700 - 4,000 (approximately GBP 37 - 40.0) but they provide the same features and functionalities for the users like any other brands. Figure-3 indicated that the largest group (103, 29.6%) of students of Dhaka University preferred to use Samsung mobile phone. The next two largest groups used Walton (51, 14.7%) and Symphony (46, 13.2%) was followed by those who used Nokia (34, 9.4%) and Huawei (26, 7.5%). Only a few (15, 4.3%) students used Apple, as they are more expensive than the other brands. Other mobile brands like LG, Xiaomi and ASUS were use by 41 (11.8%) students where some of them used more than one brands at the same time.

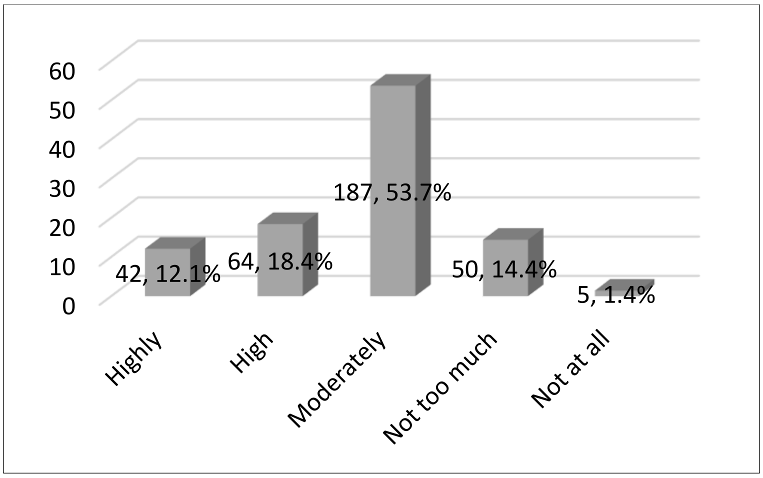

Figure 4. *University of Dhaka: participating students (n=348), by perception on safety issues*

Students were asked about how ‘safe’ do they feel when they use smartphones. Figure- 4 shows that the highest percentage of students (187, 53.7%) answered ‘Moderately’ which was followed by ‘High’ (64, 18.4%). On the other hand, 50 (14.4%) students felt ‘Not too much’ safe and 42 (12.1%) students felt ‘Highly’ secured in the use of smartphones. These overall feelings on security issues revealed that the majority of the students either felt moderately secure in regard to use of smartphones.

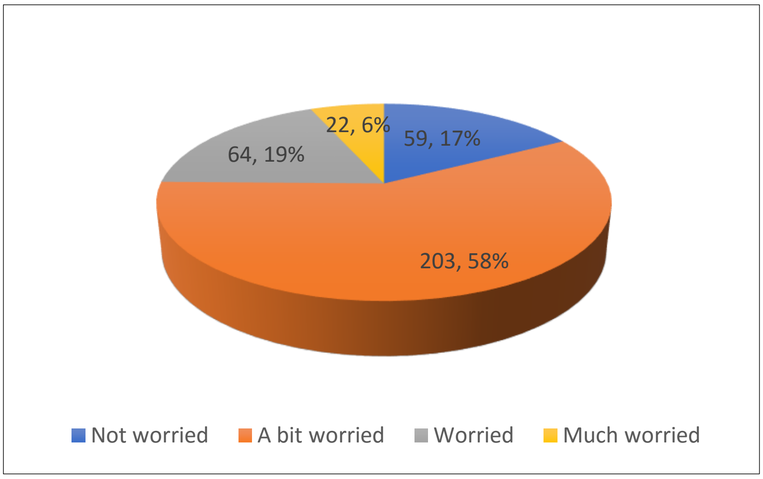

Figure 5. *University of Dhaka: participating students (n=348), by level of concern on smartphone security*

Figure- 5 represents that the highest number of students (203, 58%) were a bit worried about the smartphone security issues. Among the participants, 64 (19%) students said that they were worried about this issue. On the other hand, 59 (17%) students answered that they were not worried about the smartphone security practices. A lowest number of participants (22, 6%) said that they were much worried about the security issues of their smartphone.

Table 8. *University of Dhaka: participating students (n=348), by knowledge about risks and technical characteristics associated with smartphone*

	Knowledge about issues and risks associated with the smartphone		**Knowledge about options and technical characteristics associated with smartphone**	
	N	**%**	**N**	**%**
None	21	6.0	17	4.9
Insufficient	108	31.0	131	37.6
Sufficient	136	39.1	104	29.9
Good	71	20.4	80	23.0
Excellent	12	3.4	16	4.6
Total	348	100.0	348	100.0

Students were asked how they assess their level of knowledge about the issues and risks associated with smartphone, as well as knowledge about the options and technical characteristics of smartphones that affect the security. It is observed from Table-8 that the largest number (136, 39.1%) of students considered their knowledge as sufficient regarding the issues and risks associated with smartphone. The second largest group of students (108, 31.0%) believed that their level of knowledge was insufficient. Only 71 (20.4%) students considered that their level of knowledge was good and 12 (3.4%) students felt as excellent accordingly about the issues and risks associated with the use of smartphones where 21 (6%) students did not convey their opinion on the given issue. As the largest number of students felt that they have sufficient knowledge on issues and risks associated with smartphones, it might seem that they were much confident about the fact.

On the other hand, in the case of knowledge about options and technical characteristics of smartphone, 131 (37.6%) of the students felt that they had insufficient knowledge in those matters. At the same time, 104 (29.9%) of the students found their knowledge as sufficient about the topics; which was followed by 80 (23%) of students, who believed that their level of knowledge was good. The lowest number of students (16, 4.6%) found their level of knowledge as excellent. Notably, 17 (4.9%) students did not give any opinion on these matters.

Table 9. *University of Dhaka: participating students (n=348), by knowledge about OS and IMEI*

Knowledge about OS and IMEI	Yes	%	No	%	Unanswered	%	Total	%
Awareness about modern Operating System (OS)	223	64.1	119	34.2	6	1.7	348	100.0
Knowledge about IMEI	231	66.4	117	33.6	-	-	348	100.0

Modern Operation System (OS) and International Mobile Equipment Identity (IMEI) are two of the very important features of the smartphone. Interestingly, it was observed from Table-9 that most of the students were aware about modern OS (223, 64.1%) and IMEI (231, 66.4%), where 119 (34.2%) students were unaware about OS and 117 (33.6%) students were not aware about IMEI. Meanwhile, unlike IMEI question where all of the students answered that question successfully; in terms of OS, a very small number (6, 1.7%) of students were found unanswered to that particular question.

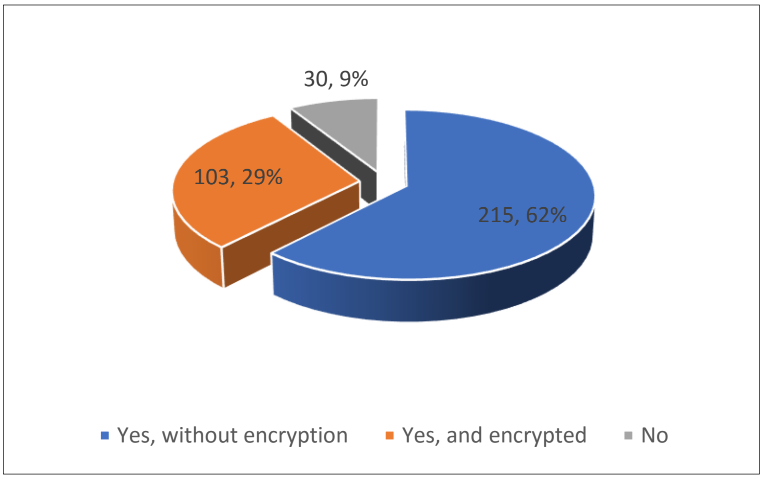

Figure 6. *University of Dhaka: participating students (n=348), by storing personal information in the smartphone*

Students usually store their personal sensitive information in their mobile phones. In answering the question of whether students store personal information in their mobile, it was found from Figure-6 that almost two third students stored personal information without encryption (215, 62%). It was really alarming that a huge number of students stored their personal information without any encryption which might lead disclosure of personal information to the unauthorized persons. 103 (29%) students stored their personal information with encryption and only 30 (9%) students said that they did not stored their personal information on their smartphone.

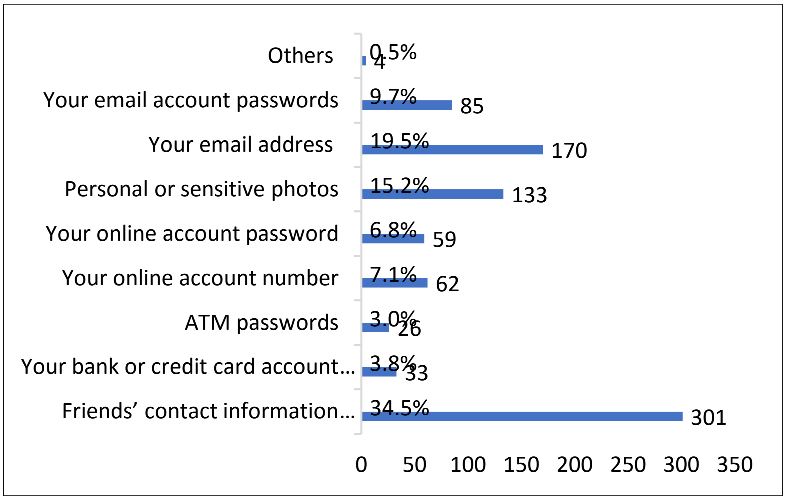

Figure 7. *University of Dhaka: participating students (n=348), by kinds or types of personal information those are storing in their mobile devices*

**** Multiple answers were permitted***

In modern days, the smartphones provide diverse facilities of storing information and the reasonable amount of spaces for storing information also encourage the users to store various personal information. The tendency of storing personal information is common among the students of University of Dhaka, Bangladesh. In terms of storing personal information in the smartphone Figure-7 shows that, the largest number of students (301, 34.5%) stored contact information. A significant number of students also stored their email addresses (170, 19.5%) and personal or sensitive photos (133, 15.2%) in their smartphone respectively. The percentages of storing other types of personal information were comparatively minimum among the students. Other types of personal information stored in the smartphones were email account password (85, 9.7%), online account number (62, 7.1%), online account password (59, 6.8%), bank or credit card account passwords (33, 3.8%), ATM passwords (26, 3.0%) and others (04, 0.5%).

Table 10. *University of Dhaka: participating students (n=348), by smartphone security risks faced*

Smartphone security risks	Frequency*	Percent
Unintentional disclosure of data	165	21.8
Data leakage resulting from device loss or theft	151	19.9
Financial malware attacks	65	8.6
Attacks on decommissioned smartphones	47	6.2
Network spoofing attacks	72	9.5
Surveillance attacks	40	5.3
Phishing attacks	54	7.1
Spyware attacks	71	9.4
Diallerware attacks	17	2.2
Network congestion	71	9.4
Other	05	0.7
Total		100.0

Multiple answers were permitted

It is quite common that most of the smartphone users have experienced some level of security risks in their life of smartphone use. Table- 10 shows the result of security risks aware of, or faced by the students. Among the participants, the biggest number of students faced the problem of unintentional disclosure of data (165, 21.8%) and data leakage caused by device theft or loss (151, 19.9%) where 72 (9.5%) students experienced the network spoofing attacks. Interestingly, a similar number (71, 9.4%) of security breaches was faced by the students through spyware attacks and network congestion. Other security risks those were experienced by the students were financial malware attacks (65, 8.6%), phishing attacks (54, 7.1%), attacks on decommissioned smartphones (47, 6.2%), surveillance attacks (40, 5.3%), diallerware attacks (17, 2.2%) and others (5, 0.7%).

Table 11. *University of Dhaka: participating students (n=348), by approaches towards avoidance of harmful behaviours*

Approaches in terms of avoidance of harmful behaviours	Always	Sometimes	Never
Switch off all data connections (e.g. by flight-mode)	(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%
Logging out of applications	(119) 34.2%	(160) 46.0%	(69) 19.8%
Configure automatic locking	(168) 48.3%	(114) 32.7%	(66) 19.0%
Avoid using smartphone location services	(101) 29.0%	(182) 52.3%	(65) 18.7%
Avoid connecting to public Wi-Fi networks	(99) 28.4%	(185) 53.2%	(64) 18.4%
Updates to smartphone systems and applications	(220) 63.2%	(104) 29.9%	(24) 6.9%
Protect from theft (e.g. by securely storing the device)	(174) 50.0%	(122) 35.1%	(52) 14.9%
Block one's identity (e.g. fake user profiles)	(182) 52.3%	(123) 35.3%	(43) 12.4%
Use messaging apps with end-to-end encryption	(100) 28.7%	(177) 50.9%	(71) 20.4%
Avoid financial apps/ functions (e.g. online banking)	(198) 56.9%	(104) 29.9%	(46) 13.2%
Use remote management apps	(55) 15.8%	(165) 47.4%	(128) 36.8%

Table- 11 demonstrates the approaches of the students of University of Dhaka, Bangladesh in regard to avoidance of harmful behaviours in the use of smartphones. Users' approaches have a great impact towards consequences in relation to information security risks in the smartphone use. In most cases, the users are given with the authority to control their security risks. Several factors like having active internet connections, taking necessary measures in dealing with third party applications, update smartphone systems and applications, automatic locking mechanism, avoid using location service, avoid accessing to public Wi-Fi, taking precautions against theft, blocking fake identity and avoiding financial activities may lead to reduce security risks. However, the survey findings on students' attitudes towards these factors are presented in the Table- 11 accordingly.

Switching off all data connection is a better technique of getting disconnected from the internet. Following this technique, the users may restrict the unauthorized access to their smartphone device. Table- 11 shows that the 220 (63.20%) students switched off all data connections as sometimes in reducing the security risks where only 74 (21.3%) students did that all the time and the 54 (15.5%) students never did it. It is alarming that only a smaller number of students were exercising this options in practice all the time but the largest number of students were still considering the technique as sometimes option.

Access authorization or checking permission to applications is another important issue in controlling the smartphone information securities. It is important to check the request permission before give the access control to mobile device because third-party applications can easily access the personal and sensitive information of the smartphone (Das and Khan, 2016). A very positive sign is that (See Table-11) the largest number (194, 55.7%) of students had always checked the permission before authorizing any third-party applications. There were 99 (28.4%) of the students who had been checking permission as sometimes and 55 (15.8%) of the students had never exercised that before going for downloading and installing any applications.

Installing unknown applications may cause serious security risk because of malware and other contraventions (Jones and Chin, 2015). So, it is important to install apps from trusted sources. It was observed from the study that 199 (57.2%) students had always avoided downloading application from unknown sources. However, 93 (26.7%) and 56 (16.1%) of students followed that security practice either in sometimes or never accordingly. It sounds quite good that the highest number of students followed appropriate security behaviour while dealing with installing apps to their smartphone.

The students use their smartphones for a number of purposes. Visiting social networking sites like Facebook, Twitter etc. and checking email are two of those. It is time consuming to log in to these applications each and every time before accessing and the students tend to keep logged in always automatically to save the time. This tendency of the students may lead to unauthorized access to the personal information. The analysis of collected data from Table-11 shows that only 119 (34.2%) of students always tried to log out from those applications while 160 (46.0%) of students had been following that security practice sometimes. 69 (19.8%) students never logged out from the applications which might become the reason of serious security breaches.

Nowadays most of the smartphones provide facilities of automatic screen locking but it normally requires first time manual activation beforehand. It generally gets activated automatically after certain time and cannot be accessed to the device without giving authentic authorization code. Automatic locking can prevent unauthorized access to the smartphones. However, in the survey result it was found that the majority number of students (168, 48.3%) always kept automatic screen lock system configured. Meanwhile, there were 114 (32.7%) and 66 (19.0%) of students who either sometimes or never configured the automatic screen locking feature respectively.

Location service is another recent feature provided by the smartphone and makes it possible to locate a person easily if he/she turn on this features in their mobile device. Generally, this feature requires internet connections but the mobile network may also determine the location of an individual. This feature may lead to serious security problems if the facility of this feature is used by unwanted or unauthorized person. Table-11 shows that 182 (52.3%) students had avoided using this feature in sometimes and 65 (18.7%) students never avoided utilizing the location service where only 101 (29.0%) students had always avoided using the feature.

In order to avoid network attack, it is recommended to avoid public Wi-Fi network (Kraus et. al., 2016). Moreover, the invader can easily steal personal information as those become available in the public network. According to Park et al. (2014), unsecured Wi-Fi connections may cause eavesdropped and sniffed of the sensitive information along with personal activities of the users. Table-11 reveals that only 99 (28.4%) students always avoided connecting to public Wi-Fi networks where the percentage of students who had avoided connecting public Wi-Fi as sometimes were 185 (53.2%) and the number of students who never avoided public network were 64 (18.4%).

The smartphone operating system and the mobile applications providers frequently recommend the users to keep up with the updates by installing required features (Jeon et al., 2011). These updates are important for the users in covering up existing vulnerabilities of the respective systems or applications (Harris and Patten, 2014). In order to ensure information security, keeping up to date with concerned operating systems and applications has got very critical roles to play. Remarkably, this study revealed that 220 (63.2%) of students had always kept updated with the latest version of operating systems and applications where only 24 (6.9%) students never did that and 104 (29.9%) of respondents had been checking the updates sometimes only.

Furthermore, in order to avoid harmful behaviour, the largest groups of students for other security practices like protecting the devices from the theft (174, 50.0%), blocking fake users profile (182, 52.3%), being alert while conducting financial activities (198, 56.9%) were found to follow those as always. On the other hand, the following biggest groups of students who considered those security factors only 'sometimes' were consist of 122 (35.1%), 123 (35.3%) and 104 (29.9%) of the students accordingly. There were 52 (14.9%), 43 (12.4%) and 46 (13.2%) of students who had 'never' taken into account of those factors at all.

On the other hand, only 100 (28.7%) and 55 (15.8%) of students 'always' consider the security factors of messaging apps with end-to-end encryption and using remote management apps respectively. The highest numbers (177, 50.9% and 165, 47.4%) of students had been considering those respective factors only 'sometimes' and 71 (20.4%) and 128 (36.8%) of the students 'never' took into account of those factors.

Table 12. *University of Dhaka: participating students (n=348), by approaches towards adopting useful phone settings and add-on utilities*

Approaches in terms of adopting useful phone settings and add-on utilities	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%
Disable Wi-Fi connection	(92) 26.4%	(179) 51.4%	(77) 22.1%
Disable Bluetooth	(171) 49.2%	(101) 29.0%	(76) 21.8%
Disable GPS	(114) 32.8%	(139) 39.9%	(95) 27.3%
Modify privacy settings of the device	(152) 43.7%	(127) 36.5%	(69) 19.8%
Avoid rooting the device	(150) 43.1%	(147) 42.2%	(51) 14.7%
Use data/ device encryption	(113) 32.5%	(134) 38.5%	(101) 29.0%
Use apps for privacy protection/ permission management	(131) 37.6%	(117) 33.6%	(100) 28.7%
Reduce online "data traces"	(71) 20.4%	(168) 48.3%	(109) 31.3%

In ensuring smartphone information security, the phone settings and add-on utilities may provide an additional layer of defense. The add-on utilities and phone settings mainly incorporate security software and applications like the SPAM filtering applications and the anti-virus software. The add-on utilities and phone settings are crucial in protecting the users against the threats of non-sophisticated attackers (Mylonas et al., 2013 a). Table- 12 describes the summary of approaches of the students of University of Dhaka, Bangladesh in utilizing the useful phone settings and ad-on utilities.

Deploying update is an important feature in this current time and most of the operating systems and mobile applications offer the facilities of updating their software through using of internet. This feature makes it convenient to cope up with updated version of the relevant systems and software. In terms of deploying update, Table- 12 exhibits that the largest group of students (150, 43.1%) had been utilizing this security feature in 'sometimes' which was followed by the frequency of 'always' (124, 35.6%) and the smallest group (74, 21.3%) of students 'never' used this feature. Therefore, the security behaviours of the students in using this feature appeared to be positive.

Meanwhile, in the case of installing antivirus software, 157 (45.1%) of students always installed antivirus software in their mobile device. There were 92 (26.4%) students who carried out this job sometimes. Accordingly, 99 (28.4%) students never installed any antivirus software in their mobile device which seemed really a very concerning issue with respect to the security against viruses and malware.

Smartphones provide the facility of connecting Wi-Fi networks. The security level of public Wi-Fi connection is not always same (Imgraben et al., 2014). Unsecured Wi-Fi connection may cause the disclosure of personal information to the third party (Park et al., 2014). The study showed an alarming picture that only 92 (26.4%) students disabled their Wi-Fi connections always. Moreover, 77 (22.1%) students never disabled Wi-Fi connection at all and 179 (51.4%) students had been disabling such connection only sometimes. Those numbers of percentages revealed that it might be important to make awareness among the students in that security issue.

Bluetooth and GPS are two of the most significant features of smartphones. Enabling Bluetooth discoverable may lead to connection of unauthorized device which may cause serious security breaches. On the other hand, enabling GPS provides the facility of tracking users' location from anywhere which may cause security breaches to users (ENISA, 2010). The study showed that a large proportion of students (171, 49.2%) had always disabled the Bluetooth in their smartphone. There were 101 (29.0%) of students who only sometimes disabled it and 76 (21.8%) students never disabled the Bluetooth options in their device. In the case of GPS, Table- 12 showed that only a limited number of students (114, 32.8%) always disabled the

GPS. There were 139 (39.9%) and 95 (27.3%) of students who sometimes and never disabled the GPS in their device accordingly.

Customizing or modifying the privacy setting of the smartphone becomes a necessity at present days. A number of privacy settings options are available in the smartphone but the users do not give time or attention for modifying privacy settings. As a result, they face the problem of security risks. It was found from Table- 12 that 152 (43.7%) students of the University of Dhaka always modified the privacy settings in their smartphone. There were 127 (36.5%) of them who put concentration on privacy settings in sometimes where 69 (19.8%) of them never followed this settings options.

Rooting the device is a process that allows users to access to the operating system code which gives the facility of changing the software code for installing those software which are not allowed by the manufacturer. But this feature leads to a huge security risk for the smartphone users like malware attacks, spyware, viruses etc. The analysis of collected data showed that the highest number of students (150, 43.1%) always avoided rooting their devices which was very positive sign in regard to security aspects. On the other hand, it was found that 147 (42.2%) and 51 (14.7%) of students either sometimes or never avoided this feature in their device.

An encrypted device is very secured compared to an unencrypted device. In the case of using device encryption, it was found that 113 (32.5%) students always encrypted their smartphone devices and 134 (38.5%) of them sometimes encrypted their data or devices. There were 101 (29.0%) students who never encrypted their devices for which the likeliness of causing security risks seemed high. On the other hand, in the case of using privacy protection apps, a large number (131, 37.6%) of students were using privacy management apps as always but in the aspect of reducing online data traces, it was found that lowest number (71, 20.4%) of students always tried to reduce online data traces from their smartphone devices. There were 117, (33.6%) and 168 (48.3%) of students who sometimes used privacy management apps and tried to reduce online data traces. On the other hand, 100 (28.7%) and 109 (31.3%) of students never followed these security features at all.

Table 13. *University of Dhaka: participating students (n=348), by approaches for disaster recovery*

Approaches for disaster recovery	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%
Blocking the device after losing it	(114) 32.8%	(100) 28.7%	(134) 38.5%
Take out insurance	(44) 12.7%	(68) 19.5%	(236) 67.8%

Table- 13 represents the disaster recovery behaviours of the students of University of Dhaka in the use of smartphones. Data backup plays an important role in recovering the information when the devices get stolen, lost or failure (ENISA, 2010). The analysis of Table- 13 showed that 64 (8.4%) students never backed up their information in their device. It is positive sign that 199 (57.2%) students always backed up their data for disaster recovery and 85 (24.4%) of them followed this procedure in sometimes. However, not having the data recovery plan in place might lead to a serious crisis once the students lose their important information.

Smartphone users store a large amount of personal information in the devices. Simply deleting the data may not be enough for protecting personal information from unauthorized access. In that case, data wipe out is an important feature for permanently deleting the unwanted data. Table- 13 showed that only 51 (14.7%) students wiped out their data from the device as always. There were 142 (40.8%) and 155 (44.5%) of students who sometimes or never wiped out their confidential information from their smartphone.

Blocking the device after losing the smartphone is very important because it will prevent the device from unauthorized access to the phone. Accordingly, taking out insurance policy is important in recovering the lost, stolen or damaged device from the insurer. In this research, the recorded responses of the students on these two factors were alarming because a large group of students never carried out the actions of blocking the devices (134, 38.5%) and taking out insurance after losing it (236, 67.8%) respectively. Only 114 (32.8%) and 44 (12.7%) of students were found in performing these actions as always where 100 (28.7%) and 68 (19.5%) of respondents sometimes carried those out respectively.

Comparison of student's information security behaviours

It was observed that in using smartphones, the information security behaviours differ among the users as different people poses different behaviour in the real life. In this study, the student's attitudes or behaviours in terms of avoiding harmful behaviours, useful phone settings or add-on utilities and disaster recovery were analyzed with an aim to determine the significant differences, if there were any, between users' characteristics and their information security behaviours from the perspective of *Faculties/institutions* and *Gender* identity. In determining the difference between these two variables, the Pearson's Chi-Square test of Independence was deployed.

Note: In the case of Faculties/Institutions, it was found from the findings that the highest responses were received from the faculty of Arts, Social Sciences, Business Studies, Pharmacy and Biological Sciences. Due to this reason, the Researcher made the comparison of students' information security behaviours among these Faculties/Institutions only.

Table 14. *University of Dhaka: 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*
Logging out of applications	.668	2	.716	53.455	28	.003*
Configure automatic locking	6.209	2	.045*	55.591	28	.001*
Avoid using smartphone location services	1.246	2	.536	52.903	28	.003*
Avoid connecting to public Wi-Fi networks	.649	2	.723	45.846	28	.018*
Updates to smartphone systems and applications	2.134	2	.344	49.412	28	.008*
Protect from theft (e.g. by securely storing the device)	4.812	2	.090	70.173	28	.000*
Block one's identity (e.g. fake user profiles)	5.367	2	.068	63.629	28	.000*
Use messaging apps with end-to-end encryption	.179	2	.914	47.497	28	.012*
Avoid financial apps/ functions (e.g. online banking)	6.008	2	.050	50.849	28	.005*
Use remote management apps	7.367	2	.025*	47.891	28	.011*

The Pearson's Chi-Square test of independence was used to find out the differences between students' information security behaviours by Gender and Faculties/Institutions in terms of avoiding harmful behaviours. The results of Chi-Square test comparing the student's attitudes or behaviours by Gender suggested that there were significant differences in two out of thirteen cases (See Table- 14). 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.

The frequency table indicated that the percentages of 'Always' (49.2%) and 'Never' (21.5%) in configuring automatic locking of male students were much higher than those of female (46.1% and 12.7%) students. But in the case of 'Sometimes', the female students (41.2%) were found preferring to configure automatic locking more than male (29.3%) students. On the other hand, the largest number of male students (18.3%) had 'Always' used remote management apps as compared to female students (9.8%). But the percentages of 'Sometimes' in using remote management apps of female students (57.8%) was higher compared to male students (43.1%). However, the percentages of 'never' in the use of remote management apps for the male (38.6%) and female (32.4%) students were also alarming. Overall, it might be observed that in terms of 'configuring automatic locking' the aggregate percentage of 'always' and 'sometimes' for the female students was higher compared to male students. Accordingly, the level of awareness for 'Use remote management apps' seemed almost same for male and female students *(See Appendix-D: Table-1).*

On other hand, student's attitudes or behaviours 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 (checking permission/Accessing authorization to applications) was greater than the significance level of 0.05. So, the null hypothesis was rejected in rest of the twelve cases and a conclusion was made that there was significant difference in terms all those twelve cases by Faculties/Institutions. Notably, only a group of selected features which were considered as more important for smartphone security were included in the comparative discussion.

It was revealed from the Chi-square test that the highest percentage of 'sometimes' was common for all Faculties in 'switching off data connections' feature among which the response percentage for the Faculty of Social Sciences (73.7%) was the highest. That was followed by the ‘always’ option apart from the Faculty of Business Studies (27.1%) and the Faculty of Pharmacy (19.4%) where in those two faculties the ‘never’ option had got the higher percentage. So, in terms of ‘switching off all data connections’, the Faculty of Arts students were more concerned than other Faculties and the Faculty of Business students were least concerned in using the feature.

In terms of ‘avoiding downloading apps from unknown sources’ it was observed that the largest number of students from all the Faculties utilize that feature as ‘always’ and, at the same time, the minimum number of students were found in utilizing it as ‘never’. Among those Faculties, the highest number (63.6%) of students from the Faculty of Arts marked for ‘always’ and the lowest number (3.4%) of students from the Faculty of Biological Science chose the ‘never’ option. In the Faculty of Business Studies, the percentage for ‘never’ (20.0%) was higher than other Faculties. Therefore, it might be said that the students of the Faculty of Arts and the Faculty of Biological Sciences were more aware compared to other Faculties and the Faculty of Business Studies students had got the minimum level of awareness in using those features.

In the case of ‘logging out of applications’, the largest group of students who belonged to the Faculty of Pharmacy, only utilized the feature as ‘always’ (41.7%) on their own and the biggest group of students (41.4%) from the Faculty of Arts had responded with ‘always’ and ‘sometimes’ jointly. After analyzing the chi-squire table, it was found that though the Faculty of Biological Sciences had got the minimum percentage of ‘never’ (6.9%) responses but the combined response rate for ‘always’ (41.4%) and ‘sometimes’ (41.4%) percentages for the Faculty of Arts was much higher than the other Faculties. Therefore, the students of the Faculty of Arts appeared to be more concerned than others.

The highest number of students from all Faculties had ‘always’ utilized the feature of ‘updates to smartphone systems and applications’. This was followed by the ‘sometimes’ response from the students of various Faculties. Remarkably, the ‘never’ option was selected by a very small percentage of students in all the Faculties. So, the students appeared to be concerned in using that feature and the students of the Faculty of Arts might be considered as moderate to good in using that specific feature because the combined percentage of ‘always’ (71.4%) and ‘sometimes’ (23.6%) response for that faculty was higher than other Faculties *(See Appendix-D: Table-2).*

Table 15. *University of Dhaka: 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*
Disable Wi-Fi connection	1.403	2	.496	62.855	28	.000*
Disable Bluetooth	.242	2	.886	58.614	28	.001*
Disable GPS	.011	2	.995	57.703	28	.001*
Modify privacy settings of the device	.474	2	.789	45.851	28	.018*
Avoid root the device	5.504	2	.064	43.069	28	.034*
Use data/ device encryption	1.309	2	.520	47.419	28	.012*
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- 15 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' attitudes or behaviours by Gender suggested that there was significant difference between Gender and in reducing online data traces ($p<.002$). It was found from the of chi-square test that in terms of 'reducing online data traces' the percentages of 'Sometimes' (52.0%) and 'Never' (32.5%) of male students were much higher than the female students. In contrary, the percentage of the female students (32.4%) for 'always' was higher than male students (15.4%). It meant that in 'reducing online data traces', female students were much concerned than male students *(See Appendix-D: Table-3).*

Moreover, comparing students' information security behaviours by Faculties/Institutions in terms of useful phone settings or add-on utilities, suggested that there were significant differences in all the cases excepts in 'reducing online data trace', since the *p*-value ($p > .094$) of that item (reducing online data trace) was greater than the significance level of 0.05. So, the null hypothesis was rejected in rest of the nine cases and a conclusion was made that there was significant difference in terms all those nine cases by Faculties/Institutions. Notably, only a group of selected features which were considered as more important for smartphone security were included in the comparative discussion.

It was appeared that for the feature of ‘Deploy updates’, the biggest group of students selected the ‘sometimes’ option and the second largest group of students chose the ‘always’ option by all the Faculties/Institutions accordingly. It was shown that the Faculty of Business Studies (35.7%) received the ‘always’ responses from the largest group of students along with the Faculty of Arts (35.7%) where the Faculty of Social Sciences (31.6%) students represented the second largest percentage. Meanwhile, in terms of ‘never’ option both the Faculty of Social Sciences (13.2%) and the Business Studies (18.6%) occupied the bottom two positions accordingly. So, it might be observed that students of the Faculty of Business Studies and the Social Sciences were more concerned in deploying updates compare to other faculties.

In the case of ‘Installation of anti-virus software or application’ feature, the percentage of ‘always’ for the faculty of Arts (57.9%) was higher and the faculty of Social Sciences (26.3%) was lower among all the Faculties/Institutions. On the other hand, the percentage of ‘never’ for the Faculty of Social Sciences (52.6%) came from the largest group and for the faculty of Arts (20.0%) from the smallest group of students among all Faculties/Institutions. Therefore, it was observable that the overall security behaviours in terms of ‘installation of anti-virus software or application’, the faculty of Social Sciences was less aware than the Faculty of Arts.

In terms of ‘Disable Bluetooth’ feature, the students of the Faculty of Biological Sciences seemed to be more aware compared to other Faculties/Institutions as the percentage of ‘never’ (6.9%) response represented the smallest group and the ‘always’ (62.1%) response came from the biggest group of students among all Faculties/Institutions. On the other hand, the Faculty of Pharmacy had got the ‘always’ (33.3%) response from the smallest group and the second largest group of students responded with ‘never’ (27.8%) response. So, it might be observed that the students of the faculty of Biological Sciences were most aware and the faculty of Pharmacy students were least concerned in using this feature.

In respect of the feature of ‘Modify privacy settings of the device,’ the biggest group of students who belonged to the Faculty of Social Sciences (42.1%), the Faculty of Business Studies (54.3%) and the Faculty of Biological Sciences (65.5%) were found to use it as ‘always’. Besides, the ‘sometimes’ option were selected by largest group of students for the other two Faculties namely the Faculty of Arts (45.0%) and the Faculty of Pharmacy (50.0%). However, the security behaviours of the students of the Faculty of Biological Sciences might only be considered comparatively secured in terms of utilizing the privacy settings of the device among all Faculties/Institutions as their ‘always’ responses were higher and ‘never’ responses were lower than other Faculties *(See Appendix-D: Table-4).*

Table 16. *University of Dhaka: 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*
Blocking the device after losing it	.197	2	.906	48.179	28	.010*
Take out insurance	6.146	2	.046*	35.364	28	0.160

Table-16 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’. Since the *p*-value of all those two 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 in student’s attitudes or behaviours by Gender in terms of ‘data backup’ and ‘taking out insurance’.

It was found from the chi-square result that in the case of ‘data backup’, the percentage of ‘always’ for male (61.8%) represented larger group of students than female (46.1%) students. On the other hand, the percentages of ‘sometimes’ (33.3%) and ‘never’ (20.6%) for female came from the much larger group of students than male (the percentages of male and female were 20.7% and 17.5% respectively). However, it could be said from the chi-square test, that male students were comparatively more aware than female students in terms of utilizing ‘data backup’ 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 (Male 64.2% and Female 76.5%). So, both male and female students were found to be unaware in this regard *(See Appendix-D: Table-5).*

On the other hand, students' attitudes or behaviours by Faculties/Institutions in terms of disaster recovery suggested that there were significant differences in almost all the cases except in 'taking out insurance' ($p > 0.160$). So, the null hypothesis was rejected in rest of the three cases and a conclusion was made that there were significant differences in terms all those three cases of disaster recovery by Faculties/Institutions. Notably, only a group of selected features which were considered as more important for smartphone security were included in the comparative discussion.

In the use of 'data backup' option, the response rate for 'always' was found as highest in the Faculty of Business Studies (75.7%) and lowest in the Faculty of Social Sciences (18.4%). The response rate of 'never' option for those two faculties presented the opposite figures (14.3% and 42.1% accordingly). Therefore, it might be argued by analyzing the response rate that the Faculty of Business Studies students were much aware and the Faculty of Social Sciences students were the least concerned among all Faculties.

It was found that apart from the Faculty of Biological Sciences, in terms of 'data wiping out upon disposal' feature, the information security behaviours of the students for all other Faculties were in vulnerable condition because only for that particular Faculty, the response percentage for 'always' (41.4%) was recorded as highest. Though the largest group of students for rest of the Faculties either chose 'never' or 'sometimes' but the vulnerability to information security breaches was most apparent for the Faculty of Social Sciences where the 'always, response was recorded as zero.

In the case of 'Blocking the device after losing it', it was observed that the Faculty of Arts (32.9%) and the faculty of Biological Sciences (41.4%) utilized that feature both 'always' and 'never' by the same percentage of students and for rest of the Faculties the highest responses were received in 'never' by the majority of students. It was found from the chi-square test that the students from Faculty of Arts had possessed a secured behaviour in regard to that feature of security issue compare to Faculty of Social Sciences. Because 'never' response of Faculty of Social Sciences (50.0%) was higher than the Faculty of Arts (32.9%) and the 'always' response of Faculty of Social Sciences (15.8%) was much lower than Faculty of Arts (32.9%) *(See Appendix-D: Table-6).*

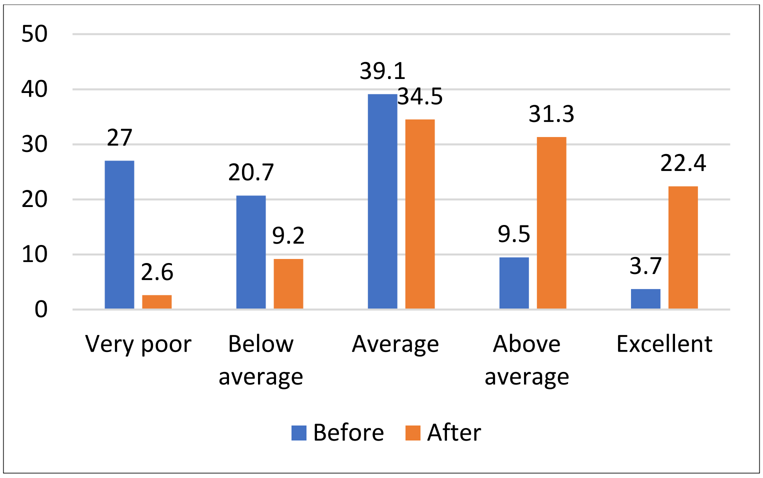

Figure 8. *University of Dhaka: participating students (n=348), by self-evaluation on the aspects of information security by the students*

In this research, the students were asked to present a self-evaluation of their knowledge on aspects those are related to information security. This assessment aimed to investigate their level of knowledge on various security issues both before and after conducting this survey. However, there were five degrees provided to express their level of knowledge ranging from one to five and those were demonstrating very poor, below average, average, above average and excellent accordingly. A very positive answer was found from the analysis of the collected data (See Figure- 8) where almost all the students said that their level of knowledge about smartphone security aspects had been increased or developed after participating to this survey. Most significantly, in the degree of 'Above average' and 'Excellent' level, the percentages were increased to a great extent (from 9.5% to 31.3% and from 3.7% to 22.4% respectively). On the other hand, the percentages of the students whose knowledge about these security issues were 'Very poor' (27.0%) and 'Below average' (20.7%) prior to participating to this survey were decreased to a significant extent (2.6% for 'very poor' and 9.2% for 'below average' accordingly) after conducting the survey. However, students' feedbacks demonstrated a positive sign because the level of understanding among the students were improved remarkably after taking part to this survey. The only exception was observed in the degree of 'Average' level where it was found that the level of knowledge among the students decreased (from 39.1% to 34.5%) in respect of their knowledge on security issues. Alternatively, it might be assumed that the percentages for the level of 'average' were affected due to the dramatic improvement of knowledge on security issues among the students and their increased diversion towards the level of 'Above average' and 'Excellent' consequently. Notably, the knowledge of 'Average' level among the students had always maintained the higher position both before and after participating to the survey.

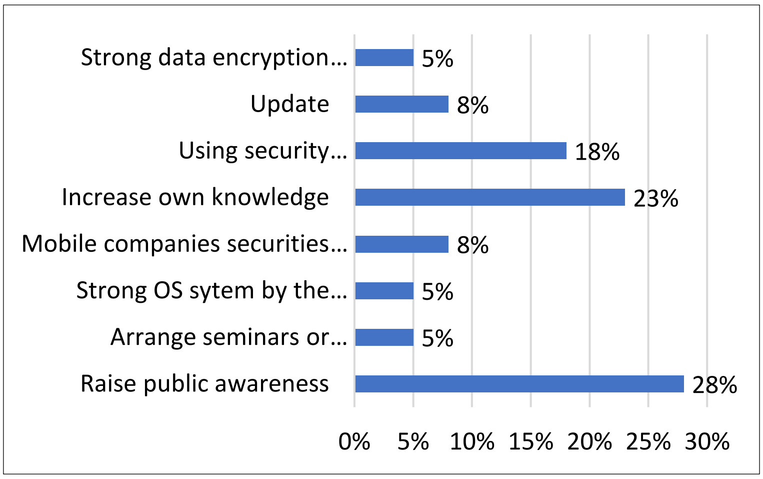

Figure 9. *University of Dhaka: participating students (n=348), by suggestions for improving the security measures in the use of smartphones*

Accordingly, the students were asked to provide their suggestion, if they had any, for improving the security measures in the use of smartphones. Figure- 9 presents the suggestions from the students for improving the security measures in the use of smartphones. Very small number of students responded to the question. The highest number of students (28%) suggested for raising public awareness and the following largest group of students (23%) suggested for the development of self-knowledge in the smartphone use. Accordingly, a significant percentage of students (18%) said that using security software or Antivirus might be focused as another important security measures in the use of smartphone. Moreover, similar number of students (8%) supported the view of developing 'mobile company's security measures' and 'update of systems and applications'. However, the same proportion of the respondents (5%) provided the suggestions for 'arranging seminars or programs', introduction of 'strong operating systems by the smartphone companies' and developing 'strong data encryption system'.

10. Discussions and Recommendations

10.1 Discussions

This study has been conducted to investigate the information security behaviour of the students of University of Dhaka, Bangladesh in the use of smartphone. The study shows that among the participants, the majority of students are male where the female participants represented only 29.5%. Furthermore, the majority of the participants belong to the age group of 18-24 who represents 83.7% of the total participants. Moreover, it is found that the 98.0% of the participants are pursuing either Bachelor or Master courses who basically belong to the age group of 18-24. In terms participating Faculties/Institutions, the highest participants came from the Faculty of Arts by representing 39.6% where the Faculty of Business Studies represents 19.7% as a second highest. Response rates from some of the participating Faculties are very low; therefore, the obtained data from those participants may not represent those respective Faculties/Institutions appropriately.

A total of 356 participants responded to the survey questionnaire; among them eight of the participants answered with not using the smartphones and they took off after completing demographic information section (Section- 1) and did not participate in the following stages of the survey. Therefore, the number of participants for the subsequent sections got reduced from 356 to 348. It is also revealed that all the participants who use smartphones, do also use internet (100%) in their mobile though their mode of internet connection is different. More than 80.0% of students, access to the internet several times a day through their smartphones. The study shows that over 35.0% of the students, access to the internet by using Wi-Fi connections and over 50.0% of them use both the Wi-Fi and Mobile Network connections. The findings indicate that the students mostly use their smartphones for range of activities, among which the major portion of students utilize it for communicating with friends, family and teachers; accessing to social networking sites; and entertainment. Notably 12.5% of students use their smartphones for academic purposes. The diverse usability of smartphones also facilitates the students for taking pictures and videos, use as a clock and alarm clock, listening to music, browsing online and many other activities. Furthermore, the research also reveals that majority of the students feel safe in using smartphones. As the students feel safe in using the smartphones, they are only a bit worried on the security issues associated with the use of smartphones. Such approaches of the students are concerning as the internet security is a great challenge in the modern world. The study found that the maximum number of students consider themselves as having at least sufficient knowledge about issues and risks related to the smartphone use. The findings also show that over 60 percent of students possess knowledge about modern operating systems and International Mobile Equipment Identity (IMEI). Furthermore, this study demonstrates that almost two third of the students store their information in the smartphone without encryption which include contact information, personal sensitive information, email addresses and so on. The findings of this study indicate that the students have experienced smartphone security risk in several ways among which unintentional disclosure of data and data leakage resulting from device loss or theft are two of the most frequent security risks faced by the students.

Information security behaviour in terms of avoiding harmful behaviours

The first objective (*RQ.1*) of this study is to investigate the approaches or behaviours of the students towards the features regarding avoidance of harmful behaviours in the use of smartphones. In that process, the students were provided with some security features to exhibit their approaches to it. The respective security features those were included to achieve this objective were the utilizing the flight mode options, configuring automatic locking, security measures when downloading applications from unknown sources, update smartphone systems and applications as well as safeguarding the smartphones from theft, using remote management applications, and so on. However, the findings of this survey present that in the issue of avoiding harmful behaviour, over half of the features were responded with positive responses by majority of students where they answered with 'always' to utilize these security features. Among these features, updates to smartphone systems and applications, avoid downloading apps from unknown sources and avoid financial apps and functions are the top three features which are utilized by most of the students (over 55.0%) as 'always'.

On the other hand, a significant number of students have responded to these features with 'sometimes' answer. The ratio of the students who answered 'sometimes' is similar to the students those responded with 'always'. The highest percentage of (63.2%) students were found to be utilizing the flight mode features as 'sometimes'. Avoid connecting to public Wi-Fi networks and avoid using smartphone location services are other two top features those are utilized by the students as 'sometimes'. However, utilizing these features only occasionally can also lead to the information security breach but it is, at least, obvious that the students are aware about these features. Although in terms of avoidance of harmful behaviour features the 'never' response remained to minimum number of percentages but these numbers cannot be ignored in any means; because the students who responded in the 'never' option are not aware about these features at all which may result in serious security breaches for them.

It is apparent that the approaches of the students towards avoidance of harmful behaviours are moderately satisfactory as over three quarter of the students utilize the provided security features in some way. Unlike other studies conducted by different authors (Esmaeili, 2014; Imgraben, 2014) the overall security knowledge of the students in this aspect is quite moderate. Nonetheless, huge improvement is required to upgrade the 'sometimes' and 'never' responses to the 'always' because that dark spot can spoil the whole security system of the network.

Information security behaviour in terms of useful phone settings and add-on utilities

The second objective (*RQ.2*) of this study is to find out the behaviours of the students in using phone settings and add-on utilities. Similar to the first objective, a list of relative features was presented before the students in order to collect their responses to understand their attitudes towards adopting useful phone settings and add-on utilities. It is revealed that about half of the features are utilized by the majority number of students in 'sometimes'. Among these features, maximum number (51.4%) of the students exercise disabling Wi-Fi connection feature. Other important features which are utilized by majority of the students occasionally, are deploying update, disabling GPS, reducing online data traces and using data or device encryption. Notably, the responses for 'root the device' feature (42.2%), the 'sometimes' option were very close to the 'always' option. Meanwhile, the features like 'disabling Bluetooth', 'installation of anti-virus software or application' and 'modify privacy settings of the device' are utilized 'always' by about half of the students. This is very concerning that features like 'disabling Wi-Fi connection' are used by very minimum number of students in 'always'.

Though the students do not utilize the security features accurately at all time but this is apparent that overall the students are not so vulnerable to information security breach in the use of smartphone in terms of useful phone settings and add-on utilities because they utilize most of the security features either 'always' or 'sometimes'. Therefore, a contrary result can be observed in this study compare to Das and Khan (2016) because the poor information security behaviours in the use of smartphone were presented in that study. However, majority of the features are utilized by the students only 'sometimes' and there is huge scope of developing this area for converting this into 'always'. Moreover, a significant number of students are left outside the use of these security features which is very concerning. However, similar to the previous outcome of the first objective of 'avoidance of harmful behaviour', it can be said that the students are moderately aware about the information security regarding the 'use of phone settings and add-on utilities' features.

Information security behaviour in terms of disaster recovery

Under third objective (*RQ.3*), the approaches of the students in disaster recovery presents very concerning results. It is found that over half of the students 'always' utilize data backup feature. Apart from this, in the case of all other disaster recovery features like blocking the device after losing it, 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 is very concerning in this regard because the importance of wiping out data before disposing or blocking the device after losing it play crucial role in securing information from the access of the third party. On the other hand, taking out insurance policy is crucial for device recovery. Therefore, in this particular area the students are very vulnerable to security risks.

Comparison of smartphone information security behaviour by Gender and Faculties/Institutions

In order to achieve the fourth research objective (*RQ.4*), a chi-square test was conducted by the Researcher to find out the differences between students' information security behaviours by Gender and Faculties/Institutions. During making comparison it is observed that in respect of 'Configuring automatic locking' female students are less vulnerable than male students. On the other hand, in case of 'Use remote management apps' the level of awareness are almost same for both male and female students. In the analysis of utilizing 'useful phone settings or add-on utilities' section, it is revealed that the female students are more aware compare to male students as their 'always' responses are better and the 'never' response is minimum than the male students in the case of 'reducing online data traces'. Under the section of 'disaster recovery' the male students are comparatively more concerned than female students in using 'Data backup'. On the other hand, in using the feature of 'Taking out insurance', both genders seem very vulnerable to security breaches because the 'never' option was selected by the maximum percentage of students from both gender between which the female students are more vulnerable than male students.

It is found from the Chi-square test, that the majority of features are significantly different with Faculties/Institutions. Among 24 Faculties/Institutions, students from 15 Faculties/Institutions participated in the survey. The highest response rate was from the faculty of Arts, Social Sciences, Business Studies, Biological Sciences and Pharmacy. For this reason, on making comparison among the Faculties/Institutions, the priorities were given to these

Faculties/Institutions. 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, mixed approaches or behaviours were found among the students of different Faculties/Institutions. None of the Faculty/ Institution possesses such behaviours or attitudes which are most secured towards all the features of smartphone information securities. A Faculty which seemed secured in using one feature are 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 compare to other Faculties/Institutions. On the other hand, in terms of 'Disabling Bluetooth' the Faculty of Biological Sciences students' are found most aware than others. Meanwhile, in using the features of 'disaster recovery' section, 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.

Suggestions for improving the security measures in smartphone

Individual behaviour towards information security practice in the use of smartphone is very crucial but information security behaviour is different for everyone. In this study, the attitudes of the students reveal that they have mixed attitudes towards information security issues in the use of smartphone. Besides, this study has significant impact in enhancing the awareness of the students regarding security issues. Analyzing the responses of the students when assessing their knowledge about information security behaviour in the use of smartphone, it is observed that it got improved in a large scale. Their response rate for 'very poor' and 'below average' got improved to 'above average' and 'excellent' after participating to this survey. The students also appreciated this survey because they became aware about a lot of issues of information security in the use of smartphone due to this study. However, finally it can be said that the students are remarkably benefited by participating to this survey.

Furthermore, the students made a number of suggestion for improving the security measures in the use of smartphones. In those suggestions, most of the students are found in believing that raising public awareness and increasing own-knowledge about security risk can minimize the smartphone security risks mostly. Undoubtedly, in this age of Information Communication Technology (ICT), there are huge scopes for self-education on information security, once the awareness is raised among the users. Another recommendation made by the large number of students were 'using security software or antiviruses. Apart from these three-major recommendations, the students also suggested for, adaptation of strong encryption system, smartphone security updates, mobile companies’ security measures, strong operating system by the smartphone manufacturers and arranging seminars or programs by the concerned authorities.

So, it can be said that unlike the research findings explored by the Jones and Heinrichs (2010), Esmaeili (2014), Imgraben (2014) and Das and Khan (2016), this study reveals that the students are not so vulnerable as it perceived from the survey result. It is apparent from the current study that the students of University of Dhaka are moderately aware about overall security concerns in the use of smartphones and they possess a moderate level of knowledge about security issues. This should also be noted that in the cases of some features, their attitude seemed vulnerable to security breaches. Many features are utilized by the students only sometimes which means that they remain vulnerable to security breaches in the other time. Under no circumstances those other times can be ignored in the assessment of vulnerability to information security risks. It is also proven from the survey result that their level of knowledge about smartphone security issues has been improved after conducting this survey. Besides, the improved knowledge of the students about information security issues has also become noticeable by the recommendations they made as they made some realistic suggestions for the improvement of the overall information security in the use of smartphones. However, still there are a lot of scopes for improvement of the security behaviours of the students which can be identified in more detail by conducting further study as well as doing a survey in a large scale.

10.2 Recommendations

Based on the data analysis and findings of the study, a detailed set of measures can be identified which may reduce the smartphone information security risks and help to maintain their security practices properly in the use of smartphone. The major recommendations are as follows:

i. It is important to configure the automatic locking system in the smartphone so that after a fixed time it locks automatically. Automatic locking system can be activated by using pin code or biometric information. It will help to reduce the unauthorized access to the devices by others.

ii. Before installing or downloading any applications in smartphone, it is recommended to check the reputation of the apps to make sure whether it is from trusted sources or not.

Downloading or installing apps from unknown sources may cause the security breaches to the users.

iii. Check access authorization or permission requirements of the application before installing the application in the smartphone. It will make the student aware about what types of personal information can be accessed by the application developers. Such knowledge will be helpful in choosing the secured application for the smartphones.

iv. Disable the location services of the smartphone when it is not necessary. Keeping the location services enabled may allow third party applications to determine the location and other confidential information stored in the smartphone devices.

v. Disable the Bluetooth and GPS of the smartphone in order to protect unauthorized access to the device. Such practice will prevent the invader from infringing information security.

vi. Be aware when using public Wi-Fi or unknown internet connection. Personal information can be acquired by unauthorized parties who are using the same network.

vii. In order to maintain the confidentiality of individual smartphone, use encrypted memory of smartphone and other detachable media of the device. It is also recommended to use encryption software for highly confidential messages and calls.

viii. Always try to configure the privacy and security settings in the smartphone device to protect unwanted disclosure of data. Configuring privacy and security settings enables the students to make the device highly secured through customization.

ix. Install proper antivirus software or firewall protection to make the smartphone free from viruses, malware or spyware. Latest antivirus will protect from the security attacks made through latest malware, spyware and viruses.

x. Deploy better data backup plan for protecting the personal data or information from unwanted theft or loss of smartphone. Data backup can be ensured by using the cloud services, email storage or personal computers through usage of drop box or other information sharing applications.

xi. 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 or links.

xii. It is not advisable by the manufacturer or the producer of the smartphone device to jailbreak or root the device. Avoiding root the device will protect the users against downloading unauthorized applications as well as the possible damages cause by those.

xiii. It is important to perform regular software and system updates in the smartphone so that new features of information security can be available in the device. Failure to keep the device updated may cause the attack made by the most recent spyware or malware.

xiv. It is recommended to wipe out all settings and data before going for mobile disposing or recycling or in case of stolen or lost mobile. The device information as well as personal setting can be disclosed by failure to conclude data wipe out.

xv. Do not store any personal or confidential information like passwords, ATM passwords, online account number or passwords, email address or passwords, personal or sensitive photos etc. in the mobile.

xvi. Users are not aware about the smartphone information security risks. A number of wrong concepts are available among the users of smartphone in regard to security aspects. For this reason, it is important to make the users aware about information security. Educating the users by organizing seminars, workshops, or train the users about handling confidential information, make them aware through different medias may make it possible to minimize the problem of information security in the use of smartphone.

11. Conclusion

In this age of Information Communication Technology (ICT), smartphone becomes an integral part of our day to day life. We cannot think of a single day without using a smartphone. Young generation in today’s world are almost addicted to the use of smartphone. Smartphone features and functions are quite different from the traditional mobile phones. It provides a diverse range of new features and facilitates for the users. Although smartphone provides a range of new facilities for the users, at the same time the use of smartphone also increases the risk of information security breaches. Lack of awareness about the smartphone security issues may cause several types of security infringement like disclosure of personal information, unauthorized access to the information contained in the mobile by the third party, confidential information leak out and many more. Therefore, it is important to understand the information security behaviours in order to design the solutions and increase awareness among the users for minimizing the smartphone information security risks. According to Jones and Chin (2015), increased awareness on information security issues in the use of smartphones could make positive impact towards the smartphone information security attitudes of the users. In this way, the users may enjoy all the benefits safely and conveniently offered through smartphone. This research investigates the information security behaviour of students of University of Dhaka, Bangladesh in the use of smartphone. Quantitative data were collected to understand the information security behaviours of the students. The findings of the study reveal that students of University of Dhaka possess a moderately secured 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 according to Gender and Faculties/Institutions.

It is found from the study that in some cases the majority of students utilize the security protocols of certain features only ‘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. However, one positive aspect is that the level of knowledge about the smartphone security issues has been improved to a great extent among the students after participating to this research survey. Besides, further studies can be carried out with large sample size by including students from other universities of Bangladesh as well as other dimensions of the smartphone information security behaviours of the students can be explored thereby. The research 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 programs for the improvement of information security in the use of smartphones. Furthermore, it will help to build transparent security features for more secured and protected systems as well as effective user interface.

12. References

Agarwal, A. (2014). *Why Forms in Google Docs are Perfect for Creating Online Surveys.* (Online) Available at: https://www.labnol.org/software/google-docs-forms-for-surveys/10056/ (Accessed 8 August 2017)

Agarwal, R. & Anderson, C. L. (2010). Practising safe computing: a multimethod empirical examination of home computer user security behavioral intentions, *MIS Quarterly*, Vol. 34 No.3. pp. 613-643.

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.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, Vol. 22 No. 4, pp. 308-313.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, Vol 22 No.2, pp.171-192.

Androulidakis, L. & Kandus, G. (2011). Mobile Phone Security Awareness and Practices of Students in Budapest. *The Sixth International Conference on Digital Telecommunications*, pp. 18-24.

Ballagas, R., Borchers, J., Rohs, M., & Sheridan, J. G. (2006). The smart phone: A ubiquitous input device. *Pervasive Computing, IEEE*, Vol. 5 No.1, pp. 70-77.

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).

Banglapedia, National Encyclopedia of Bangladesh (2015). *Hartog, Sir Philip Joseph* (Online) Available at: http://en.banglapedia.org/index.php?title=Hartog,_Sir_Philip_Joseph (Accessed 22 July 2017)

Ben-Asher, N., Kirschnick, N. , Sieger, H., Meyer, J., Ben-Oved, A. & M¨oller, S. (2011). On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. ACM*, pp. 465–473.

Benton, K., Camp, L. J. & Garg, V. (2013). Studying the effectiveness of android application permissions requests. *Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE International Conference on. IEEE,* pp. 291–296.

Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F. & Savvides, M. (2015). Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. *Proc. USEC*, pp.1-2.

Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V., & Iftode, L. (2010). Rootkits on smart phones: Attacks, implications and opportunities. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, pp. 49-54.

Bird, D. K. (2009). The use of questionnaires for acquiring information on public perception of natural hazards and risk mitigation - a review of current knowledge and practice. *Natural Hazards & Earth System Sciences*, Vol.9 No.4, pp. 1307 –1325.

Bojmaeh, H. Y. (2015). The Main Factors Influencing Information Security Behavior, *International Journal of Science and Engineering Applications*, Vol. 4 No. 6. pp. 353-356. (Online) Available at: http://www.ijsea.com/archive/volume4/issue6/IJSEA04061004.pdf (Accessed 7 July 2017).

Botha, R. A., Furnell, S.M. & Clarke, N.L. (2009). From desktop to mobile: examining the security experience. *Computers & Security*, Vol.28 No.3-4, pp. 130-137.

Brenner, J. (2013). *Pew Internet: Mobile. Pewinternet.org.* (Online) Available at: http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx (Accessed 23 July 2017)

Burns, A. J., & Johnson, M. E. (2015). Securing health information. *IT Professional*, Vol. 17 No.1, pp. 23-29.

Business Insider (2013). *The number of smartphones in use is about to pass the number of PCs.* (Online) Available at: www.businessinsider.com/number-of-smartphones-tablets-pcs-2013-12 (Accessed 21June 2017).

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

Chang, Y.F., Chen, C.S. & Zhou, H. (2009). Smart phone for mobile commerce. *Computer Standards & Interfaces,* Vol. 31 No. 4, pp.740-747.

Chin, E., Felt, A.P., Sekar, V. and Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *In Proceedings of the eighth symposium on usable privacy and security, July.* (p. 1). ACM.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security,* Vol.10 No.3, pp.13-19.

CNBC (2014). *Most Americans don't secure their smartphones.* (Online) Available at: www.cnbc.com/id/101611330# (Accessed 1 July 2017).

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

Dourish, P., Grinter, R., de la Flor, J., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, Vol. 8 No. 6, pp. 91-401.

ENISA: European Union Agency for Network and Information Security (2010). *Smartphone security: information security risks, opportunities and recommendations for users.* (Online) Available at: www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/ at_download/fullReport (Accessed 1 July 2017).

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

Furnell, S. (2005). Handheld hazards: the rise of malware on mobile devices. *Computer Fraud & Security*, Vol. 2005 No. 5, pp. 4-8.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal internet users. *Computers & Security,* Vol.26 No.1, pp. 410-417.

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security,* Vol.27 No.7-8, pp.235-240.

Gajjar, K. and Parmar, A. (2015). A Study of Challenges and Solutions for Smart Phone Security. *Emerging Research in Computing, Information, Communication and Applications, Bangalor, India*, Springer India, pp 325-334.

Gravetter, F. & Wallnau, L. (2009). *Statistics for the behavioral sciences.* 8th ed. Belmont, CA: Wadsworth.

Harbach, M., Hettig, M., Weber, S. & Smith, M. (2014 a). Using personal examples to improve risk communication for security & privacy decisions. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems.* ACM, pp. 2647–2656.

Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A. & Smith, M., (2014 b). It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. *Symposium on usable privacy and security (SOUPS)* July, pp. 9-11.

Harris, M.A. & Patten, K.P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility, *Information Management & Computer Security*, Vol.22 No. 1, pp. 97-114.

Harris, M.A., Furnell, S. & Patten, K. (2015). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy & Security*, Vol.10 No.4, pp. 186 – 202.

Hart, C. (2009). *Doing your Masters Dissertation*. London: Sage

Hogben, G. & Dekker, M. (2010). Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency*, Vol. 710, No. 01.

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, Available at: https://doi.org/10.1108/ILS-10-2016-0075

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.

Husted, N., Saïdi, H., & Gehani, A. (2011). Smartphone security limitations: Conflicting traditions. *Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies*, pp. 5-12.

IDC (2016). *Smartphone OS market share, Q3 2016,* (Online) Available at: www.idc.com/prodserv/smartphone-os-market-share.jsp (Accessed 21 June 2017).

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.

ISO/IEC 27000:2014. (2014). *International standard. Information technology - Security techniques Information security management systems - Overview and vocabulary.* Haettu 28.4.2014 osoitteesta (Online) Available at: http://www.iso27001security.com/html/27000.html (Accessed 27 August 2017)

Jeon, W., Kim, J., Lee, Y. & Won, D. (2011). A Practical Analysis of Smartphone Security. *Human Interface and the Management of Information. Interacting with Information, Orlando, FL, USA*, Springer Verlag, Heidelberg, pp.311-320.

Jones, B.H. & Chin, A.G. (2015). On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time", *International Journal of Information Management*, Vol.35 No.5, pp. 561-571.

Jones, B.H. & Heinrichs, L. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, Vol.53 No.2, pp. 22-30.

Jones, B.H., Chin, A.G. & Aiken, P. (2014). Risky business: students and smartphones. *Techtrends Linking Research & Practice to Improve Learning*, Vol.58 No.6, pp. 73-83.

Karamizadeh, S., Shayan, J., Alizadeh, M., & Kheirkhah, A. (2013). Information security awareness behavior: a conceptual model for cloud. *International Journal of Computers & Technology*, Vol. 10 Vol. 1, pp. 1186-1191.

Kelley, P. G., Cranor, L. F. & Sadeh, N. (2013). Privacy as part of the app decision-making process. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM*, pp. 3393–3402.

Keys, A., (2013). Smartphone Financial Transactions: Security Risks and Control Options. *Master's thesis,* Applied Information Management and the Graduate School, University of Oregon.

Kissel, R. (2013). Glossary of key information security terms. *National Institute of Standards and Technology*, Tech. Rep. NISTIR 7298 Revision 2.

Kraus, L., Wechsung, I. & Moller, S. (2014). Using statistical information to communicate android permission risks to users. *Socio-Technical Aspects in Security and Trust (STAST), Workshop on. IEEE,* pp. 48–55.

Kraus, L., Wechsung, I. & Moller, S. (2016). Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones. *Proceedings of the 1st European Workshop on Usable Security (EURO USEC),* July. DOI: dx.doi.org/10.14722/eurousec.2016.23009

La Polla, M., Martinelli, F. & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE communications surveys & tutorials*, Vol. 15 No.1, pp.446-471.

Landman, M. (2010). Managing smart phone security risks. *2010 Information Security Curriculum Development Conference*, pp.145-155.

Larkin, E. (2009). Banking by phone: Convenient and safe? *PC World*, Vol. 27 No. 11, pp. 39.

Lawton, G. (2008). Is it finally time to worry about mobile malware? *Computer,* Vol.41 No.5, pp.12-14.

Lazou, A., & Weir, G. R. (2011). Perceived risk and sensitive data on mobile devices. *Cyberforensics: Issue and Perspectives*, pp.183–196.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, Vol. 48 No. 8, pp. 72-77.

Li, X.T., Ren, S., Cheng, W., Xiang, L.S. & Liu, X.Y. (2014). Smartphone: Security and Privacy Protection, *Joint International Conference on Pervasive Computing and the Networked World, Vina del Mar, Chile,* Springer, Swizerland, pp.289-302.

Li, Y. & Siponen, M. (2011). A call for research on home users' information security behavior, *In PACIS 2011 Proceedings,* pp. 1-12.

Lin, C., & Varadharajan, V. (2010). Mobiletrust: A trust enhanced security architecture for mobile agent systems. *International Journal of Information Security*, Vol. 9 No.3, pp.153-178.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal*, Vol.24 No.3, pp.1-8.

M¨oller, A., Michahelles, F., Diewald, S., Roalter, L. & Kranz, M. (2012). Update behavior in app markets and security implications: A case study in google play. *Proc. of the 3rd Intl. Workshop on Research in the Large. Held in Conjunction with Mobile HCI*, pp. 3–6.

Mattord, H. J. & Whitman, M.E. (2012). *Principles of information security*. 4th ed. Course Technology: Cengage Learning.

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). 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.

Mylonas, A., Kastania, A. & Gritzalis, D. (2013 b). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, Vol. 34 (May), pp. 47-66.

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. (2015a). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information & Computer Security*, *23*(4), pp.406-420.

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

Nist glossary. (2013). *Glossary of Key Information Security Terms*. National Institute of Standards and Technology. Haettu 28.4.2014 osoitteesta (Online) Available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (Accessed 12 July 2017)

Nurse, J. R., Erola, A., Goldsmith, M., & Creese, S. (2015). Investigating the leakage of sensitive personal and organisational information in email headers. *Journal of Internet Services and Information Security (JISIS)*, Vol.5 No.1, pp.70-84.

Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking. *Information Systems Security*, Vol.16 No.6, pp. 302-314.

Oppenheim, A. (1992). *Questionnaire Design, Interviewing and Attitude Measurement*, London: Printer.

Park, J.H., Yi, K.J. & Jeong, Y.S. (2014). An enhanced smartphone security model based on information security management system (ISMS). *Electronic Commerce Research*, Vol.14 No.3, pp. 321-348.

Peng, S., Wu, M., Wang, G. & Yu, S. (2014). Propagation model of smartphone worms based on semi-Markov process and social relationship graph. *Computers & Security*, Vol. 44 (July), pp. 92-103.

Pitt, L.F., Parent, M., Junglas, I., Chan, A. & Spyropoulou, S., (2011). Integrating the smartphone into a sound environmental information systems strategy: Principles, practices and a research agenda. *The Journal of Strategic Information Systems*, Vol. 20, No.1, pp.27-37.

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).

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyberattacks and novice IT management in a small university. *Journal of Cases on Information Technology,* Vol.8 No.4, pp. 24-34.

Rantonen, K. (2014). Explaining information security behavior – case of the home user", Master's thesis, Department of Computer Science. University of Jyväskylä. (Online) Available at: https://jyx.jyu.fi/dspace/bitstream/handle/123456789/45877/URN:NBN:fi:jyu-201505121832.pdf?sequence=1 (Accessed 3 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.

Ross P. E. (2011). Top 11 technologies of the decade. *IEEE Spectrum,* Vol. 48, No. 1, pp. 27-63. Doi: 10.1109/MSPEC.2011.5676379

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, Vol.63 No.9, pp.1278-1308.

Sari, P.K. (2012). A Concept of Information Security Management for Higher Education. *Proceedings of the 3rd International Conference on Technology and Operation Management, Bandung,* Indonesia, 4-6 July.

Simpson, J. P. (2016). Empirical Analysis of Socio-Cognitive Factors Affecting Security Behaviors and Practices of Smartphone Users. *Doctoral dissertation*. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (951) http://nsuworks.nova.edu/gscis_etd/951.

Souppaya, M. & Scarfone, K. (2013). *Guidelines for managing the security of mobile devices in the enterprise.* (Online) Available at: http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf (Accessed 8 May 2017).

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user behavior. *Computers & Security*, Vol.24, pp.124-133.

TechCrunch (2014). *iTunes app store now has 1.2 million apps, has seen 75 billion downloads to date.* (Online) Available at: http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/ (Accessed 21 June 2017).

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

Van Niekerk & Von Solms. (2010). Information security culture: A management perspective. *Computers & Security,* Vol.29, pp. 476-486.

Waehlisch, M. , Trapp, S. , Schiller, J. , Jochheim, B. , Nolte, T. , et al. (2012). Vitamin c for your smartphone: The SKIMs approach for cooperative and lightweight security at mobiles. *Computer Communication Review,* Vol. 42 No. 4, pp. 271-274.

Wang, Y., Streff, K. & Raman, S. (2012) Smartphone security challenges. *Computer*, Vol.45 No.12, pp. 52-58.

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.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, Vol.16 No.6, pp. 315-331.

Yoon, C., Hwang, J.W. & Kim, R., (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education,* Vol. 23 No. 4, p.407.

Zhang, J., Reithel, B.J. & Li, H. (2009). Impact of perceived technical protection on security behaviours. *Information Management & Computer Security*, Vol. 17 No. 4, pp. 330-340.

Zissis, D. & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture", *Government Information Quarterly*, Vol. 28 No. 2, pp. 239-251.

Zonouz, S., Houmansadr, A., Berthier, R. , Borisov, N. , & Sanders, W. , et al. (2013). Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. *Computers & Security*, Vol. 37, pp. 215-227.

13. Appendices
Appendix-A: Reflection

I found the process of carrying out this dissertation as very challenging and time consuming but completion of the research, ultimately, made me feel very rewarding and peace in my mind. One of the main positive aspects I felt during doing this dissertation was the freedom of choosing my own topic in this regard. In the process of doing that, I had a consultation with my Supervisor about my proposed topic where he primarily encouraged me to go for further study and explore insight of it for preparing a research proposal. I felt very happy because I have been given the opportunity to work on such topic of which I am passionate about. I was a bit of worried about it at the beginning but I felt confident on that very moment when my proposal got accepted and I started look forward to my final dissertation project. I must admit that, even though I have been given the liberty to work on my own topic, I deeply felt the shortage of time in exploring my topic in greater detail in practice. However, at the end of the research, I feel satisfied about my overall research project because I became able to address the aims I intended in the first place and the objectives I had set initially got achieved finally. Meanwhile, it was not possible to addressed all of the objectives in depth, those were hoped initially.

The research was conducted on the information security behaviour of the students of University of Dhaka, Bangladesh in the use of smartphones. Due to the time constraint, the research project has been limited only to the students of University of Dhaka, Bangladesh. However, further research can be conducted in a large extent on this topic where students from the University of Dhaka as well as other universities of Bangladesh can be included.

The students had a choice of providing their opinion about this research and I am glad to share that a significant number of students have acknowledged that this research was very helpful for them in terms of making them aware about smartphone security. Moreover, many students have also given me feedback through personal email by acknowledging that they have learned a lot of things out of this research. The students also believe that there ought to be more research in this area of study as the information and smartphone are the most significant subject that people are involved in, at the present time.

I have gone through constant learning process during conducting this research. A lot of information on smartphone security issues were unknown to me before starting work to this research project. I have noticed that there is a huge gap of research on the aspect of information security risks of the students in the use of smartphones. I found this very difficult to work on without having any existing literature that indicate various core issues of information security risks in the perspective of Bangladesh.

In conducting this research, Google Doc Form was used to collect the responses from the participants due to its nature of being free, mobile friendly, and unlimited respondents can participate in the survey. The respondents were able to fill out the survey questionnaire by making a simple click on the provided link: https://goo.gl/forms/LJ4FoQz6w25JW5mx2. In the process of preparing the online survey questionnaire I have learned a lot about how an online survey helps to reach huge number of participants within a very short time.

Moreover, I have also learned different statistical approach in the process of analyzing the findings part of my dissertation. On the above, during working on this research, I have come to know that how to manage the time effectively. In this process, I have followed the workplan or time schedule that I have mentioned in my research proposal.

I am very satisfied by conducting this research for a number of reasons. As mentioned earlier, one of such reason is that, I have got so many positive responses and personal e-mail by mentioning that the students were benefitted in a great extent due to this research. Other reason is my satisfaction on the outcome of the research where it was revealed that the students possess moderately secure attitudes or behaviours towards the information security issues in the use of smartphones. But one concerning issue that I must want to mention that in the cases of some issue, they appeared to have very much security consciousness where in other cases they were found to be very reckless in ensuring their information security. Because of this attitude, 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. However, this study will help to the students in gaining better understanding about information security behaviours in the use of smartphone. Moreover, I am quite satisfied with the works as I have learned a lot of things about smartphone security aspects which are very important issues or subject in this present days.

Appendix-B: Dissertation Proposal

Working title

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

Introduction

In this age of information communication technology, mobile phone is considered as a very useful instrument for communication and becomes an integral part of our daily life. Mobile phone communication facilities have been upgraded by the introduction of smartphone device. Apart from mere call or text facilities, smartphone offers a wide range of computing capabilities and connectivity options as like as traditional computers in the form of various applications. The usage of these applications has great impact towards the behaviour of smartphone users (Alfawareh and Jusoh, 2014). Along with other group of users, students are also great fond of using smartphones. Currently students do use smartphone applications for diverse range of academic purposes (Woodcock et al., 2012), using various social networking sites, online shopping and banking, access to email and many more. Therefore, the smartphones are becoming very popular day by day among students.

Due to the availability of internet facilities in the smartphones, various mobile applications are used in it which inevitably increases a range of information security risks. Because of the diverse use of these mobile applications, personal information gets collected and stored in the smartphones which can easily be aggregated to draw a complete information and be used maliciously (Jones and Chin, 2015). In such circumstances, protecting personal information through adaptation of security measures are very crucial. However, it is critical to understand the information security behaviour in the use of smartphones. This study will investigate the information security behaviour of the students of University of Dhaka, Bangladesh in the use of smartphones. The method of this research would include a comprehensive review of relevant literature to gain an understanding about the topic clearly which will expectedly help to set up appropriate questionnaire for data collection. The collected data will be analyzed to gain an understanding about the information security behaviours of the students in consideration of various measures like their behaviours in using specific applications, avoidance of harmful attitudes, measuring their preparation for disaster recovery, their knowledge about useful phone settings and add-on utilities, and finally making a comparison of information security behaviour among the students of University of Dhaka, Bangladesh.

Aims and Objectives

The aim of this research is to explore the students' information security behaviour in the use of smartphone of University of Dhaka, Bangladesh and assisting relevant department or institutions with it in adopting necessary steps as well as developing strategies and policies, and designing training programs for the students regarding information securities.

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 uses smartphones?

Scope and definition

This study will investigate students' attitudes towards the information security behaviour in the University of Dhaka, Bangladesh. The University of Dhaka, Bangladesh has been chosen carefully because it is one of the best public universities of Bangladesh with huge resources, large number of students, great reputation, strong faculties as well as the researcher has got the direct contact with the institution. The study will 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 upon considering the result of this study through inclusion of other universities' students to raise information security awareness among the students and take necessary initiatives from the side of the authority to resolve this issue.

In this study, the information security behaviours of the students will be evaluated in respect of smartphone using. Referred smartphones are expected to contain the minimum efficiency of using mobile applications by using the internet facilities. According to Jeon et al., (2011) the smartphones can be defined as a device which provides advanced computing ability and connectivity on the top of the basic features of the mobile phones. Accordingly, the information security demonstrates “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide information confidentiality, integrity, and availability” (Kissel, 2013, p.94). Generally, information security comprises the information confidentiality, authenticity, availability, integrity and accountability (Zissis and Lekhas, 2011).

It is difficult to define information security behaviour because of its vastness and complexity (Rantonen, 2014). Different people have measured the information security behaviours in different aspects. Information security behaviour is nothing but taking precautions by adaptation of necessary measures to secure one’s information, devices and so on. Due to the wider use of the internet, individual users put the fellow users at risk along with themselves, therefore, recognising the risks and taking necessary precautions are important subject in the present time (Li and Siponen, 2011). Agarwal and Anderson (2010) defined information security behaviour as the understanding of individual willingness in taking recommended security precautions like running and updating antivirus software, securing passwords, utilising a firewall and becoming cautious about emails sent by unknown sources at their own accord to protect themselves. So, it can be said that the student’s information security behaviour in the use of smartphone demonstrates, taking necessary precautions for the safety of individual’s own personal smartphone device as well as others in the internet with an aim to improve information security measures.

Research context / literature review

Smartphone brings range of facilities by incorporating various technologies into it like a computer. Among many other diverse usage, smartphones are used for the storing various personal information like contact details, location information, bank detail, emails, and so on of an individual (Jeon et al., 2011). It becomes essential to understand the importance of securing this personal information contains in the smartphone.

Due to storing of various personal information in the smartphone several information security risks are associated with this. In most cases third party applications are used in the smartphones who may sometimes get the automatic access to the personal information without the consent of the users (Das and Khan, 2016). Generally, the smartphone users download and use the applications without being aware about security measures of those applications which may lead to the serious security risk for them (Gajjar and Parmar, 2015). Besides, the smartphones can be lost or stolen in which case the personal information of the users can be acquired by the third parties as well as the sensitive information might be destroyed permanently (Imgraben et al., 2014). Apart from this the smartphones which are connected through the Bluetooth or Wi-Fi, can be affected by malwares where the unauthorised access might be gained to collect and damage sensitive information by performing meaningless operations (Wang et al., 2012; Jeon et al., 2011).

To resolve this crisis of information security in the smartphone, several technological advancements like strong passwords, antivirus, anti-spyware, encryption, firewalls, and strong passwords has been made. Users may minimise the risk of breaching information security by adopting these latest technologies (Esmaeili, 2014). Using appropriate password may prevent unauthorised access to personal information by others, the backup function may recover the sensitive information and sometimes antivirus software helps to prevent attacks from unsafe links, viruses, phishing, and malwares accordingly (Park et al., 2014; Li et al., 2014; Jeon et al., 2011). Information security would be vulnerable if the users do not maintain proper information security behaviour. According to Esmaeili (2014) individual’s information security behaviour can play significant role towards securing the personal information in using smartphones.

A wide range of research has been carried out for understanding information security behaviour in the use of smartphone from different aspects. Ngoqo and Flowerday (2015) conducted a study on information security behaviours of the student mobile phone users with an aim to levering security awareness as a way of stimulating safer information security behaviours where they proposed a framework that can be used to profile the students’ information security behaviour. It was examined by Harris and Patten (2014) that in downloading mobile applications from the repositories, the smartphone users show over confidence which cause information security risks. In a study Jones et al. (2014) said that it is important to investigate security features of the mobile applications before downloading because the applications from unknown sources are considered as the major risk to information security. Besides, several researches were conducted with drawing a suggestion about various safety measures to protect information security by using appropriate technologies, add-on utilities and effective encryption mechanism (Jones and Heinrichs, 2012; Souppaya and Scarfone, 2012; Park et al.,2014).

Bangladesh is well known as one of the largest and fastest growing mobile phone market of the world. It is reported by the Bangladesh Telecom Regulatory Commission (BTRC, 2017) that, by the end of the February 2017 the mobile phone subscriptions has reached to 129.584 million. Furthermore, the smartphone sales in the capital city of Dhaka are much higher compare 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 37064 pupils are studying (www.du.ac.bd). Though there have been many research works conducted on the area of information security behaviour of the smartphone users but no research has been conducted yet on this field in Bangladesh. However, this paper aims to conduct an empirical study on the information security behaviours of the students of University of Dhaka, Bangladesh in the use of smartphone to protect information security of the students.

Methodology

This research aims to understand the information security behaviours of the Dhaka University (DU) students in the use of smartphones. This exploratory research will follow the quantitative methodology where questionnaire will be developed to conduct online survey in order to achieve research objectives. Survey method is considered as one of the prominent ways of acquiring relevant information like social characteristics, behaviours, attitudes of the focussed group of people on any given topic (Bird, 2009; Rhee et al., 2009). Therefore, online survey method has been determined for this research to collect data towards gaining understanding the information security behaviours of the students of University of Dhaka in the use of smartphones. Notably, in carrying out the online survey, the Google Forms will be used to collect the responses from the respondent in this study.

With the view of achieving research objectives properly, the survey questionnaire will be developed in two parts (ENISA, 2010; Jones and Heinrichs, 2012). In the first part of the questions, the demographic information of the participants will be collected. The second part will aim to collect the exploratory information related to information security of the students in the use of smartphones. Questionnaire will be pilot-tested accordingly to be assured about the validity of the findings. Necessary modification of the questionnaire will be brought upon considering the feedback of the pilot-testing. Finally, a statistical analysis will be conducted with the collected data by using descriptive analysis and Pearson’ Chi-square test to investigate the students’ behaviour in the use of smartphone.

Work plan

Expected timeframe and working plan for completing the dissertation.

	May		June		July		August		September	
Generating ideas for dissertation topic and proposal submission	■									
Searching and reading relevant and current literature		■	■	■						
Preparing questionnaire and pilot-testing; making correction if required			■							
Start writing Introduction and Literature review					■	■				
Sending online questionnaire to the participants				■	■					
Assess response rate and send reminder email if needed					■					
Start analyzing and writing the results of questionnaire responses						■	■			
Writing up recommendations and conclusion of the dissertation								■		
Revising, editing and Proof reading of the research paper									■	
Finish up writing the full dissertation and submit it										■

Resources

In order to prepare survey questionnaire and distribute those, the Google Forms will be used due to its quality of being free, mobile friendliness and capability to receive huge number of responses. In addition to this, the collected data will be processed by using IBM SPSS Statistics and Microsoft Excel.

Ethics

In any given research, ethical issues are the very important aspects to consider because ethical issues may arise in any stage and out of any consequence of progression of the research. According to Hart (2009, p.296), "... ethical issues can arise during all stages of your research, from the design stage through to the reporting stage ...". In this study, it is expected that no major ethical issues will arise because of the nature of the research. The survey of this research will be conducted through online questionnaire and all the prospective participants are the university students who are over 18 years old. Besides, it is not intended to collect any personal data of the respondents which might raise the ethical issues. Moreover, the participants will neither be called for face to face interview, nor will be expected to attend to any private premises. Copyright issues will be taken care of appropriately as the citation will be maintained appropriately for using of relevant literature. So, overall it can be expected that no ethical issues will arise in this study. Additionally, an ethics check list form provided by the university has been incorporated at the end of this research proposal.

Confidentiality

In this research, a survey will be conducted among students of University of Dhaka, Bangladesh where it is expected that they will answer the survey questions with fair, open and honest attitude. There are very slim chances of coming across sensitive information because the researcher will not collect any personal information of the students. The participants will be kept anonymous during collecting their responses and the highest level of personal information will include only the department and faculty name of the students to enable us comparing their information security behaviours in the use of smartphones. Besides, the email addresses of the respondents may be asked for, if they become willing to be contacted for any further correspondence or referrals by making sure that those details remain confidential. However, there is no possibility of using those information in a manner which may be considered abusive towards the respondents because respondents would not be identifiable and the collected information will be handled with confidentiality.

References

Agarwal, R. and Anderson, C. L. (2010). Practising safe computing: a multimethod empirical examination of home computer user security behavioral intentions, *MIS Quarterly,* Vol. 34 No.3. pp. 613-643.

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).

Bird, D. K. (2009). The use of questionnaires for acquiring information on public perception of natural hazards and risk mitigation - a review of current knowledge and practice, *Natural Hazards & Earth System Sciences*, Vol.9 No.4, pp. 1307 –1325.

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

ENISA. (2010). Smartphone Security: Information Security Risks, Opportunities and Recommendations for Users, (Online) Available at: https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users (Accessed 2 May 2017)

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

Gajjar, K. and Parmar, A. (2015). A Study of Challenges and Solutions for Smart Phone Security, *Emerging Research in Computing, Information, Communication and Applications, Bangalor, India*, Springer India, pp 325-334.

Harris, M.A. and Patten, K.P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility, *Information Management & Computer Security*, Vol.22 No. 1, pp. 97-114.

Hart, C. (2009). *Doing your Masters Dissertation*. London: Sage

Hossain, M.E. and 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. and 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.

Jeon, W., Kim, J., Lee, Y. and Won, D. (2011). A Practical Analysis of Smartphone Security, *Human Interface and the Management of Information. Interacting with Information, Orlando, FL, USA,* Springer Verlag, Heidelberg, pp.311-320.

Jones, B.H. and Chin, A.G. (2015). On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time, *International Journal of Information Management*, Vol.35 No.5, pp. 561-571.

Jones, B.H. and Heinrichs, L. (2012). Do business students practice smartphone security?, *Journal of Computer Information Systems,* Vol.53 No.2, pp. 22-30.

Jones, B.H., Chin, A.G. and Aiken, P. (2014). Risky business: students and smartphones, *Techtrends Linking Research & Practice to Improve Learning,* Vol.58 No.6, pp. 73-83.

Kissel, R. (2013). Glossary of key information security terms, *National Institute of Standards and Technology,* Tech. Rep. NISTIR 7298 Revision 2.

Li, X.T., Ren, S., Cheng, W., Xiang, L.S. and Liu, X.Y. (2014). Smartphone: Security and Privacy Protection, *Joint International Conference on Pervasive Computing and the Networked World, Vina del Mar, Chile*, Springer, Swizerland, pp.289-302.

Li, Y. and Siponen, M. (2011). A call for research on home users' information security behavior, *In PACIS 2011 Proceedings,* pp. 1-12.

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

Park, J.H., Yi, K.J. and Jeong, Y.S. (2014). An enhanced smartphone security model based on information security management system (ISMS), *Electronic Commerce Research*, Vol.14 No.3, pp. 321-348.

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).

Rantonen, K. (2014). Explaining information security behavior – case of the home user", Master's thesis, Department of Computer Science. University of Jyväskylä. (Online) Available at: https://jyx.jyu.fi/dspace/bitstream/handle/123456789/45877/URN:NBN:fi:jyu-201505121832.pdf?sequence=1 (Accessed 3 May 2017)

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

Souppaya, M. and Scarfone, K. (2013). *Guidelines for managing the security of mobile devices in the enterprise,* (Online) Available at: http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf (Accessed 8 May 2016).

Wang, Y., Streff, K. and Raman, S. (2012). Smartphone security challenges, *Computer*, Vol.45 No.12, pp. 52-58.

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.

Zissis, D. and Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture, *Government Information Quarterly*, Vol. 28 No. 2, pp. 239-251.

Ethics Review Form: LIS Masters projects

Part A: Ethics Checklist

If your answer to any of the following questions (1 – 3) is YES, you must apply to an appropriate external ethics committee for approval:		Delete as appropriate
1.	Does your project require approval from the National Research Ethics Service (NRES)? (E.g. because you are recruiting current NHS patients or staff? If you are unsure, please check at http://www.hra.nhs.uk/research-community/before-you-apply/determine-which-review-body-approvals-are-required/)	**No**
2.	Will you recruit any participants who fall under the auspices of the Mental Capacity Act? (Such research needs to be approved by an external ethics committee such as NRES or the Social Care Research Ethics Committee http://www.scie.org.uk/research/ethics-committee/)	**No**
3.	Will you recruit any participants who are currently under the auspices of the Criminal Justice System, for example, but not limited to, people on remand, prisoners and those on probation? (Such research needs to be authorised by the ethics approval system of the National Offender Management Service.)	**No**

If your answer to any of the following questions (4 – 11) is YES, you must apply to the Senate Research Ethics Committee for approval (unless you are applying to an external ethics committee):		Delete as appropriate
4.	Does your project involve participants who are unable to give informed consent, for example, but not limited to, people who may have a degree of learning disability or mental health problem, that means they are unable to make an informed decision on their own behalf?	**No**
5.	Is there a risk that your project might lead to disclosures from participants concerning their involvement in illegal activities?	**No**
6.	Is there a risk that obscene and or illegal material may need to be accessed for your project (including online content and other material)?	**No**
7.	Does your project involve participants disclosing information about sensitive subjects?	**No**
8.	Does your project involve you travelling to another country outside of the UK, where the Foreign & Commonwealth Office has issued a travel warning? (http://www.fco.gov.uk/en/)	**No**
9.	Does your project involve invasive or intrusive procedures? For example, these may include, but are not limited to, electrical stimulation, heat, cold or bruising.	**No**
10.	Does your project involve animals?	**No**
11.	Does your project involve the administration of drugs, placebos or other substances to study participants?	**No**

If your answer to any of the following questions (12 – 18) is YES, you should consult your supervisor, as you may need to apply to an ethics committee for approval.		Delete as appropriate
12.	Does your project involve participants who are under the age of 18?	**No**
13.	Does your project involve adults who are vulnerable because of their social, psychological or medical circumstances (vulnerable adults)? This includes adults with cognitive and / or learning disabilities, adults with physical disabilities and older people.	**No**
14.	Does your project involve participants who are recruited because they are staff or students of City University London? For example, students studying on a particular course or module. (If yes, approval is also required from the Project Tutor.)	**No**
15.	Does your project involve intentional deception of participants?	**No**
16.	Does your project involve identifiable participants taking part without their informed consent?	**No**
17.	Does your project pose a risk to participants or other individuals greater than that in normal working life?	**No**
18.	Does your project pose a risk to you, the researcher, greater than that in normal working life?	**No**

If your answer to the following question (19) is YES and your answer to all questions 1 – 18 is NO, you must complete part B of this form.		
19.	Does your project involve human participants? For example, as interviewees, respondents to a questionnaire or participants in evaluation or testing.	**Yes**

Part B: Ethics Proportionate Review Form

The following questions (20 – 24) must be answered fully.		Delete as appropriat e
20.	Will you ensure that participants taking part in your project are fully informed about the purpose of the research?	**Yes**
21.	Will you ensure that participants taking part in your project are fully informed about the procedures affecting them or affecting any information collected about them, including information about how the data will be used, to whom it will be disclosed, and how long it will be kept?	**N/A**
22.	When people agree to participate in your project, will it be made clear to them that they may withdraw (i.e. not participate) at any time without any penalty?	**Yes**
23.	Will consent be obtained from the participants in your project, if necessary? Consent from participants will only be necessary if you plan to gather personal data. "Personal data" means data relating to an identifiable living person, e.g. data you collect using questionnaires, observations,	**N/A**

	interviews, computer logs. The person might be identifiable if you record their name, username, student id, DNA, fingerprint, etc. If YES, attach the participant information sheet(s) and consent request form(s) that you will use. You must retain these for subsequent inspection. Failure to provide the filled consent request forms will automatically result in withdrawal of any earlier ethical approval of your project.	
24.	Have you made arrangements to ensure that material and/or private information obtained from or about the participating individuals will remain confidential? Provide details:	**N/A**

If the answer to the following question (25) is YES, you must provide details		Delete as appropriate
25.	Will the research involving participants be conducted in the participant's home or other non-University location? If **YES**, provide details of how your safety will be ensured: The questionnaire for the survey will be sent electronically by university email and the researcher is an employee of the respective university.	**No**

Attachments (these must be provided if applicable):	Delete as appropriate
Participant information sheet(s)	**Not applicable**
Consent form(s)	**Not applicable**
Questionnaire(s)	**Will be provided later**
Topic guide(s) for interviews and focus groups	**Not applicable**
Permission from external organisations (e.g. for recruitment of participants)	**Not applicable**

Appendix-C: Questionnaire

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

Dear all,

Currently I am pursuing my MSc in Library Science at City, University of London. As part of my master's dissertation I am conducting a survey on "Information security behaviour of smartphone users: An empirical study on the students of University of Dhaka, Bangladesh". This study seeks to determine the students' information security behaviour in the use of smartphone. This is purely an academic research. Please spend 10 minutes of your valuable time to fill out a brief questionnaire. I do believe that participating in this research project will not cause even a minimal risk to you. Participation in this survey is voluntary and completely up to you. Filling out the survey implies that you provide an informed consent to use the data you provide in this questionnaire for research purposes. Your privacy and confidentiality will be strictly protected. All data gathered will be stored securely by the researcher. If you have any questions/comments or would like to know more about my research project, please feel free to contact me at shohana.nowrin@city.ac.uk

You will be able to fill out the survey questionnaire by making a simple click on the provided link: https://goo.gl/forms/LJ4FoQz6w25JW5mx2 .

Thank you so much in advance for your kind cooperation.

Shohana Nowrin
PG Student
Department of Library and Information Science
City, University of London
United Kingdom
E-mail: shohana.nowrin@city.ac.uk

Section A: Academic and demographic information

1. Please specify your gender.

□ Male
□ Female

2. Please specify your age group.

□ Under 18
□ 18-24
□ 25-34
□ 35-44
□ 45-54
□ 55 and over

3. Please specify your faculty.

□ Faculty of Arts
□ Faculty of Science
□ Faculty of Social Sciences
□ Faculty of Business Studies
□ Faculty of Law
□ Faculty of Biological Sciences
□ Faculty of Pharmacy
□ Faculty of Engineering and Technology
□ Faculty of Earth and Environmental Sciences
□ Faculty of Fine Arts
□ Faculty of Medicine
□ Faculty of Education
□ Faculty of Postgraduate Medical Sciences & Research
□ Institute of Social Welfare and Research
□ Institute of Health Economics
□ Institute of Nutrition and Food Science
□ Institute of Disaster Management and Vulnerability Studies
□ Institute of Modern Languages
□ Institute of Leather Engineering and Technology
□ Institute of Statistical Research and Training
□ Institute of Energy
□ Institute of Education and Research
□ IIT
□ IBA

4. Please specify the level of education that you are currently studying.

□ PhD
□ MPhil
□ Master
□ Bachelor

Section B: Information security behaviour related questions

5. Do you use smartphone?

   □ Yes
   □ No (If No, please discontinue)

6. How long have you been using it for?

   □ Less than 1 year
   □ 1 - 2 years
   □ 3 - 4 years
   □ 5 - 6 years
   □ More than 6 years

7. Do you use internet in your mobile phone?

   □ Yes
   □ No

8. Please specify your frequency of internet use in your mobile phone.

   □ Several times everyday
   □ A few times everyday
   □ At least once a day
   □ A few times a week
   □ At least once a week
   □ At least once a month
   □ Other

9. What is your mode of internet access in your mobile phone?

   □ Mobile network
   □ Wi-Fi
   □ Both

10. What is your preferred search engine in your mobile phone?

   □ Google
   □ Bing
   □ Ask.com
   □ Yahoo!
   □ Other

11. What is/are the reason/s that drives you mostly to use a smartphone? (You can choose multiple options)

□ Communicating with family, friends and teachers
□ Academic purpose
□ Browsing online
□ Using social networking sites
□ Entertainment
□ Listening to music
□ Taking pictures
□ Taking videos
□ Use as a watch
□ Use as an alarm clock
□ Sending and receiving emails
□ Other, please specify ……

12. Which brand of mobile phone hand set you are currently using?

□ Nokia
□ Samsung
□ Apple
□ Symphony
□ Sony Ericson
□ Walton
□ Motorola
□ Huawei
□ OPPO
□ HTC
□ Other

13. How safe do you consider in using smartphones?

□ Highly
□ High
□ Moderately
□ Not too much
□ Not at all

14. How concerned are you about the security of your smartphone?

□ Not worried
□ A bit worried
□ Enough worried
□ Much worried

15. Are you aware of information security in using the smartphone?

□ Yes
□ No

16. How do you assess your knowledge of issues and risks associated with the use of your smartphone?

□ None
□ Insufficient
□ Sufficient
□ Good
□ Excellent

17. Please specify your level of knowledge about how the options and technical characteristics of mobile phone affect its security?

□ None
□ Insufficient
□ Sufficient
□ Good
□ Excellent

18. Do you have knowledge about mobile operating system?

□ Yes
□ No (If No, please go to question 20)

19. Which operating system is run in your phone?

□ Android OS (Google Inc.)
□ BlackBerry OS
□ iPhone OS / iOS (Apple)
□ Windows Mobile (Windows Phone)
□ WebOS (Palm/HP)
□ Bada (Samsung Electronics)
□ MeeGo OS (Nokia and Intel)
□ Symbian OS (Nokia)
□ Other

20. Are you aware about the security measures that are offered by the modern operating system?

□ Yes
□ No

21. Do you know about International Mobile Equipment Identity (IMEI)?

□ Yes
□ No (If No, please go to question 23)

22. Have you written down your IMEI code?

□ Yes
□ No

23. Do you know that your contact lists may be uploaded to the central servers when you are using social networking apps?

□ Yes
□ No

24. Do you store personal information in your mobile phone?

□ Yes, without encryption
□ Yes, and encrypted
□ No (If No, please go to question 26)

25. What kind of personal information has been stored in your smartphone? (You can choose multiple options)

□ Friends’ contact information (phone number, email address etc.)
□ Your bank or credit card account passwords
□ ATM passwords
□ Your online account number
□ Your online account password
□ Personal or sensitive photos
□ Your email address
□ Your email account passwords
□ Others

26. Please specify which security risk you are aware of or you have faced in using the smartphone from the following list (You can choose multiple options)

□ Unintentional disclosure of data.
□ Data leakage resulting from device loss or theft.
□ Financial malware attacks.
□ Attacks on decommissioned smartphones.
□ Network spoofing attacks.
□ Surveillance attacks.
□ Phishing attacks.
□ Spyware attacks.
□ Diallerware attacks: an attacker steals money from the user by means of malware that makes hidden use of premium short message services or numbers.
□ Network congestion.
□ Other

27. Please specify your approaches towards reducing the risk of information securities regarding the use of smartphone.

	Always	Sometimes	Never
Switch off all data connections (e.g. by flight-mode)	□	□	□
Check permission/Access authorization to applications	□	□	□
Avoid downloading apps from unknown sources	□	□	□
Logging out of applications	□	□	□
Configure automatic locking	□	□	□
Avoid using smartphone location services	□	□	□
Avoid connecting to public Wi-Fi networks	□	□	□
Updates to smartphone systems and applications	□	□	□
Protect from theft (e.g. by securely storing the device)	□	□	□
Block one’s identity (e.g. fake user profiles)	□	□	□
Use messaging apps with end-to-end encryption	□	□	□
Avoid financial apps/ functions (e.g. online banking)	□	□	□
Use remote management apps	□	□	□

28. Please specify your approaches regarding the use of smartphone settings and add-on utilities.

	Always	Sometimes	Never
Deploy updates	□	□	□
Installation of anti-virus software or application	□	□	□
Disable Wi-Fi connection	□	□	□
Disable Bluetooth	□	□	□
Disable GPS	□	□	□
Modify privacy settings of the device	□	□	□
Avoid rooting the device	□	□	□
Use data/ device encryption	□	□	□
Use apps for privacy protection/ permission management	□	□	□
Reduce online “data traces”	□	□	□

29. Please specify your approaches regarding the disaster recovery while you face the loss of data from your smartphone

	Always	Sometimes	Never
Data backup	□	□	□
Data wiping out upon disposal	□	□	□
Blocking the device after losing it	□	□	□
Take out insurance	□	□	□

30. On a scale from 1 (Very poor) to 5 (Excellent) how do you assess your knowledge on aspects related to information security, both before and after participating this survey?

Before	1	2	3	4	5
After	1	2	3	4	5

(NB: 1- very poor; 2- below average; 3- average; 4- above average; 5- excellent)

31. Please specify your suggestions, if you have any, for improving the security measures in the use of smartphone?

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………

32. Anything else you wish to say?

………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………
………………………………………………………………………………………………

Thank you very much for your kind cooperation.

Appendix-D: Tables of group comparison

Table 1: *University of Dhaka (n=348), comparison of students' information security behaviours by gender in terms of avoidance of harmful behaviours*

		Configure automatic locking			Total
		Always	Sometimes	Never	
Male	Frequency	121	72	53	246
	% within Gender	49.2%	29.3%	21.5%	100.0%
	% of Total	34.8%	20.7%	15.2%	70.7%
Female	Frequency	47	42	13	102
	% within Gender	46.1%	41.2%	12.7%	100.0%
	% of Total	13.5%	12.1%	3.7%	29.3%
Total	Frequency	168	114	66	348
	% within Gender	48.3%	32.8%	19.0%	100.0%
	% of Total	48.3%	32.8%	19.0%	100.0%
		Use of remote management apps			Total
		Always	Sometimes	Never	
Male	Frequency	45	106	95	246
	% within Gender	18.3%	43.1%	38.6%	100.0%
	% of Total	12.9%	30.5%	27.3%	70.7%
Female	Frequency	10	59	33	102
	% within Gender	9.8%	57.8%	32.4%	100.0%
	% of Total	2.9%	17.0%	9.5%	29.3%
Total	Frequency	55	165	128	348
	% within Gender	15.8%	47.4%	36.8%	100.0%
	% of Total	15.8%	47.4%	36.8%	100.0%

Table 2: *University of Dhaka (n=348), comparison of students' information security behaviours by Faculties/Institutions in terms of avoidance of harmful behaviours*

		Switch off all data connections			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	36	94	10	140
	% within Faculty	25.7%	67.1%	7.1%	100.0%
	% of Total	10.3%	27.0%	2.9%	40.2%
Faculty of Social Sciences	Frequency	5	28	5	38
	% within Faculty	13.2%	73.7%	13.2%	100.0%
	% of Total	1.4%	8.0%	1.4%	10.9%
Faculty of Business Studies	Frequency	15	36	19	70
	% within Faculty	21.4%	51.4%	27.1%	100.0%
	% of Total	4.3%	10.3%	5.5%	20.1%
Faculty of Biological Sciences	Frequency	9	15	5	29
	% within Faculty	31.0%	51.7%	17.2%	100.0%
	% of Total	2.6%	4.3%	1.4%	8.3%
Faculty of Pharmacy	Frequency	5	24	7	36
	% within Faculty	13.9%	66.7%	19.4%	100.0%
	% of Total	1.4%	6.9%	2.0%	10.3%
Other faculties/institutions	Frequency	4	23	8	35
	% within Faculty	11.4%	65.7%	22.9%	100.0%
	% of Total	1.1%	6.6%	2.3%	10.0%
Total	Frequency	74	220	54	348
	% within Faculty	21.3%	63.2%	15.5%	100.0%
	% of Total	21.3%	63.2%	15.5%	100.0%
		Avoid downloading apps from unknown sources			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	89	27	24	140
	% within Faculty	63.6%	19.3%	17.1%	100.0%
	% of Total	25.6%	7.8%	6.9%	40.2%
Faculty of Social Sciences	Frequency	22	12	4	38
	% within Faculty	57.9%	31.6%	10.5%	100.0%
	% of Total	6.3%	3.4%	1.1%	10.9%
Faculty of Business Studies	Frequency	39	17	14	70
	% within Faculty	55.7%	24.3%	20.0%	100.0%
	% of Total	11.2%	4.9%	4.0%	20.1%
Faculty of Biological Sciences	Frequency	16	12	1	29
	% within Faculty	55.2%	41.4%	3.4%	100.0%
	% of Total	4.6%	3.4%	.3%	8.3%
Faculty of Pharmacy	Frequency	18	12	6	36
	% within Faculty	50.0%	33.3%	16.7%	100.0%
	% of Total	5.2%	3.4%	1.7%	10.3%
Other faculties/institutions	Frequency	15	13	7	35
	% within Faculty	42.9%	37.1%	20%	100.0%
	% of Total	4.3%	3.7%	2.0%	10.0%
Total	Frequency	199	93	56	348
	% within Faculty	57.2%	26.7%	16.1%	100.0%
	% of Total	57.2%	26.7%	16.1%	100.0%

		Logging out of applications			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	58	58	24	140
	% within Faculty	41.4%	41.4%	17.1%	100.0%
	% of Total	16.7%	16.7%	6.9%	40.2%
Faculty of Social Sciences	Frequency	10	20	8	38
	% within Faculty	26.3%	52.6%	21.1%	100.0%
	% of Total	2.9%	5.7%	2.3%	10.9%
Faculty of Business Studies	Frequency	21	32	17	70
	% within Faculty	30.0%	45.7%	24.3%	100.0%
	% of Total	6.0%	9.2%	4.9%	20.1%
Faculty of Biological Sciences	Frequency	8	19	2	29
	% within Faculty	27.6%	65.5%	6.9%	100.0%
	% of Total	2.3%	5.5%	.6%	8.3%
Faculty of Pharmacy	Frequency	15	10	11	36
	% within Faculty	41.7%	27.8%	30.6%	100.0%
	% of Total	4.3%	2.9%	3.2%	10.3%
Other faculties/institutions	Frequency	7	21	7	35
	% within Faculty	20%	60%	20%	100.0%
	% of Total	2.0%	6%	2.0%	10.0%
Total	Frequency	119	160	69	348
	% within Faculty	34.2%	46.0%	19.8%	100.0%
	% of Total	34.2%	46.0%	19.8%	100.0%
		Updates to smartphone systems and applications			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	100	33	7	140
	% within Faculty	71.4%	23.6%	5.0%	100.0%
	% of Total	28.7%	9.5%	2.0%	40.2%
Faculty of Social Sciences	Frequency	19	17	2	38
	% within Faculty	50.0%	44.7%	5.3%	100.0%
	% of Total	5.5%	4.9%	.6%	10.9%
Faculty of Business Studies	Frequency	40	25	5	70
	% within Faculty	57.1%	35.7%	7.1%	100.0%
	% of Total	11.5%	7.2%	1.4%	20.1%
Faculty of Biological Sciences	Frequency	18	9	2	29
	% within Faculty	62.1%	31.0%	6.9%	100.0%
	% of Total	5.2%	2.6%	.6%	8.3%
Faculty of Pharmacy	Frequency	19	14	3	36
	% within Faculty	52.8%	38.9%	8.3%	100.0%
	% of Total	5.5%	4.0%	.9%	10.3%
Other faculties/institutions	Frequency	24	6	5	35
	% within Faculty	68.6%	17.1%	14.3%	100.0%
	% of Total	6.9%	1.7%	1.4%	10.0%
Total	Frequency	220	104	24	348
	% within Faculty	63.2%	29.9%	6.9%	100.0%
	% of Total	63.2%	29.9%	6.9%	100.0%

Table- 3: *University of Dhaka (n=348), comparison of students' information security behaviours by Gender in terms of useful phone settings or add-on utilities*

		Reduce online data traces			Total
		Always	Sometimes	Never	
Male	Frequency	38	128	80	246
	% within Gender	15.4%	52.0%	32.5%	100.0%
	% of Total	10.9%	36.8%	23.0%	70.7%
Female	Frequency	33	40	29	102
	% within Gender	32.4%	39.2%	28.4%	100.0%
	% of Total	9.5%	11.5%	8.3%	29.3%
Total	Frequency	71	168	109	348
	% within Gender	20.4%	48.3%	31.3%	100.0%
	% of Total	20.4%	48.3%	31.3%	100.0%

Table- 4: *University of Dhaka (n=348), comparison of students' information security behaviours by Faculties/Institutions in terms of useful phone settings or add-on utilities*

		Deploy updates			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	50	54	36	140
	% within Faculty	35.7%	38.6%	25.7%	100.0%
	% of Total	14.4%	15.5%	10.3%	40.2%
Faculty of Social Sciences	Frequency	12	21	5	38
	% within Faculty	31.6%	55.3%	13.2%	100.0%
	% of Total	3.4%	6.0%	1.4%	10.9%
Faculty of Business Studies	Frequency	25	32	13	70
	% within Faculty	35.7%	45.7%	18.6%	100.0%
	% of Total	7.2%	9.2%	3.7%	20.1%
Faculty of Biological Sciences	Frequency	9	12	8	29
	% within Faculty	31.0%	41.4%	27.6%	100.0%
	% of Total	2.6%	3.4%	2.3%	8.3%
Faculty of Pharmacy	Frequency	11	17	8	36
	% within Faculty	30.6%	47.2%	22.2%	100.0%
	% of Total	3.2%	4.9%	2.3%	10.3%
Other faculties/institutions	Frequency	18	14	3	35
	% within Faculty	51.4%	40.0%	8.6%	100.0%
	% of Total	5.2%	4.0%	0.8%	10.0%
Total	Frequency	125	150	73	348
	% within Faculty	35.9%	43.1%	21.0%	100.0%
	% of Total	35.9%	43.1%	21.0%	100.0%
		Installation of anti-virus software or application'			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	81	31	28	140
	% within Faculty	57.9%	22.1%	20.0%	100.0%
	% of Total	23.3%	8.9%	8.0%	40.2%
Faculty of Social Sciences	Frequency	10	8	20	38
	% within Faculty	26.3%	21.1%	52.6%	100.0%
	% of Total	2.9%	2.3%	5.7%	10.9%
Faculty of Business Studies	Frequency	26	20	24	70
	% within Faculty	37.1%	28.6%	34.3%	100.0%
	% of Total	7.5%	5.7%	6.9%	20.1%
Faculty of Biological Sciences	Frequency	13	10	6	29
	% within Faculty	44.8%	34.5%	20.7%	100.0%
	% of Total	3.7%	2.9%	1.7%	8.3%
Faculty of Pharmacy	Frequency	17	7	12	36
	% within Faculty	47.2%	19.4%	33.3%	100.0%
	% of Total	4.9%	2.0%	3.4%	10.3%
Other faculties/institutions	Frequency	10	16	9	35
	% within Faculty	28.6%	45.7%	25.7%	100.0%
	% of Total	2.9%	4.5%	2.6%	10.0%
Total	Frequency	157	92	99	348
	% within Faculty	45.1%	26.4%	28.4%	100.0%
	% of Total	45.1%	26.4%	28.4%	100.0%

		Disable Bluetooth			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	63	47	30	140
	% within Faculty	45.0%	33.6%	21.4%	100.0%
	% of Total	18.1%	13.5%	8.6%	40.2%
Faculty of Social Sciences	Frequency	17	9	12	38
	% within Faculty	44.7%	23.7%	31.6%	100.0%
	% of Total	4.9%	2.6%	3.4%	10.9%
Faculty of Business Studies	Frequency	45	11	14	70
	% within Faculty	64.3%	15.7%	20.0%	100.0%
	% of Total	12.9%	3.2%	4.0%	20.1%
Faculty of Biological Sciences	Frequency	18	9	2	29
	% within Faculty	62.1%	31.0%	6.9%	100.0%
	% of Total	5.2%	2.6%	.6%	8.3%
Faculty of Pharmacy	Frequency	12	14	10	36
	% within Faculty	33.3%	38.9%	27.8%	100.0%
	% of Total	3.4%	4.0%	2.9%	10.3%
Other faculties/institutions	Frequency	16	11	8	35
	% within Faculty	45.7%	31.4%	22.9%	100.0%
	% of Total	4.6%	3.2%	2.2%	10.0%
Total	Frequency	171	101	76	348
	% within Faculty	49.1%	29.0%	21.8%	100.0%
	% of Total	49.1%	29.0%	21.8%	100.0%
		Modify privacy settings of the device			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	53	63	24	140
	% within Faculty	37.9%	45.0%	17.1%	100.0%
	% of Total	15.2%	18.1%	6.9%	40.2%
Faculty of Social Sciences	Frequency	16	12	10	38
	% within Faculty	42.1%	31.6%	26.3%	100.0%
	% of Total	4.6%	3.4%	2.9%	10.9%
Faculty of Business Studies	Frequency	38	16	16	70
	% within Faculty	54.3%	22.9%	22.9%	100.0%
	% of Total	10.9%	4.6%	4.6%	20.1%
Faculty of Biological Sciences	Frequency	19	6	4	29
	% within Faculty	65.5%	20.7%	13.8%	100.0%
	% of Total	5.5%	1.7%	1.1%	8.3%
Faculty of Pharmacy	Frequency	12	18	6	36
	% within Faculty	33.3%	50.0%	16.7%	100.0%
	% of Total	3.4%	5.2%	1.7%	10.3%
Other faculties/institutions	Frequency	14	12	9	35
	% within Faculty	40%	34.3%	25.7%	100.0%
	% of Total	4.0%	3.4%	2.6%	10.0%
Total	Frequency	152	127	69	348
	% within Faculty	43.7%	36.5%	19.8%	100.0%
	% of Total	43.7%	36.5%	19.8%	100.0%

Table- 5: *University of Dhaka (n=348), comparison of students' information security behaviours by Gender in terms of disaster recovery*

		Data backup			Total
		Always	Sometimes	Never	
Male	Frequency	152	51	43	246
	% within Gender	61.8%	20.7%	17.5%	100.0%
	% of Total	43.7%	14.7%	12.4%	70.7%
Female	Frequency	47	34	21	102
	% within Gender	46.1%	33.3%	20.6%	100.0%
	% of Total	13.5%	9.8%	6.0%	29.3%
Total	Frequency	199	85	64	348
	% within Gender	57.2%	24.4%	18.4%	100.0%
	% of Total	57.2%	24.4%	18.4%	100.0%
		Take out insurance			
		Always	Sometimes	Never	
Male	Frequency	32	56	158	246
	% within Gender	13.0%	22.8%	64.2%	100.0%
	% of Total	9.2%	16.1%	45.4%	70.7%
Female	Frequency	12	12	78	102
	% within Gender	11.8%	11.8%	76.5%	100.0%
	% of Total	3.4%	3.4%	22.4%	29.3%
Total	Frequency	44	68	236	348
	% within Gender	12.6%	19.5%	67.8%	100.0%
	% of Total	12.6%	19.5%	67.8%	100.0%

Table- 6: *University of Dhaka (n=348), comparison of students' information security behaviours by Faculties/Institutions in terms of disaster recovery*

		Data backup			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	82	40	18	140
	% within Faculty	58.6%	28.6%	12.9%	100.0%
	% of Total	23.6%	11.5%	5.2%	40.2%
Faculty of Social Sciences	Frequency	7	15	16	38
	% within Faculty	18.4%	39.5%	42.1%	100.0%
	% of Total	2.0%	4.3%	4.6%	10.9%
Faculty of Business Studies	Frequency	53	7	10	70
	% within Faculty	75.7%	10.0%	14.3%	100.0%
	% of Total	15.2%	2.0%	2.9%	20.1%
Faculty of Biological Sciences	Frequency	13	12	4	29
	% within Faculty	44.8%	41.4%	13.8%	100.0%
	% of Total	3.7%	3.4%	1.1%	8.3%
Faculty of Pharmacy	Frequency	19	7	10	36
	% within Faculty	52.8%	19.4%	27.8%	100.0%
	% of Total	5.5%	2.0%	2.9%	10.3%
Other faculties/institutions	Frequency	25	4	6	35
	% within Faculty	71.4%	11.4%	17.2%	100.0%
	% of Total	7.2%	1.1%	1.7%	10.0%
Total	Frequency	199	85	64	348
	% within Faculty	57.2%	24.4%	18.4%	100.0%
	% of Total	57.2%	24.4%	18.4%	100.0%
		Data wiping out upon disposal			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	17	65	58	140
	% within Faculty	12.1%	46.4%	41.4%	100.0%
	% of Total	4.9%	18.7%	16.7%	40.2%
Faculty of Social Sciences	Frequency	0	12	26	38
	% within Faculty	.0%	31.6%	68.4%	100.0%
	% of Total	.0%	3.4%	7.5%	10.9%
Faculty of Business Studies	Frequency	10	28	32	70
	% within Faculty	14.3%	40.0%	45.7%	100.0%
	% of Total	2.9%	8.0%	9.2%	20.1%
Faculty of Biological Sciences	Frequency	12	7	10	29
	% within Faculty	41.4%	24.1%	34.5%	100.0%
	% of Total	3.4%	2.0%	2.9%	8.3%
Faculty of Pharmacy	Frequency	3	16	17	36
	% within Faculty	8.3%	44.4%	47.2%	100.0%
	% of Total	.9%	4.6%	4.9%	10.3%
Other faculties/institutions	Frequency	9	14	12	35
	% within Faculty	25.7%	40%	34.3%	100.0%
	% of Total	2.6%	4.0%	3.4%	10.0%
Total	Frequency	51	142	155	348
	% within Faculty	14.7%	40.8%	44.5%	100.0%
	% of Total	14.7%	40.8%	44.5%	100.0%

		Blocking the device after losing it			Total
		Always	Sometimes	Never	
Faculty of Arts	Frequency	46	48	46	140
	% within Faculty	32.9%	34.3%	32.9%	100.0%
	% of Total	13.2%	13.8%	13.2%	40.2%
Faculty of Social Sciences	Frequency	6	13	19	38
	% within Faculty	15.8%	34.2%	50.0%	100.0%
	% of Total	1.7%	3.7%	5.5%	10.9%
Faculty of Business Studies	Frequency	27	13	30	70
	% within Faculty	38.6%	18.6%	42.9%	100.0%
	% of Total	7.8%	3.7%	8.6%	20.1%
Faculty of Biological Sciences	Frequency	12	5	12	29
	% within Faculty	41.4%	17.2%	41.4%	100.0%
	% of Total	3.4%	1.4%	3.4%	8.3%
Faculty of Pharmacy	Frequency	11	10	15	36
	% within Faculty	30.6%	27.8%	41.7%	100.0%
	% of Total	3.2%	2.9%	4.3%	10.3%
Other faculties/institutions	Frequency	12	11	12	35
	% within Faculty	34.3%	31.4%	34.3%	100.0%
	% of Total	3.4%	3.2%	3.4%	10.0%
Total	Frequency	114	100	134	348
	% within Faculty	32.8%	28.7%	38.5%	100.0%
	% of Total	32.8%	28.7%	38.5%	100.0%