INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Mobile Communications

ISSN online: 1741-5217 - ISSN print: 1470-949X
https://www.inderscience.com/ijmc

Digital divide and socio-economic differences in smartphone information security behaviour among university students: empirical evidence from Pakistan

Naurin Farooq Khan, Naveed Ikram, Sumera Saleem

DOI: 10.1504/IJMC.2023.10042359

Article History:
Received: 11 October 2020
Accepted: 15 June 2021
Published online: 04 July 2023

Digital divide and socio-economic differences in smartphone information security behaviour among university students: empirical evidence from Pakistan

Naurin Farooq Khan*, Naveed Ikram and Sumera Saleem

Riphah International University,
Main Campus, I-14, Islamabad, Pakistan
Email: naurin.zamir@riphah.edu.pk
Email: naveed.ikram@riphah.edu.pk
Email: sumera.saleem@riphah.edu.pk
*Corresponding author

Abstract: Protection of smartphone devices is a capital-enhancing activity that is rooted in the safe and secure use of these devices. However, the socio-economic and digital disparities affect such protective behaviour – specifically in developing nations where such differences are rife. This study explores the information security behaviour of smartphone users through digital and socio-economic disparities along with demographic characteristics. A survey questionnaire was administered to 306 students in universities of Pakistan employing a stratified multi-stage sampling technique. Analysis was carried out using frequencies and Pearson's Chi-square statistics. The findings suggest that students show lax smartphone information security behaviour. Digital divide and socio-economic differences reveal that students with greater Internet access and higher socio-economic status exhibited better behaviour in using smartphone settings and disaster recovery mechanisms. The study provides relevant institutes and government departments with insights to develop interventions, strategies, policies and specific training programs to better users' information security behaviour.

Keywords: smartphone use; information security; digital divide; socio-economic status; developing countries; Pakistan.

Reference to this paper should be made as follows: Khan, N.F., Ikram, N. and Saleem, S. (2023) 'Digital divide and socio-economic differences in smartphone information security behaviour among university students: empirical evidence from Pakistan', *Int. J. Mobile Communications*, Vol. 22, No. 1, pp.1–24.

Biographical notes: Naurin Farooq Khan is a PhD scholar at Riphah International University. Her areas of interest are Information security, digital economy, and human aspect of information security.

Naveed Ikram is a Professor of Software Engineering and Associate Dean, Faculty of Computing at Riphah International University. He received his PhD in Software Engineering from University of Salford, United Kingdom. He has supervised many MS and PhD theses and is an editorial review member of many journals. His research interests are information systems, information security, requirements engineering and software development.

Sumera Saleem is a PhD scholar at Riphah International University. Her areas of interest are cyber bullying, cyber harassment and information security.

1 Introduction

Mobile technology has seen unprecedented growth over the past decade with 5.2 billion subscribers worldwide. Currently, with 3.8 billion mobile Internet users worldwide, an additional 1.2 billion are estimated to use the Internet by 2025 (GSMA | The Mobile Economy – The Mobile Economy, no date). This growth in Information and Communication Technologies (ICTs) especially mobile technology is seen as a major source of socio-economic activity and contributes towards the global economy with estimations of 5% contribution to global GDP in 2022 (GSMA | The Mobile Economy - The Mobile Economy, no date). Therefore, mobile technology is a major factor in the socio-economic development of nations ('The Mobile Economy Asia Pacific 2020', no date). The access to the Internet via mobile technologies is a boon for individuals to maintain virtual communications, hence resulting in increased access to resources and opportunities. Students' dependency on mobile technology (Crompton et al., 2016; Pimmer et al., 2016) to get access to educational resources is on the rise. Educational organisations especially tertiary institutes adopt smartphones for academic activities (Arain et al., 2018) due to their widespread use. The ease of use and convenience allows the students to learn inside and outside the classrooms (Sung et al., 2016). Specifically, amidst the COVID-19 pandemic, the online continuation of academic activities (Bao, 2020) has increased mobile usage.

Smartphones have a great impact on individuals – both positive as well as negative. One example is easy access to help, which enhances an individual's perception of personal security (Ling et al., 2006) which is known as the capital-enhancing consequences of the Internet (van Ingen and Matzat, 2018). At the same time, there are cyber-security and privacy concerns associated with smartphone devices (Zhou et al., 2014). The cyber-crimes using smartphones have also grown exponentially (Abawajy et al., 2018; Yan and Yan, 2018) and are disavowing the positive impacts of mobile technology. These cyber-crimes include identity theft, ransomware attacks and financial frauds to name a few (Butler, 2020). The financial costs associated with these cyber-crimes are estimated to be the USA $ 600 trillion in 2020 (Lallie et al., 2021) and they disrupt the economic development of the nations. Tertiary institutes are the least secure environment therefore smartphone devices need to be protected against cyber-crimes (Botha et al., 2009) and the responsibility of such protection lies with the user (Tu et al., 2014). Increased use of smartphones especially among students mandates that they protect themselves from cyber-attacks (B. Kim, 2014) in order to fully exploit the capital-enhancing activities on the Internet. Students should possess smartphone security self-efficacy (Tu et al., 2014) - such as password protection and creating back up to name just a few security practices - in order to protect their devices.

The information security behaviour of smartphone users is also influenced by digital and socio-economic disparities just like other behaviour (Van Dijk, 2005). Despite the growth of ICTs and the opportunities that they provide to individuals, it should be noted that such technologies are not disseminated in society in a balanced way (Lal, 2017). This

results in a digital divide in which accessibility of ICTs is stratified across different socio-economic classes (Cik et al., 2018). The digital and socio-economic disparities tend to affect developing countries mostly due to a lack of technical and financial constraints (Abascal et al., 2016). This is specifically the case where the increased unemployment is rife and digital labour platforms are used as the main source of income alternatively (Berg, 2015). Pakistan being a developing nation has a high Internet penetration. With 76% of the mobile connection penetration, it is one of the leading nations in the Asia Pacific in mobile uptake ('The Mobile Economy Asia Pacific 2020', no date). Almost 50% of the country's population currently possess smartphones with the majority being youngsters. Moreover, the country is the fourth largest digital economy, the growth of which is fuelled by the young population (Masood et al., no date). Mobile technology has provided its fair share in this digital socio-economic development in Pakistan ('The Mobile Economy Asia Pacific 2020', no date). At the same time, due to socio-political and hostile regional settings, it faces increased cyber-threats (Shad, 2019) that have the potential to disrupt this development. Smartphone Information security is a capital-enhancing consequence of the use of ICTs and necessitates the safe, secure and responsible use of these devices. For individuals belonging to socially disadvantaged countries with growing digital economy such as Pakistan, safe and secure access to online opportunities is vital. With this backdrop, this study aims to quantitatively explore the smartphone information security behaviours of students enrolled in tertiary institutes in Pakistan. Moreover, the difference in information security behaviour due to digital and social disparities necessitates the understanding of smartphone information security behaviours with respect to the digital divide and socio-economic status of students along with demographics. The following research questions are posed:

RQ1 What are the current smartphone information security practices and behaviours of students enrolled in tertiary institutes of Pakistan?

RQ2 Is there a difference in the smartphone information security practices and behaviours of students in terms of gender, age, socio-economic status and digital divide?

2 Related work

The literature on smartphone information security establishes the protection of smartphones to be a multidimensional problem containing technical as well as behavioural aspects (Alsaleh et al., 2017). Most of the literature has been dedicated to the technical aspect of smartphone information security (BalaGanesh et al., 2018; Eppler and Wang, 2018) with recent attention given to the human aspect. The behavioural literature on smartphone information security is mostly from organisational (Brodin and Rose, 2020; Palanisamy et al., 2020), app developer and general user perspective (Butler, 2020). Nevertheless, there is a dearth of studies in the context of smartphone users' security behaviour (McGill and Thompson, 2017). The importance of users' information security behaviour is argued by many (Tamrin et al., 2017) since they are deemed to be responsible for ensuring their devices are protected against unwanted threats.

2.1 Theoretical background

The stratification model of diffusion of technologies states that countries with pre-existing digital and socio-economic advantage will maintain their edge in the digital economy despite the increase in the take-up of digital platforms (Van Dijk, 2005; Van Deursen et al., 2017). This means that countries that were late adopters of ICTs and are developing will experience impediments in Internet access resources and social capital that is derived from such activities. The digital divide theory posits that once individuals cross the access divide threshold, differences still exit that are associated with Internet usage (Van Dijk, 2005). It influences the online welfare of individuals (Van Deursen et al., 2017) and affects their online behaviour. Similarly, the socio-economic disparities are associated with the technical skills of the individuals (Robinson et al., 2015) such as information security behaviour. Many studies report that individuals who access the Internet more frequently and users who belong to higher socio-economic status benefit from the Internet more and possess higher ICTs skills (Livingstone and Helsper, 2010). This includes the information security practices of smartphones which are affected by digital and social stratification. Therefore, the study of information security in terms of capital enhancing activity is affected by digital and social stratification just like any other social behaviour. In the next subsections, the relevant literature is discussed in the context of developing and developed nations followed by the limitations of the previous work and the present study.

2.2 Smartphone security in developed countries

Few studies have contributed towards understanding the smartphone information security users' behaviour in developed countries. One of the earlier studies conducted in the USA by (Harris et al., 2014) examined the information security preparedness of university students and IT professionals. The survey of 310 responses revealed that both students, as well as professionals, did not adopt adequate measures to secure their smartphones. The study (Jones and Heinrichs, 2012) administered an online survey at a regional university in the USA. The findings from 205 responses indicated insecure smartphone behaviour with a majority of the students not practicing usage of anti-virus software, encryption and data backup/cleaning before disposing-off their smartphone. An updated evaluation of students in the same university by the authors (Jones and Chin, 2015) was carried out in the subsequent year to compare and understand the information security behaviours over time. The survey results extracted from 218 undergraduate students indicated alarming decreased information security behaviours using their smartphones. The students exhibited an increase in opening multimedia attachments from an unknown source, inability to log off from social networking sites/email and downloading apps that requested access to personal information. In another study (Chin et al., 2020), another updated evaluation of smartphone behaviours was carried out. The results from 309 respondents indicated that although the students showed a high degree of proficiency in some areas of smartphone information security, they lacked good information security practices in others. An online survey containing 210 responses (Breitinger et al., 2020) was mounted online to understand the information security behaviours of general users using their desktop computers and smartphones. Users exhibited less secure behaviour while using their smartphones compared to computers. Similarly, (Stylios et al., 2016) conducted a study on 204 participants from a university in Greece. The findings showed

that the majority of the respondents stored bank PINs and sensitive data on their smartphones and seldom changed passwords. Another study (Das and Khan, 2016) measured the six-smartphone information security behaviour of 500 participants from Qatar using a face-to-face survey. The findings from the study suggested a lack of security concerns about malware/data leakage.

2.3 Smartphone security behaviour in developing countries

With most of the literature on smartphone information security behaviour carried out in developed countries, there are few studies conducted in the developing nations. A study (Zhang et al., 2017) gauged the smartphone information security practices of 341 Chinese participants via an online survey. The results showed low-security behaviour in terms of avoiding harmful behaviour with a majority of the participants downloading apps from untrusted sources, failing to update smartphone apps, connecting to insecure Wi-Fi and data backup/erasure. Similarly, (Nowrin and Bawden, 2018) surveyed 356 students from a large public university in Bangladesh to explore smartphone information security practices. The survey revealed that half of the students did not adopt secure use of smartphone settings and add-on utilities and failed to take adequate measures such as wiping data before disposal. Recently, (Shah and Agarwal, 2020) measured the smartphone information security practices of 300 general users from India via an online survey. The results indicated that the majority of the users adopted popular security features such as screen locks but showed insecure practices of installing apps from untrusted sources, connecting to free Wi-Fi. Other notable mentions include the evaluation of partial smartphone information security behaviours of participants. In Sari (2014), a survey was carried out on 106 general users from Indonesia to find their knowledge, awareness and behaviour of smartphone information security. Out of five areas, users showed low-security behaviour in reading security policies, installing anti-virus, and reporting the security incidents of fraud and spam to the telecommunication operators. The summary of the related work is presented in Table 1.

2.4 Socio-economic and digital disparities and information security behaviour

Although literature exhibits smartphone-security empirical evidence, few limitations hinder the study of the phenomenon. Digital inequalities and socio-economic status have not been addressed in understanding smartphone information security behaviour. Demographic characteristics such as gender and age have been studied to explain smartphone information security behaviours by many studies (Jones and Chin, 2015; Zhang et al., 2017; Breitinger et al., 2020; Chin et al., 2020; Shah and Agarwal, 2020) as shown in Table 1. Literature on general information security literature shows socio-economic and digital divide to be influencing factors in the information security behaviours. The users who are more digitally connected exhibit more information security knowledge and practices gathered through the usage of the Internet (Dodel and Mesch, 2018). Similarly, socio-economic inequalities are also related to information security disparities (Dodel and Mesch, 2017). Users with higher socio-economic status exhibit better information security behaviour in Israel. A study from the UK yields lower information security behaviour of using security software by lower socio-economic groups (McGuire and Dowling, 2013). However, there is a lack of evidence with respect to digital and socio-economic disparities.

Table 1 Summary of the related work

Study	*Sample demographics*	*Variables used*
Developed countries		
Harris et al. (2014), USA	University student and IT professionals, online survey, 3 universities	Frequency analysis
Jones and Chin (2015), USA	University students, 1 university	Frequency analysis, gender and age
Chin et al. (2020), USA	University students, face-to-face survey, 1 university,	Frequency analysis, gender
Breitinger et al. (2020)	General participants, online survey	Frequency analysis, mobile Operating System, familiarity of security, desktop and phone
Stylios et al. (2016), Greece	General participants	Frequency analysis, age and gender
Das and Khan (2016), Qatar	General participants	Gender, age, mobile Operating System,
Developing countries		
Sari (2014), Indonesia	General participants	Frequency analysis
Zhang et al. (2017), China	General participants	Frequency analysis, gender, education, occupation
Nowrin and Bawden (2018), Bangladesh	University students, 1 university	Frequency analysis, gender, age, department
Shah and Agarwal (2020), India	General participants, online survey	Frequency analysis, gender, age, mobile OS, mother tongue
This study	University students, face to face survey, 6 universities	Gender, age, language, IT /non-IT department, socio-economic status, frequency of Internet access, quality of Internet access

While these studies provide evidence of socio-economic status and digital divide variables in the context of general information security behaviour, no study comprehensively focuses on smartphone security behaviour differences. Moreover, as identified earlier, the socio-economic and digital divide disparities are not being studied in the smartphone information security behaviours. This study reports on closing this gap in information security literature by carrying out a survey in a developing country's context and extends previous work by including digital divide and socio-economic status variables along with other demographic characteristics.

3 Method

3.1 Data collection

The survey method was employed using face-to-face interaction and a pencil and paper approach. The survey questions were taken from (Jones and Chin, 2015; Chin et al., 2020). The questions are arranged into three main categories that is:

1 avoid harmful behaviour and attitude

2 protections through settings and add-on utilities

3 prepare for disaster recovery.

A multistage stratified random sampling was used (Jain and Hausman 2006) which is a viable choice for conducive representation of the population and reduces sample size (Shi, 2015). At the first stage, one province in Pakistan was selected and its cities were stratified in poverty strata as per the multidimensional poverty index (MPI) (Multidimensional Poverty in Pakistan, no date). At the second stage, universities recognised by the higher education commission of the country were identified in these cities. At stage three, one university was chosen from each poverty stratum randomly. At stage four, students were randomly selected from each university. A total of 328 students filled the questionnaire out of which a minimum of 306 responses was used for analysis after cleaning the data.

3.2 Measures

In demographics, gender and age were dichotomous variables, whereas language spoken at home is coded as categorical with 1 for national, 2 for local and 3 for multiple. The department variable is also dichotomous with 0 representing students pursuing non-IT-related degrees and 1 representing students enrolled in IT-related degrees. For socio-economic status, the variables are urban/rural (dichotomous) and poverty strata. The poverty strata variable is coded as ordinal. The digital divide is presented with two variables in terms of quality of Internet access coded as 1 for access from home, 2 for access from university/friends/family and 3 for access from multiple places. The other variable frequency of Internet access is dichotomous with 1 for multiple times a day and 0 for once a day. The following hypotheses are framed with respect to demographics, socio-economic status and the digital divide.

3.3 Hypothesis

3.3.1 Demographic-based hypotheses

Gender

Research on gender studies exhibits that female are not very confident in the technicalities of their smartphones hence they are not proficient in smartphone settings and add-on utilities (Jones and Chin, 2015). Similarly, other studies report that they tend to use public Wi-Fi (Jones and Heinrichs, 2012). Moreover, the research in computer security reveals that females are less confident in their computer usage (He and Freeman, 2019) and suffered from computer anxiety that culminates itself in differences in computer attitude and behaviours (Cooper, 2006). Therefore, our hypothesis is

H1 Females are less likely to adopt phone settings and add-on utilities and prepare for disaster recovery.

On the other hand, smartphone information security behaviour in the context of using emails, social networking sites and downloading apps is less technical in nature. Nevertheless, their unsafe use entails riskier behaviour such as opening attachments and

downloading apps from sources that can't be trusted. Males have been found to exhibit riskier behaviour when it comes to such unsafe smartphone practices (Jones and Heinrichs, 2012). A comprehensive review of the literature (Eckel and Grossman, 2008), established that males mostly engaged in riskier behaviours compared to females generally. Therefore, we posit that

H2 Females will demonstrate secure behaviours by avoiding harmful behaviour and practices of smartphones.

Age

Younger adults are brought up using technology in their everyday life (Padilla-MeléNdez et al., 2013) which mediates their attitude of expectancy and acceptance toward it. Due to their increased online presence and their acceptance of technology, they have greater information security concerns than older people (Blank et al., 2014). Therefore, we posit that younger adults are more likely to adopt security measures.

H3 Students aged 18–20 are more likely to adopt phone settings and add-on utilities than users aged 21 and above.

H4 Younger students will demonstrate secure behaviour by avoiding harmful behaviour and practices of the smartphone.

Degree

Previous studies have found that smartphone security behaviours significantly differ with respect to the degree that the students are pursuing (Nowrin and Bawden, 2018). Therefore, we posit that

H5 The type of degree that students are pursuing will have an association with smartphone information security behaviours.

Language

Research has established certain smartphone information security behaviours such as locking smartphones to be used less likely by the participants from Asia (Sawaya et al., 2017). Other studies have found that the native languages and the ethnic background of participants influence the adoption of secure mechanisms (Parker et al., 2015). Similarly, (Shah and Agarwal, 2020) found that the mother tongue had an association with certain smartphone information security behaviours positively while negatively with others. We posit the following hypothesis:

H6 The languages spoken at home will have an association with smartphone information security behaviours.

3.3.2 Socio-economic status-based hypotheses

Socio-economic status has been associated with information security behaviours of individuals. The studies (McGuire and Dowling, 2013; Dodel and Mesch, 2017) found that lower socio-economic status and educational level influenced less secure cyber-practices of the individuals. Similarly, a study by (Dodel and Mesch, 2018) reveals that

socio-economic status had a strong effect on an individual's information security skills and information security behaviours. In a study (Dodel and Mesch, 2019), socio-economic status has a direct effect on information security behaviours such as installing anti-virus and password safety. Therefore, we posit that

H7 The students belonging to rural areas will less likely to adopt smartphone information security behaviours.

H8 The students belonging to areas of low poverty will more likely to adopt smartphone information security behaviours.

3.3.3 Digital divide-based hypotheses

There is limited research carried out to see digital divide differences on information security and smartphone information security behaviour. In (Büchi et al., 2017), the participants who were disadvantaged in terms of Internet usage were vulnerable to cyber-threats. Similarly, a study by (Reyns et al., 2016) revealed that the role of Internet attributes is associated with cyber-preventive behaviours. In (Dodel and Mesch, 2018), it was established that there is an indirect relationship between quality of Internet access and anti-virus behaviour. The digital divide is associated directly with participants' digital security skills which in turn is associated with anti-virus behaviours. The frequency of Internet use by the participants is found to be related to the information security behaviour of passwords and instalments of anti-virus (Dodel and Mesch, 2019). The study finds that the higher the frequency of Internet use, the more the participants' engagement in information security behaviours. Based on the studies in the information security behaviour of the computer, we posit the hypotheses on digital divide variables as follows:

H9 The students who access the Internet less frequently will less likely to adopt smartphone information security behaviours.

H10 The students who access the Internet from multiple places will more likely to adopt smartphone information security behaviours.

4 Result and analysis

This section answers our research questions RQ1 and RQ2. Responses were analysed using SPSS statistical V. 21 software. Descriptive analysis included frequencies and categorical analysis was carried out using Pearson's Chi-square. The significance level of 0.05 is used in this study based on previous studies. Post hoc analysis was conducted using Bonferroni correction. The frequency of demographic, socio-economic and digital divide variables is present in Table 2.

4.1 Avoiding harmful behaviour and attitude

To fully exploit the Internet without falling victim to cyber-crimes, users are required to avoid harmful behaviour while using smartphones. There are seven secure practices in this category as shown in Figure 1. Failing to adopt these, users can fall victims to phishing in which sensitive information is extracted by enticing them to click on links

(Arachchilage and Love, 2014). These links are usually emailed or texted to users and the sender is from an unknown source. Similarly, malware attacks are exacerbated by users clicking on links and downloading apps from unknown sources.

Table 2 Variables and frequencies

Variables		*Frequency*	*%*
Gender	Male	167	54.6
	Female	139	45.4
Age	18–20 years	174	56.9
	21 and above	132	43.1
Department	IT-related degree	199	40
	Non-IT-related degree	184	60
Language	National	97	31.7
	Local	182	59.5
	Multiple languages	27	8.8
Urban/rural	Urban	132	44
	Rural	174	57
Poverty strata	Less than 10%	33	10
	20–29.9%	35	11.4
	30–39.9%	59	19.3
	40–49.9%	40	13.1
	50–59.9%	109	35.6
	60–69.9%	30	9.8
Quality of internet access	Home	166	54.2
	University/friends/family	69	22.5
	Multiple places	71	23.2
Frequency of internet access	Multiple times a day	267	87
	Once a day	39	13

A total of 59% of students responded that they opened multimedia attachments from unknown sources as shown in Figure 1. Almost 46% admitted that they have clicked on website links received via email from unknown sources. This behaviour showed that the majority of the students were engaged in harmful behaviour and attitude that puts them at risk of phishing as well as malware attacks. A further look into the frequency analysis reveals that almost 23.5% of students always/often opened attachments whereas 14.3% always/often click on the links received from unknown sources. A total of 57% had downloaded apps from sources which they could not trust and gave apps permissions to access their personal information. Such high percentages of students engaged in downloading apps from an unknown source and granting excessive permissions is concerning since such apps cannot be trusted for their legitimacy and security (Jones and Chin, 2015). Users can unknowingly install malware that can hamper the security and privacy of their smartphones. Almost 44% of the students said that they never disconnected from email/social networks when they finished using them. This behaviour which may be attributed to the convenience of the user is harmful and it increases the risk

of information loss in case smartphone gets stolen (Zhang et al., 2017). Comparatively, a small number of students (18%) failed to check for updates on their smartphones. Constant updates are necessary to avoid malware attacks and other security incidents (Harris et al., 2014).

Figure 1 Avoiding harmful behaviour and protection though settings

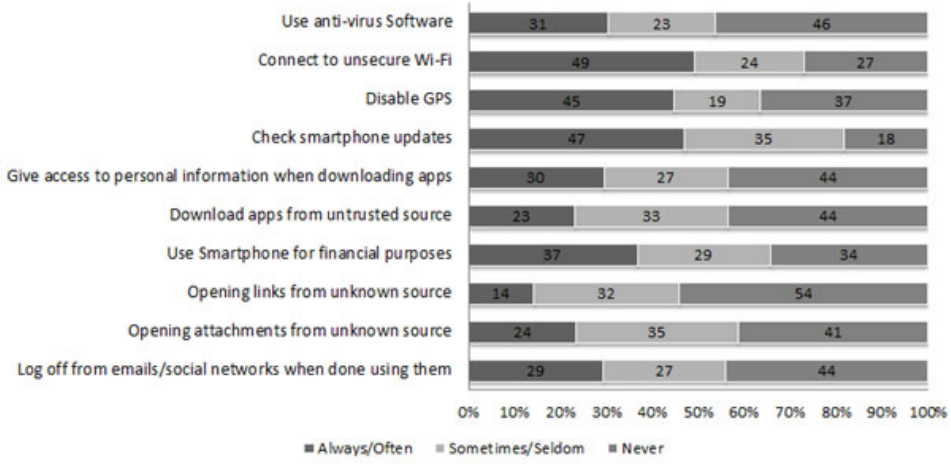
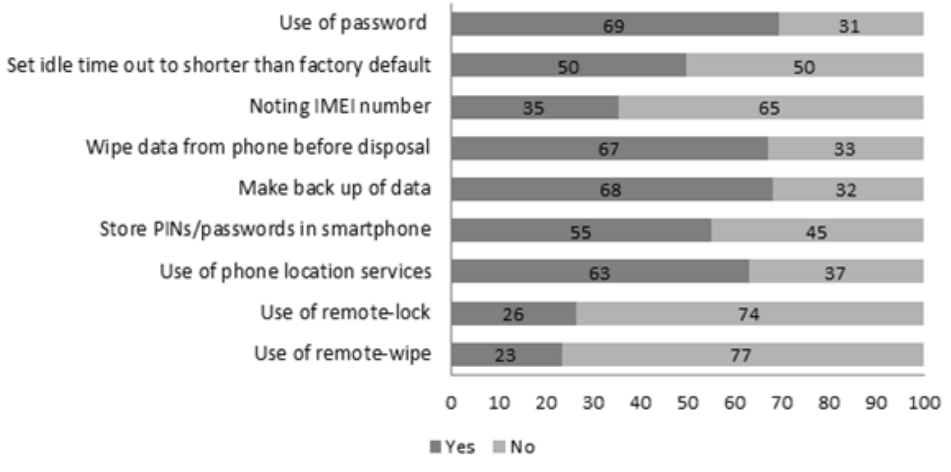


Figure 2 Prepare for disaster recovery



4.2 Protection through settings and add-on utilities

Protection through smartphone settings includes the use of a password, disabling global positioning system (GPS), using anti-virus programs, idle time out settings and connecting to password-protected Wi-Fi networks. Students using protective settings were comparatively better than avoiding harmful behaviour. Only 30% of them did not use a password to lock their smartphones as shown in Figure 2. A total of 50.2% of them had not reset the shorter idle time out than the factory default (Figure 2). These settings

allow the user to keep their smartphone data safe from unauthorised access (Imgraben et al., 2014) since password protection mechanism is considered the first line of defence in smartphone information security. The use of anti-virus software is adopted by a few of the students (30.5%) with only 46.3% claiming that they had never used the software for scanning their smartphones. The GPS is disabled when not in use by a majority of the students, 44.8% saying they always practice it, 18.7% sometimes practice it whereas 36.5% never turn off GPS when not in use. Keeping the GPS on all the time puts the users at the risk of being tracked by others. A total 49.2% of students always/often connected to a password-protected Wi-Fi as shown in figure 1. On the other hand, a vast majority of them have seldom (23.28%) and never (27%) used encrypted Wi-Fi. Free Wi-Fi is offered in many places and it is not always secure. Participants using them can fall victim to man-in-the-middle attacks. Cyber-criminals can sniff data and information transmitted over unsecured Wi-Fi (Imgraben et al., 2014).

4.3 Prepare for disaster recovery

Smartphones can get lost or are disposed of as a result of which sensitive data and information can be compromised. The preparation for such incidents involves backing up of data, knowing international mobile equipment identity (IMEI) number of smartphones, using remote-wipe, remote-lock, phone location features and wipe clean the smartphone before disposal as shown in figure 2.

A majority of students lacked preparedness in case of a disaster. A large number of them (77%) did not use the remote-wipe feature and (74%) failed to use the remote-lock feature. But on the other hand, a small percentage (almost 37%) did not use phone location services. A large number of the students (64.8%) did not record their smartphone IMEI number which is beneficial in reporting the theft of the device. Almost half of the students (54.9%) stored PINs/passwords in their smartphones for further reference. It can be dangerous since sensitive information can be exploited to gain access to bank accounts, emails, etc. in case of phone loss. On the other hand, a small percentage of the students (33%) did not wipe their smartphone clean before disposing it off and 32% failed to back up data on their smartphone. Such measures of wiping data before disposal, using remote-lock/wipe features, phone location services are important in avoiding vulnerabilities of sensitive data loss.

4.4 Categorical analysis

We used the Pearson's Chi-square test to find an association between demographic, socio-economic, digital divide variables and smartphone information security behaviours. Table3. presents the significant results and Chi-square test statistics.

4.4.1 Demographic characteristics

Gender. We found three significant differences between smartphone information security behaviours and gender, two in disaster preparedness and one in avoiding harmful behaviour and attitude. Females who did not use remote-lock and remote-wipe features of smartphones were comparatively more than those who used them. Therefore, females showed less secure smartphone behaviour in prepare for disaster recovery. Hence H1 is supported. A post hoc analysis with Bonferroni correction showed that in avoiding

harmful behaviour females exhibited good smartphone information security in not granting access to personal information while downloading apps, therefore H2 is also supported.

Age. We found two significant differences between age and smartphone information security behaviours. Younger students aged 18–20 showed good smartphone information security behaviour in refraining to download apps from untrusted sources as well as in granting access to personal information to these apps. Younger students avoided harmful behaviour and attitude than older ones, hence H4 is supported. No significant differences were found in protection through smartphone settings therefore, H3 is not supported.

Department. We found five significant differences between students who were pursuing IT-related degree and smartphone information security behaviours. Three of these differences were in prepare for disaster recovery. The students who were pursuing non-IT-related who used remote wipe, remote lock features and noted IMEI were comparatively more than those who did not. Two differences were in avoiding harmful behaviour and attitude. A post hoc test with Bonferroni correction revealed that student pursuing non-IT-related degree showed better security by never downloading apps from untrusted sources and granting access to personal information. Therefore, H5 is supported.

Language. A total of four significant differences were found between language variable and smartphone information security behaviour. Three of these differences were in prepare for disaster recovery and one in protection through settings and add-on utilities. A post hoc with Bonferroni correction revealed that students who spoke multiple languages at home showed more secure smartphone information security behaviours in setting Idle time out to shorter than the factory default and in giving access of personal information to downloaded apps. Those who spoke multiple languages were less apt in adopting remote-wipe features. Those who spoke only the local language showed less secure smartphone information security behaviour by failing to note IMEI number and setting idle time out to shorter than the factory default. Therefore, H6 is supported.

4.4.2 Socio-economic status

Urban/rural. Three significant differences were found between smartphone information security behaviour and urban/rural variables. Students belonging to urban areas used location services and noted the IMEI number of the smartphone, therefore, exhibiting better preparedness for disaster recovery. Similarly, urban area dwellers that set the idle time out to shorter than the factory default were comparatively greater than those who used default idle time out. Students from urban areas exhibited better smartphone information security in protection through setting add-on utilities. Hence H7 is supported.

Poverty strata. We found six significant differences between smartphone information security behaviour and the poverty level of the city from where the students belonged to. A post hoc Bonferroni correction revealed that students belonging from rich or less poor poverty strata showed secure smartphone behaviours such as never connecting to unsecured Wi-Fi, logging off after using email/social networks, disabling GPS when not in use, never downloading apps from untrusted sources and giving permissions to access personal information to downloaded apps. Hence students showed better smartphone information security in protection through add-on utilities as well as in avoiding harmful behaviour and attitude. However, students belonging to low poverty strata did not use

phone location services hence were not prepared well for disaster in case of smartphone loss or theft. Therefore, H8 is partially supported.

4.4.3 Digital divide

Frequency of Internet access. There were seven significant differences in smartphone information security and frequency of Internet access – three from protection through settings, three from avoiding harmful behaviour and attitude and one from disaster recovery. The results revealed that students who frequently accessed the Internet used phone location services, therefore, were more prepared for disaster recovery. Similarly, students accessing the Internet multiple times a day avoided harmful behaviour by setting the idle time out to shorter than factory default and using passwords. However, these students connected to unsecured Wi-Fi more frequently and carried out financial activities more regularly. On the other hand, a post hoc Bonferroni correction revealed that students who were digitally more connected avoided harmful behaviour and attitude by refraining from giving access to personal information to downloaded apps and frequently checking updates on their smartphones. Therefore, H9 is supported.

Quality of Internet access. We found nine significant differences in smartphone information security and quality of Internet access variables. There were three significant differences from each of the three smartphone information security categories. A post hoc Bonferroni correction revealed that students who accessed the Internet from multiple places used phone location services and made a backup of smartphone content comparatively more than those who did not. However, these students stored sensitive information such as PINs/passwords in their smartphones. Similarly, students who had access to multiple places were more apt in adopting smartphone add-on utilities when it comes to setting the idle time out to shorter than factory default and use of passwords. However, they adopted less secure behaviour by not disabling their GPS when not in use. In avoiding harmful behaviour and attitude, students who accessed the Internet from multiple places showed better protection of their smartphone by not opening attachments received from unknown sources and checking for updates. These students allowed access to personal information while downloading apps thereby showing less secure smartphone behaviour. Since the users who are digitally more connected exhibited more secure behaviour in six out of nine smartphone information security behaviours, H10 is partially supported.

5 Discussion

This study sheds light on the smartphone information security behaviour of university students from a developing country's perspective. The frequency analysis highlights low smartphone information security exhibited by the students. More than 50% of the users do not take measures to avoid harmful behaviour and attitudes. Opening of attachments and links and downloading apps from unknown/untrusted sources make them vulnerable to phishing attacks. The use of anti-virus software by less than 55% of the users makes them even more vulnerable to malware and ransomware attacks. Connecting to unsecured Wi-Fi leaves the students prone to man-in-the-middle attacks which can compromise their overall smartphone information security. Students have the worst smartphone information security when it comes to preparing for disaster recovery. More than 65% of

the students are ill prepared for scenarios where their smartphone gets lost or stolen. A vast majority of students not using remote-wipe/lock features, failing to back up data and noting the IMEI number of their smartphones. Failing to take these simple measures puts them at clear dangers of data loss, confidentiality and privacy breach especially when almost 30% do not use a password to lock their smartphones. These losses can even lead to sinister crimes such as financial frauds since more than 45% store PINs/passwords and account details of their banks. For females, it can lead to even more grave consequences such as being victims of blackmail. The sensitive data stored in smartphones includes pictures and videos which cyber-criminals can exploit to blackmail females in a tight culture as Pakistan's.

Demographic differences revealed that females are not prepared for disaster recovery in case their smartphone gets lost or stolen compared to males. These findings are similar to (Nowrin and Bawden, 2018) where males were more concerned about disaster recovery of their smartphones and used remote-lock/wipe features. The females are more apt in avoiding harmful behaviour and attitude while being concerned, and not granting access to personal information to downloaded apps. The findings are similar to (Zhang et al., 2017) but are contrary to (Shah and Agarwal, 2020) in which males showed good security practices in giving apps permissions. Similarly, younger students exhibited better smartphone information security by avoiding harmful behaviour and activities. They showed precaution in downloading apps from untrusted sources and allowing access to personal information. Our results are in contrast to (Das and Khan, 2016; Stylios et al., 2016; Shah and Agarwal, 2020) in which older users avoided harmful behaviour. But it should be noted that the older participants in those studies were above the age of 25 hence are wise in the use of technology. Our results are also in contrast to (Jones and Chin, 2015) in which no differences were found between users aged (18–20) and (21–25). The type of degree that students were pursuing affected their smartphone information security behaviours. Those who pursued IT-related degree did not show precautions in disaster recovery behaviours and were less secure by downloading apps from untrusted sites and giving excessive permissions to these apps. The findings are in line with (Nowrin and Bawden, 2018). Language spoken at home affected the smartphone information security behaviours of students in our study. Those who only spoke the local language at home were not prepared for disaster recovery by failing to note the IMEI number of their smartphones while those who spoke multiple languages at home were lax in the use of remote-wipe feature. The multilingual individuals showed more secure behaviour in setting idle time out to short than factory default and in avoiding giving excessive permissions to downloaded apps. These findings are in line with (Shah and Agarwal, 2020) where the mother tongue of the participants affected the information security behaviours of the participants.

Urban dwellers are associated with better socio-economic status and exhibited better smartphone information security by use of settings and add-on utilities, and disaster recovery. Similarly, users from low poverty strata were more apt in adopting smartphone settings and avoided harmful behaviour and activities. These findings are similar to (Dodel and Mesch, 2017) where participants from lower socio-economic groups showed lesser information security practices such as the use of anti-virus software.

Table 3 Categorical analysis

Smartphone information security behaviour	*Demographic*				*Socio-economic Status*		*Digital divide*	
	Gender	*Age*	*Degree*	*Language*	*Urban/rural*	*Poverty Strata*	*Frequency of internet access*	*Quality of internet access*
Avoiding harmful behaviour and attitude								
Log off from emails/social networks when done using them	NS	NS	NS	NS	NS	$\chi2(10) = 30.4$, $p = .001$	NS	NS
Opening attachments from unknown source	NS	NS	NS	NS	NS	NS	NS	$\chi2(4) = 20.5$, $p = .001$
Opening links from unknown source	NS	NS	NS	NS	NS	NS	NS	NS
Use Smartphone for Financial Purposes	NS	NS	NS	NS	NS	NS	$\chi2(2) = 10.6$, $p = .005$	NS
Download apps from untrusted source	NS	$\chi2(2) = 7.6$, $p = .02$	$\chi2(2) = 14.0$, $p = .001$	NS	NS	$\chi2(10) = 18.4$, $p = .04$	NS	NS
Give access to personal information when downloading apps	$\chi2(2) = 9.26$, $p = .01$	$\chi2(2) = 13.2$, $p = .001$	$\chi2(2) = 16.7$, $p = .000$	$\chi2(4) = 10.9$, $p = .02$	NS	$\chi2(10) = 41.9$, $p = .001$	$\chi2(2) = 8.7$, $p = .01$	$\chi2(4) = 24.3$, $p = .001$
Check smartphone updates	NS	NS	NS	NS	NS	NS	$\chi2(2) = 10.3$, $p = .006$	$\chi2(4) = 9.691$, $p = .04$
Protection through settings add-on utilities								
Disable GPS	NS	NS	NS	NS	NS	$\chi2(10) = 22.1$, $p = .01$	NS	$\chi2(4) = 12.2$, $p = .01$
Connect to unsecure Wi-Fi	NS	NS	NS	NS	NS	$\chi2(10) = 22.7$, $p = .01$	$\chi2(2) = 12.2$, $p = .002$	NS
Use anti-virus software	NS	NS	NS	NS	NS	NS	NS	NS
Set idle time out to shorter than factory default	NS	NS	NS	$\chi2(2) = 14.0$, $p = .001$	$\chi2(1) = 9.6$, $p = .002$	NS	$\chi2(1) = 16.0$, $p = .001$	$\chi2(2) = 28.0$, $p = .001$
Use of password	NS	NS	NS	NS	NS	NS	$\chi2(1) = 10.0$, $p = .001$	$\chi2(2) = 13.3$, $p = .001$

Note: NS stands for not significant

Table 3 Categorical analysis (continued)

	Demographic				*Socio-economic Status*		*Digital divide*	
	Gender	*Age*	*Degree*	*Language*	*Urban/rural*	*Poverty Strata*	*Frequency of internet access*	*Quality of internet access*
Prepare for disaster recovery								
Use of remote-wipe	$\chi2(1) = 6.08$, p = .01	NS	$\chi2(1) = 7.076$, p = .008	$\chi2(2) = 6.9$, p = .03	NS	NS	NS	NS
Use of remote-lock	$\chi2(1) = 5.05$, p = .02	NS	$\chi2(1) = 5.143$, p = .02	NS	NS	NS	NS	NS
Use of phone location services	NS	NS	NS	NS	$\chi2(1) = 6.32$, p = .01	$\chi2(5) = 17.0$, p = .004	$\chi2(1) = 9.70$, p = .002	$\chi2(2) = 19.1$, p = .001
Store PINs/password in smartphone	NS	NS	NS	NS	NS	NS	NS	$\chi2(2) = 10.6$, p = .005
Make back up of data	NS	NS	NS	NS	NS	NS	NS	$\chi2(2) = 8.09$, p = .01
Wipe data from smartphone before disposal	NS	NS	NS	NS	NS	NS	NS	NS
Noting IMEI number	NS	NS	$\chi2(1) = 8.86$, p = .003	$\chi2(2) = 8.25$, p = .01	$\chi2(1) = 4.48$, p = .03	NS	NS	NS

Note: NS stands for not significant

The digital divide in terms of quality and frequency of Internet access showed mixed results. Students having a lesser digital divide exhibited better security in disaster recovery and use of smartphone settings and add-on utilities. This includes setting idle time out to shorter than factory default, use of passwords, use of phone location services and backing up contents in their smartphones. Our findings are in line with (Dodel and Mesch, 2018) in which seniority of Internet access is an important determinant of both digital security skills and anti-virus behaviour. These findings are also similar to (Dodel and Mesch, 2019) in which the digital divide in terms of frequency of Internet access has a direct and indirect impact on the information security behaviours of password and anti-virus software usage.

Information security practices require digital knowledge and skills. The more a user accesses the Internet, the more he/she is to acquire those practices as well as knowledge and experience (Dodel and Mesch, 2018). Hence, the digital divide is associated with information security behaviours as well as smartphone behaviours. On the other hand, less secure smartphone behaviour for those who were digitally more connected was observed in a few of the practices such as connecting to unsecured Wi-Fi, use of financial purposes, storing PINs/passwords in smartphones, disabling GPS and allowing excessive permissions to apps. This unsecure behaviour can partly be explained by the fact that those who less frequently accessed the Internet do not get the chance to use a smartphone for financial purposes. Low mobile data levels are also associated with the use of insecure Wi-Fi (Sombatruang et al., 2019) which is more likely to be the case with students who less frequently access the Internet. On the other hand, storing PINs/passwords, not disabling GPS and allowing excessive access to downloaded apps were observed in students who accessed the Internet from multiple places. The reasons for such insecure behaviour from more digitally connected users can be the cost-benefits considerations and trust. The downloading of apps that required excessive permission is attributed to their trust in the app platforms (Bonné et al., 2017). Users trust that these platforms have already carried out anti-virus scans on the hosted apps and are therefore safe to download (Imgraben et al., 2014; Alsaleh et al., 2017). Moreover, the benefits of downloading free apps outweigh their concerns for security (Barth et al., 2019). Similarly, users are known to value convenience over security. The GPS being turned on even when not in use can be explained by the fact that privacy settings are considered a one-time set-it matter (Bonné et al., 2017). Users' constant update of such settings instils inconvenience and they do not adopt such practices. The storing of sensitive information on smartphones even by more digitally connected users is associated with the misconception that smartphone information security is dependent in their physical ability to control their smartphones (Serrano-Tellería, 2018).

6 Theoretical and practical implications

The empirical findings from our study contribute towards theory and application in safe and secure access to the cyber-space specifically the field of information security. From a theoretical aspect, we make a contribution by empirically evaluating the smartphone information security of students belonging to tertiary institutes in a developing country. To the best of our knowledge, this is the first study conducted that measures smartphone information security behaviour with respect to the digital divide and socio-economic status of the participants. This contributes towards capacity building – one of the five

criteria that measure a nation's information security commitment (Shad, 2019). Pakistan currently stands at the 66th position in the global cybersecurity index (GCI) and is still a maturing nation in its commitment to information security. The country seriously lacks attention, planning and interventions in information security capacity building (Shad, 2019) in order to provide its citizens access to capital-enhancing activities in the cyber-space.

From an application point of view, our work can identify smartphone information security areas that can be improved in terms of practices and consequent policies that can be adopted in tertiary institutes. First and foremost are the educational implications that require a smartphone information security education in universities. With a large number of youngsters contributing towards Pakistan's growing freelance economy (Payoneer | The Global Gig-Economy Index: Q2 2019, no date), they must be educated in the information security best practices of their devices including smartphones. Access to economic opportunity in the cyber-space entails self-efficacy in safe and secure usage of these devices. Development of educational models – to bring cultural change in universities, and smartphone education security apps – to instil constant awareness of the deviation from good security practices as argued in (Aharony et al., 2020). Moreover, understanding current information security practices and targeted educational programs will contribute towards cyber-securitisation of the country increasing its GCI among other nations and consequently securing access of the Internet.

The findings from our study highlight smartphone information security amidst the digital divide and socio-economic disparities. Tertiary institutes, as well as government agencies such as national response centre for cyber-crimes, can identify population which is at risk and take up of subsequent interventions in enhancing their smartphone information security practices. Such interventions include tailored smartphone information security training programs as advocated by other researchers (Ma et al., 2019) for digitally less connected and economically less privileged. These programs can allow these marginalised populations to make use of digital economic opportunities with safe and secure access to the Internet. With developing countries maintaining low resources such as budget (Von Solms and Von Solms, 2015) for the development of information security controls, customised mobile security trainings as suggested by researchers (Brodin and Rose, 2020) established for their efficacy hold promise for efficient utilisation of these resources.

7 Limitations

Several limitations should be noted in the conduction of this study. First of all, the empirical evidence is hinged on the self-report data that is criticised for measurement errors and boredom effects (Spector, 1992). Since the first and third authors themselves visited the tertiary institutes and collected the data personally, these errors were minimised. As compared to online data collection, face-to-face interaction with the students took care of the boredom effects.

Moreover, the self-report data suffers from biases such as dispositional and situational characteristics (Donaldson and Grant-Vallone, 2002). Again, the face-to-face data collection reduces these biases. The respondents were not asked to provide their name or personally identifiable information and they were reassured by the authors that their data remains confidential and anonymous. These measures help reduce dispositional

characteristics i.e., leading them to give socially desirable answers and situational characteristics which make the respondents assume possible punishment on truthful answers. Although actual smartphone information security behaviours of the participants were not measured, it should be noted that information security objective assessment has some limitations due to inadequacy to measure actual incidents (Parsons et al., 2014). Therefore, self-report behaviour in assessing smartphone information security is a valid alternative. Furthermore, self-reports are not to be considered an inferior method as pointed out by (Spector, 1994) and provides valuable insights into the initial test of the hypothesis. Another limitation is the generalisability of the results. The study is carried out in one province of the country therefore; it may generalise well for the tertiary institute's students and not for the whole population of the country. Moreover, the results of the study are not generalisable worldwide due to Pakistan's cultural influence.

8 Conclusions and future work

Access to the capital-enhancing activities on the Internet entails safe and secure Information security practices of individuals. This is particularly true for developing nations where the growing ICTs and growing digital economy provide many opportunities to the citizens but the uptake of ICTs is hampered by digital and socio-economic disparities. This study carries out a survey to understand the smartphone information security behaviours of students enrolled in universities of Pakistan with respect to digital and socio-economic disparities. The results reveal that students are lax in their smartphone usage, exhibiting risky behaviours. It includes their unpreparedness for disaster recovery, unprotected behaviour and attitude and under usage of smartphone information security add-on features and utilities. Moreover, significant differences were found with respect to gender, age, language, socio-economic status and the digital divide. The findings necessitate an improved awareness of smartphone usage by targeted education and training programs and, development of cyber-policies and strategies. The results from this study can be used to develop specialised training programs for a specific gender, ages as well as for those belonging to lower socio-economic status and the wider digital divide. These targeted interventions can effectively enhance the information security posture of the developing nation which is already constrained by budget and resources. Future directions include similar research carried out in the context of cultural differences in the country. The results of which can be used to execute nationwide smartphone information security training programs. The effectiveness of these programs can be measured by adopting celebrated training evaluation frameworks. Furthermore, longitudinal studies can be conducted to see the behaviour change overtime with a constant feedback loop from trainings' effectiveness.

9 Funding

The research was partially funded by an internal grant

10 Availability of data

Data can be obtained by emailing to the corresponding author.

References

Abascal, J. et al. (2016) *Rethinking Universal Accessibility: A Broader Approach Considering the Digital Gap*, Universal Access in the Information Society, Vol. 15, No. 2, pp.179–182.

Abawajy, J. et al. (2018) 'Identifying cyber threats to mobile-IoT applications in edge computing paradigm', *Future Generation Computer Systems*, Vol. 89, No. 16, pp.525–538.

Aharony, N., Bouhnik, D. and Reich, N. (2020) 'Readiness for information security of teachers as a function of their personality traits and their assessment of threats', *Aslib Journal of Information Management*, Vol. 72, No. 5, pp.787–812.

Alsaleh, M., Alomar, N. and Alarifi, A. (2017) 'Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods', *PloS One*, Vol. 12, No. 3, p. e0173284.

Arachchilage, N.A.G. and Love, S. (2014) 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in Human Behavior*, Vol. 38, No. 9, pp.304–312.

Arain, A.A. et al. (2018) 'An analysis of the influence of a mobile learning application on the learning outcomes of higher education students', *Universal Access in the Information Society*, Vol. 17, No. 2, pp.325–334.

B Kim, E. (2014) 'Recommendations for information security awareness training for college students', *Information Management & Computer Security*, Vol. 22, No. 1, pp.115–126.

BalaGanesh, D., Chakrabarti, A. and Midhunchakkaravarthy, D. (2018) 'Smart devices threats, vulnerabilities and malware detection approaches: a survey', *European Journal of Engineering Research and Science*, Vol. 3, No. 2, pp.7–12.

Bao, W. (2020) 'COVID-19 and online teaching in higher education: a case study of Peking University', *Human Behavior and Emerging Technologies,* Vol. 2, No. 2, pp.113–115.

Barth, S. et al. (2019) 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telematics and informatics*, Vol. 41, No. 8, pp.55–69.

Berg, J. (2015) 'Income security in the on-demand economy: Findings and policy lessons from a survey of crowdworkers', *Comp. Lab. L. & Pol'y J.*, Vol. 37, No. 3, p. 543.

Blank, G., Bolsover, G. and Dubois, E. (2014) 'A new privacy paradox: Young people and privacy on social network sites', in *Prepared for the Annual Meeting of the American Sociological Association*.

Bonné, B. et al. (2017) 'Insecure network, unknown connection: Understanding Wi-Fi privacy assumptions of mobile device users', *Information*, Vol. 8, No. 3, p.76.

Botha, R.A., Furnell, S.M. and Clarke, N.L. (2009) 'From desktop to mobile: examining the security experience', *Computers & Security*, Vol. 28, Nos. 3–4, pp.130–137.

Breitinger, F., Tully-Doyle, R. and Hassenfeldt, C. (2020) 'A survey on smartphone user's security choices, awareness and education', *Computers & Security*, Vol. 88, p.101647.

Brodin, M. and Rose, J. (2020) 'Mobile information security management for small organisation technology upgrades: the policy-driven approach and the evolving implementation approach', *International Journal of Mobile Communications*, Vol. 18, No. 5, pp.598–618.

Büchi, M., Just, N. and Latzer, M. (2017) 'Caring is not enough: the importance of Internet skills for online privacy protection', *Information, Communication & Society*, Vol. 20, No. 8, pp.1261–1278.

Butler, R. (2020) 'A systematic literature review of the factors affecting smartphone user threat avoidance behaviour', *Information & Computer Security*.

Chin, A.G., Little, P. and Jones, B.H. (2020) 'An analysis of smartphone security practices among undergraduate business students at a regional public university', *International Journal of Education and Development using Information and Communication Technology*, Vol. 16, No. 1, pp.44–61.

Cik, V.K., Zagar, D. and Grgic, K. (2018) 'A framework for optimal techno-economic assessment of broadband access solutions and digital inclusion of rural population in global information society', *Universal Access in the Information Society*, Vol. 17, No. 3, pp.517–540.

Cooper, J. (2006) 'The digital divide: The special case of gender', *Journal of Computer Assisted Learning*, Vol. 22, No. 5, pp.320–334.

Crompton, H. et al. (2016) 'The use of mobile learning in science: a systematic review', *Journal of Science Education and Technology*, Vol. 25, No. 2, pp.149–160.

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

Dodel, M. and Mesch, G. (2017) 'Cyber-victimization preventive behavior: A health belief model approach', *Computers in Human Behavior*, Vol. 68, No. 3, pp.359–367.

Dodel, M. and Mesch, G. (2018) 'Inequality in digital skills and the adoption of online safety behaviors', *Information, Communication & Society*, Vol. 21, No. 5, pp.712–728.

Dodel, M. and Mesch, G. (2019) 'An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices', *Computers & Security*, Vol. 86, pp.75–91.

Donaldson, S.I. and Grant-Vallone, E.J. (2002) 'Understanding self-report bias in organizational behavior research', *Journal of business and Psychology*, Vol. 17, No. 2, pp.245–260.

Eckel, C.C. and Grossman, P.J. (2008) 'Men, women and risk aversion: experimental evidence', *Handbook of Experimental Economics Results*, Vol. 1, pp.1061–1073.

Eppler, J. and Wang, Y. (2018) 'Towards improving the security of mobile systems using virtualization and isolation', in *Fourth International Conference on Mobile and Secure Services (MobiSecServ)*, IEEE, pp.1–6.

GSMA | The Mobile Economy - The Mobile Economy (no date) [online] https://www.gsma.com/mobileeconomy/ (accessed: 10 August 2020).

Harris, M.A., Furnell, S. and Patten, K. (2014) 'Comparing the mobile device security behavior of college students and information technology professionals', *Journal of Information Privacy and Security*, Vol. 10, No. 4, pp.186–202.

He, J. and Freeman, L.A. (2019) 'Are men more technology-oriented than women? the role of gender on the development of general computer self-efficacy of college students', *Journal of Information Systems Education*, Vol. 21, No. 2, p.7.

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', *Behaviour & Information Technology*, Vol. 33, No. 12, pp.1347–1360.

Jain, A.K. and Hausman, R.E (2006*) Stratified Multistage Sampling*, Encyclopedia of Statistical Sciences.

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.R. (2012) 'Do business students practice smartphone security?', *Journal of Computer Information Systems*, Vol. 53, No. 2, pp.22–30.

Lal, K. (2017) 'Investigating ICT infrastructure to develop an information society in India', *Universal Access in the Information Society*, Vol. 16, No. 2, pp.517–528.

Lallie, H.S. et al. (2021) 'Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Computers & Security*, Vol. 105, No. 6, p.102248.

Ling, C., Hwang, W. and Salvendy, G. (2006) 'Diversified users' satisfaction with advanced mobile phone features', Universal Access in the Information Society, 5(2, pp.239–249.

Livingstone, S. and Helsper, E. (2010) 'Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy', New media & society, 12(2, pp.309–329.

Ma, S. et al. (2019) 'Exploring information security education on social media use', *Aslib Journal of Information Management*, Vol. 71, No. 5, pp.618–636.

Masood, F. et al. (no date) 'A systematic literature review and case study on influencing factor and consequences of freelancing in Pakistan', *International Journal of Scientific & Engineering Research*, December, Vol. 9, No. 12.

McGill, T. and Thompson, N. (2017) 'Old risks, new challenges: exploring differences in security between home computer and mobile device use', *Behaviour & Information Technology*, Vol. 36, No. 11, pp.1111–1124.

McGuire, M. and Dowling, S. (2013) 'Cyber-crime: a review of the evidence', Summary of key findings and implications', *Home Office Research Report*, Vol. 75, ISBN: 1782462457, 9781782462453.

Multidimensional Poverty in Pakistan (no date) *UNDP in Pakistan* [online] http://www.pk.undp.org/content/pakistan/en/home/library/hiv_aids/Multidimensional-Poverty-in-Pakistan.html (accessed: 25 January 2018).

Nowrin, S. and Bawden, D. (2018) 'Information security behaviour of smartphone users', *Information and Learning Science*, Vol. 119, Nos. 7–8, pp.444–455.

Padilla-MeléNdez, A., Del Aguila-Obra, A.R. and Garrido-Moreno, A. (2013) 'Perceived playfulness, gender differences and technology acceptance model in a blended learning scenario', *Computers & Education*, Vol. 63, No. 2, pp.306–317.

Palanisamy, R., Norman, A.A. and Kiah, M.L.M. (2020) 'Compliance with bring your own device security policies in organizations: a systematic literature review', *Computers & Security*, Vol. 28, No. 11, p.101998.

Parker, F. et al. (2015) 'Security awareness and adoption of security controls by smartphone users', in *Second International Conference on Information Security and Cyber Forensics (InfoSec)*, IEEE, pp.99–104.

Parsons, K. et al. (2014) 'Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)', *Computers & Security*, Vol. 42, No. 3, pp.165–176.

Payoneer | The Global Gig-Economy Index: Q2 2019 (no date) [online] https://explore.payoneer.com/q2_global_freelancing_index/ (accessed: 11 July 2020).

Pimmer, C., Mateescu, M. and Gröhbiel, U. (2016) 'Mobile and ubiquitous learning in higher education settings. a systematic review of empirical studies', *Computers in Human Behavior*, Vol. 63, No. 11, pp.490–501.

Reyns, B.W., Randa, R. and Henson, B. (2016) 'Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis', *Crime Prevention and Community Safety*, Vol. 18, No. 1, pp.38–59.

Robinson, L. et al. (2015) 'Digital inequalities and why they matter', *Information, Communication & Society*, Vol. 18, No. 5, pp.569–582.

Sari, P.K. (2014) 'Measuring information security awareness of Indonesian smartphone users', *Telkomnika*, Vol. 12, No. 2, pp.493–500.

Sawaya, Y. et al. (2017) 'Self-confidence trumps knowledge: A cross-cultural study of security behavior', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp.2202–2214.

Serrano-Tellería, A. (2018) 'Users 'management of mobile devices and privacy', *El Profesional De La Información*, Vol. 27, No. 4.

Shad, M.R. (2019) 'Cyber threat landscape and readiness challenge of Pakistan', *Strategic Studies*, Vol. 39, No. 1, pp.1–19.

Shah, P. and Agarwal, A. (2020) 'Cybersecurity behaviour of smartphone users in India: an empirical analysis', Information & Computer Security.

Shi, F. (2015) 'Study on a stratified sampling investigation method for resident travel and the sampling rate', *Discrete Dynamics in Nature and Society*, Vol. 2015, pp.1–7.

Sombatruang, N. et al. (2019) 'Factors influencing users to use unsecured wi-fi networks: evidence in the wild', in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp.203–213.

Spector, P.E. (1992) 'A consideration of the validity and meaning of self-report measures of job conditions', in Cooper, C.L. and Roberston, I.T. (Eds.) *International Review of Industrial and Organizational Psychology*, Wiley, Chichester, Vol. 7, pp.123–151.

Spector, P.E. (1994) 'Using self-report questionnaires in OB research: a comment on the use of a controversial method', *Journal of Organizational Behavior*, Vol. 15, No. 5, pp.385–392.

Stylios, I. et al. (2016) 'Users' attitudes on mobile devices: can users' practices protect their sensitive data?', in *MCIS*, p.1.

Sung, Y-T., Chang, K-E. and Liu, T-C. (2016) 'The effects of integrating mobile devices with teaching and learning on students' learning performance: A meta-analysis and research synthesis', *Computers & Education*, Vol. 94, pp.252–275.

Tamrin, S.I., Norman, A.A. and Hamid, S. (2017) 'Information systems security practices in social software applications', *Aslib Journal of Information Management*, Vol. 69, No. 2, pp.131–157.

The Mobile Economy Asia Pacific 2020 (no date) *The Mobile Economy* [online] https://www.gsma.com/mobileeconomy/asiapacific/ (accessed: 26 July 2020).

Tu, Z., Yuan, Y. and Archer, N. (2014) 'Understanding user behaviour in coping with security threats of mobile device loss and theft', *International Journal of Mobile Communications*, Vol. 12, No. 6, pp.603–623.

Van Deursen, A.J. et al. (2017) 'The compoundness and sequentiality of digital inequality', *International Journal of Communication*, Vol. 11, pp.452–473.

Van Dijk, J.A. (2005) *The Deepening Divide: Inequality in The Information Society*. Sage Publications, London.

van Ingen, E. and Matzat, U. (2018) 'Inequality in mobilizing online help after a negative life event: the role of education, digital skills, and capital-enhancing Internet use', *Information, Communication & Society,* Vol. 21, No. 4, pp.481–498.

Von Solms, R. and Von Solms, S. (2015) 'Cyber safety education in developing countries', *Syst. Cybern. Informatics*, Vol. 13 , No. 2, pp.14–19.

Yan, P. and Yan, Z. (2018) 'A survey on dynamic mobile malware detection', *Software Quality Journal*, Vol. 26, No. 3, pp.891–919.

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

Zhou, J., Rau, P-L.P. and Salvendy, G. (2014) 'Age-related difference in the use of mobile phones', *Universal Access in the Information Society*, Vol. 13, No. 4, pp.401–413.