2-2021

Exploring the information security practices on the smartphone by the postgraduate students of University of Calicut

Vysakh C

Amina Jasmina K V
amskv666@gmail.com

Exploring the information security practices on the smartphone by the postgraduate students of University of Calicut

Vysakh. C
Research Scholar
DOSR in Library & Information Science
Tumkur University, Karnataka-India
chingathvysakh@gmail.com,+919744050979.

Amina Jasmina. K V
Library and Information Associate (Intern)
Indian Institute of Management- Kozhikode
Kunnamangalam, Kerala-India
amskv666@gmail.com,+919188179754.

Abstract

This paper aims to report on the information security practices on the smartphone by the students of the University of Calicut, Kerala. Data were gathered by using a survey questionnaire which was administered to 344 smartphone cohorts at the postgraduate level. The study findings reported the scanty knowledge of the participants regarding the issues and risks associated with smartphones even though most of the respondents were aware of the information security practices available in the smartphones. The data analysis delineated the habit of students storing secret and sensitive information like ATM password, bank or credit card account details and personal photos on their smartphones. Data leakage resulting from device loss or theft was the major security risk faced by the participants. The number of participants misplaces their smartphone also found high. Data backup and blocking the device once lost were the major security practices adopted by the participants to recover from the disaster. This is to be sure, first of its kind study to survey the postgraduate students at the university level in India and the findings of the study would help the smartphone users in general and students in particular to protect their information stored in their smartphones.

Keywords – Information security, Information security practices, Smartphone, Security risks, Cybersecurity, University of Calicut.

Introduction

The interest of students in m-learning has increased exponentially because it lets them learn from anywhere anytime. It offers a collaborative and interactive way of teaching and learning which minimizes most of the barriers faced in the conventional way of teaching (Fan et al., 2020). The use of smartphones in India is skyrocketing especially among students. Vaidya in their study reported that the majority of the Indian students are smartphone users with 98% of them having an internet connection(Vaidya, Pathak, & Vaidya, 2016). Furthermore, the smartphone use among them found a significant difference in terms of gender, age and educational level (Tikadar & Bhattacharya, 2019). The scholarly interest in smartphone usage has increased with the recent developments in mobile communication technology(Ariel, Elishar-Malka, Avidar, & Levy, 2017). Apart from educational purposes like making notes and searching academic information, students are now exploring various activities through smartphone including gaming, online shopping and social chatting. The addiction of students to social networking and gaming is quite visible and have been reported in various previous studies(Raj, Bhattacherjee, & Abhijit, 2019;

Al-Menayes, 2015 & Azizi, Soroush, & Khatony, 2019). The use of smartphones is always at high risk and the use of social networking sites in the smartphone has created a loss of 50 million user records in 2019 through Facebook and 52 million in Google+ (Srivastava, Dube, Shrivastaya, & Sharma, 2019; Hamid, Alam, Sheherin, & Pathan, 2020). There are security systems and techniques to avoid these kinds of hazards and students in other countries are well aware of the same(Poland-Szumski, 2018; Indonesia-Kohar, Riadi, & Lutfi, 2015 & Malaysia-(Al-Jerbie & Jali, M. Z.). The status of Indian students on practicing information security techniques are yet to be explored and this study is conducted to bridge this gap. With no earlier studies found regarding the information security practices of smartphone users at the postgraduate level, this investigation would be an eye-opener to many ones especially students in India who are using smartphones for personal and academic activities at large. In short, the study is trying to find answers to the following underpinned questions.

RQ1: To what extent the postgraduate students of the University of Calicut are aware of the information security practices on the Smartphone?

RQ2: What are the major smartphone security risks faced by the postgraduate students of the University of Calicut?

RQ3: What are the major approaches followed by the postgraduate students towards the harmful behaviour on the smartphone?

RQ4: What are the major approaches followed by the postgraduate students in useful phone settings and add-on utilities?

RQ5: What are the key disaster recovery practices followed on the smartphone by the postgraduate students of the University of Calicut?

Previous studies

Students use the smartphone for a variety of reasons viz. edutainment, entertainment, infotainment etc.(M. Alfawareh & Jusoh, 2014; Masika et al., 2015; Dukic, Chiu, & Lo, 2015 & Wai, Ng, Chiu, Ho, & Lo, 2018). The smartphone addiction among the students has raised various concerns including life stress(Chiu, 2014) and psychological issues (Pearson & Hussain, 2016). Apart from these issues, smartphone addiction affects the academic activities of the students. According to the studies, college students have the highest rate of IT and smartphone adoption (Muhirwe & White, 2016). While, the use of the same is reported to be at high risk(Srivastava et al., 2019). Cybercrimes through smartphones are increasing at an alarming rate especially in India(Vijayakumar, 2016). Qudah et al. (2019) reported that smartphone addiction would lead to smartphone bullying. To stay away from cyber-attacks, the users need to be aware of various cyber issues happening in cyberspace. There is a direct association between security awareness and prevention action(Al-Janabi & Al-Shourbaji, 2016).

The study conducted by Szumski (2018) among the Polish students reported that the majority of the students were concerned about the securities on the internet. Kohar, Riadi, & Lutfi (2015) found that Indonesian users were also well aware of cybersecurity activities. The cybersecurity awareness among the students had a significant difference in terms of their academic level and domain(Peker, Ray, Silva, & Gibson, 2016). For example, secondary students at the Libyan school, Malaysia had adequate awareness

about the security practices (Al-Jerbie & Jali, M. Z., 2014), while higher education students were not having requisite knowledge (Muniandy, Muniandy, & Samsudin, 2017).

Jones & Heinrichs (2012) investigated whether business students in a regional public university in the USA practice any smartphone security and found that students were lax. The study also reported that men were more willing to engage in risky behaviour than women. There were no differences in behaviours based upon maturity level or use of smartphones for financial transactions. Al-Janabi & Al-Shourbaji (2016) from the Middle East, Abbas (2019) from the USA, Androulidakis & Kandus (2011) from Hungary too reported that students lack requisite knowledge about the information security practices. As far as India is concerned, the general smartphone users were aware of the security issues and the mechanism to get rid of them, even though they were reported to be quite casual in protecting their devices(Bagga, Sodhi, Shukla, & Qazi, 2017). To what extent students in India are aware of these security practices is yet to be explored and thus, the need for conducting the present study has become the need of the hour.

Scope and Methodology of the Study

The target population of the study were the postgraduate students of the University of Calicut. The University of Calicut is the largest universities in the state of Kerala with NAAC "A" grade. It has more than 400 hundred affiliated colleges and 35 departments. This study was confined only to those who were studying on the main campus. To collect the data for the study, the investigators selected students randomly who were using a smartphone and distributed the questionnaire. The main purpose of the questionnaire was to measure the degree to which students practice information security on their smartphones. The questionnaire included 2 parts. The first part sought information regarding the demographic details and smartphone usage of the participants. The second part addressed the information security practices adopted by the students. As many as 382 questionnaires distributed to smartphone cohorts, 355 were completed and returned. Out of which 11 found not adequate and so excluded from the subsequent analysis. Thus, a total of 344 questionnaires were analyzed. The collected survey responses were checked for finding missing data and further entered into SPSS for analysis. Descriptive statistics including percentage and frequency methods were applied. The major findings of the study are discussed in the following section.

Analysis and interpretation

(Data given in parentheses can be read as a percentage)

General information

Table 1 illustrates the general information of the respondents. Of the total of 344 respondents surveyed, the majority were female with 184 participants compared to their male counterparts with 160 respondents. The department-wise distribution of the participants showed that the majority of the respondents were Art students with 28.2% followed by Humanities and Commerce with 27.1% and 23.8% respectively. A good number of participants (72 or 20.9%) also participated in the survey from the Science stream.

Table:1 General information

Response	Male	Female	Total
Gender	160 (46.51)	184 (53.48)	344 (100)
Department			
Arts	48(30)	49(26.65)	97(28.2)
Commerce	40(25)	42(22.82)	82(23.8)
Science	30(18.75)	42(22.82)	72(20.9)
Humanities	42(26.25)	51(27.71)	93(27.1)
Total	**160 (100)**	**184 (100)**	**344 (100)**

Reason for using smartphones

The major reasons for using the smartphone among the students is depicted in Figure 1. According to the figure, the majority of male participants (97.8%) used a smartphone for communicating with their family. It is seen that 88.88% of the male students used it for academic purposes followed by 82.2% for accessing social networking sites. Ironical to male students, the majority of the female respondents(94.23%) used smartphones mainly for academic purposes followed by accessing social networking sites(73.08%). It is interesting to see that the use of smartphones for online gaming is very less among the participants.

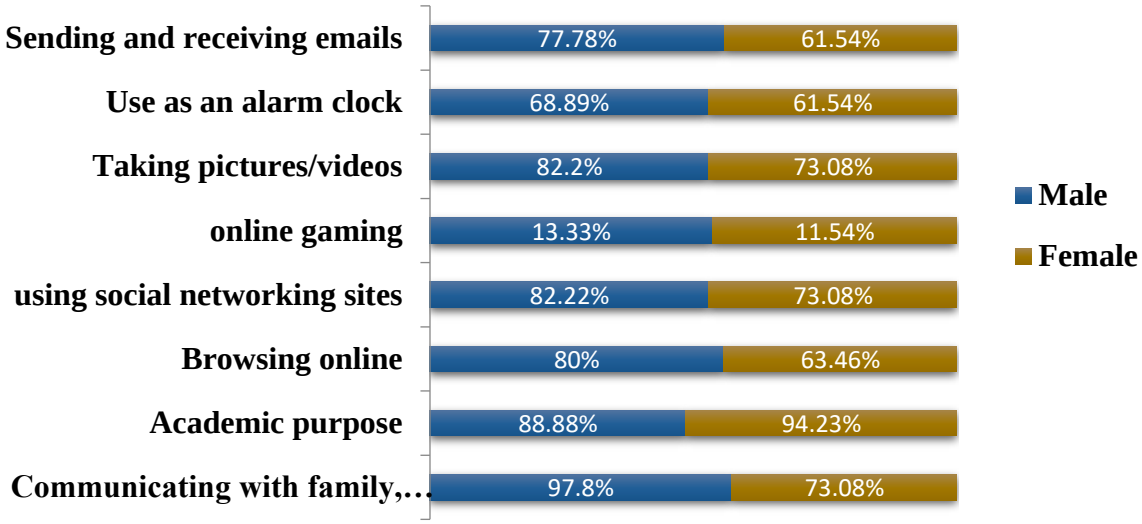

Figure 1 - Reason for using smartphones

Knowledge about issues and risks & Awareness about information security practices

The study attempted to measure the knowledge level of the participants on the issues and risk associated with the use of the smartphone. The result is given in Figure 2. Ostensibly, only a few females (5.43%) and male(11.25%) participants have excellent knowledge. 32.6% of the female and 31.25% of the male participants have good knowledge. A good number of male(26.25%) and female(36.95%) participants have sufficient understanding while 22.8% female and 25% male participants have an insufficient grip about smartphone-related issues and risks. The main objective of the study was to investigate the awareness of the students about the information security practices on smartphones and it is clear from figure 3 that the majority of the participants (female -80.43% & Male-80%) are aware (RQ1).

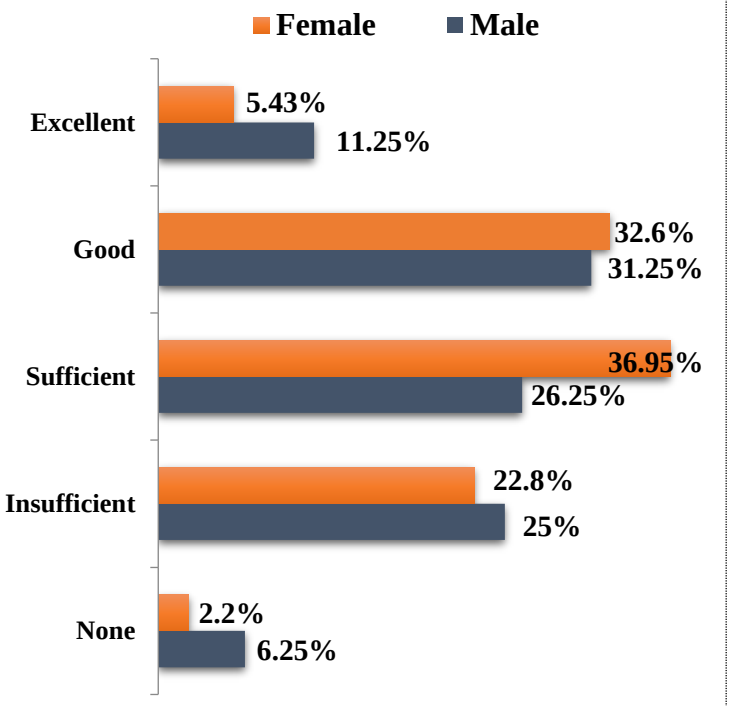

Figure 2 - Knowledge about issues and risks associated with the Smartphones

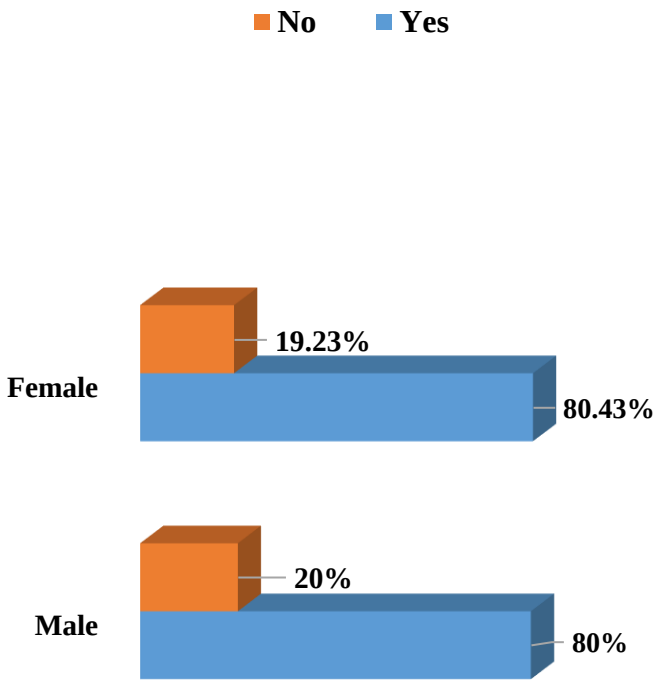

Figure 3 - Awareness about the information security practices on Smartphones

Knowledge about the modern operating system and IMEI

Apart from measuring the understanding of the participants about the issues and risks associated with the smartphone, the study tried to investigate whether they are aware of the modern operating system and IMEI. As per the data in Figure 4, male participants are more aware of both the operating system and IMEI. 57.78% of the male participants are aware of the operating system and 68.89% of them are aware of IMEI. Nearly half of the female participants(47.15%) are not aware of the operating systems. It is also noted that a large number of female participants (78.85%) are unaware of IMEI.

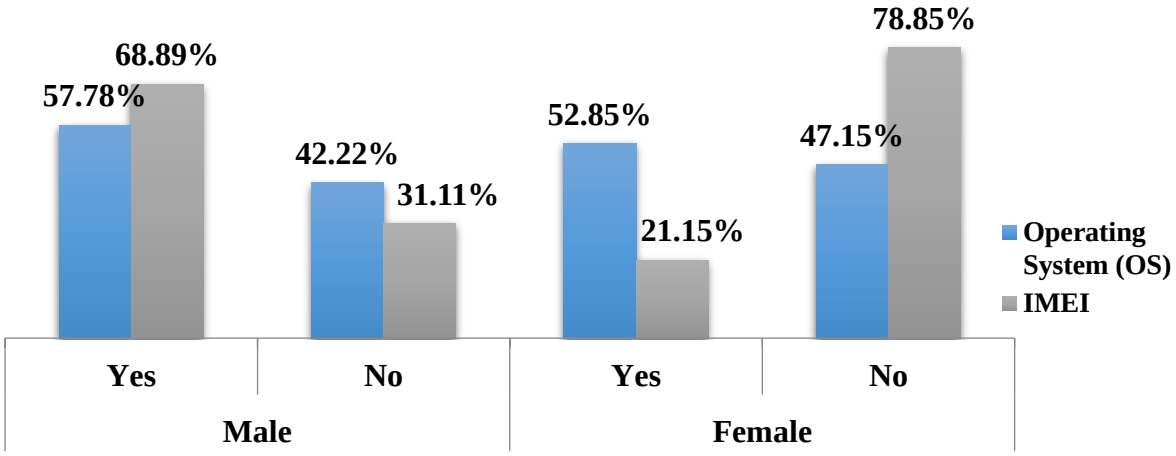

Figure 4 -Knowledge about modern operating system and IMEI

Personal information those are storing on smartphone

Participants were also asked about what kind of personal information that they normally store in smartphones and the result is illustrated in Figure 5. The majority of both male and female participants stored their email account passwords in their smartphone. More than half of the participants (57.77%) used smartphones to store their ATM passwords. 61.54% of male respondents stored bank or credit card details on their smartphone while 44.44% of female respondents did store the same. Students especially male at a good number (17.3%) used to store sensitive information on smartphones while it is less in the case of female ie 6.66%. A very few males (3.85%) and female (8.88%) participants stored online account number on their smartphone.

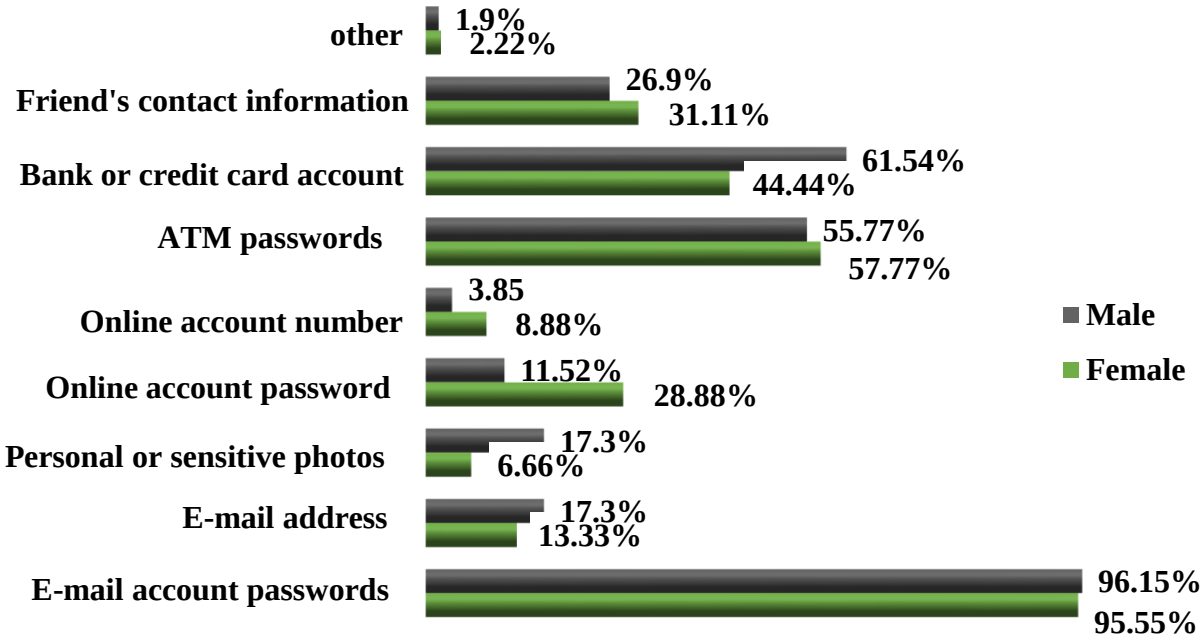

Figure 5-Personal information those are storing in smartphone

Smartphone security risks faced by students

Risks especially related to information security is plenty and our study asked 10 most happening perils with which the students faced while dealing with their smartphones. According to Figure 6, the major risk faced by the respondents is data leakage which is cited as a major concern by nearly half of the male (46.67%) and a good number of female respondents(34.61%) (RQ2). Unintentional disclosure of data has been cited as a major risk by 37.78% male and 23.08% female respondents. 33.33% of the male participants opined network spoofing attacks as a major risk being faced by them in the smartphone. The same is cited as a major peril by 21.15% of female participants. Financial malware attack and spyware attack have been a major threat to 31.1% of male participants. It is seen that the same is cited as a major threat by female accounted for 26.9% and 17.31% respectively.

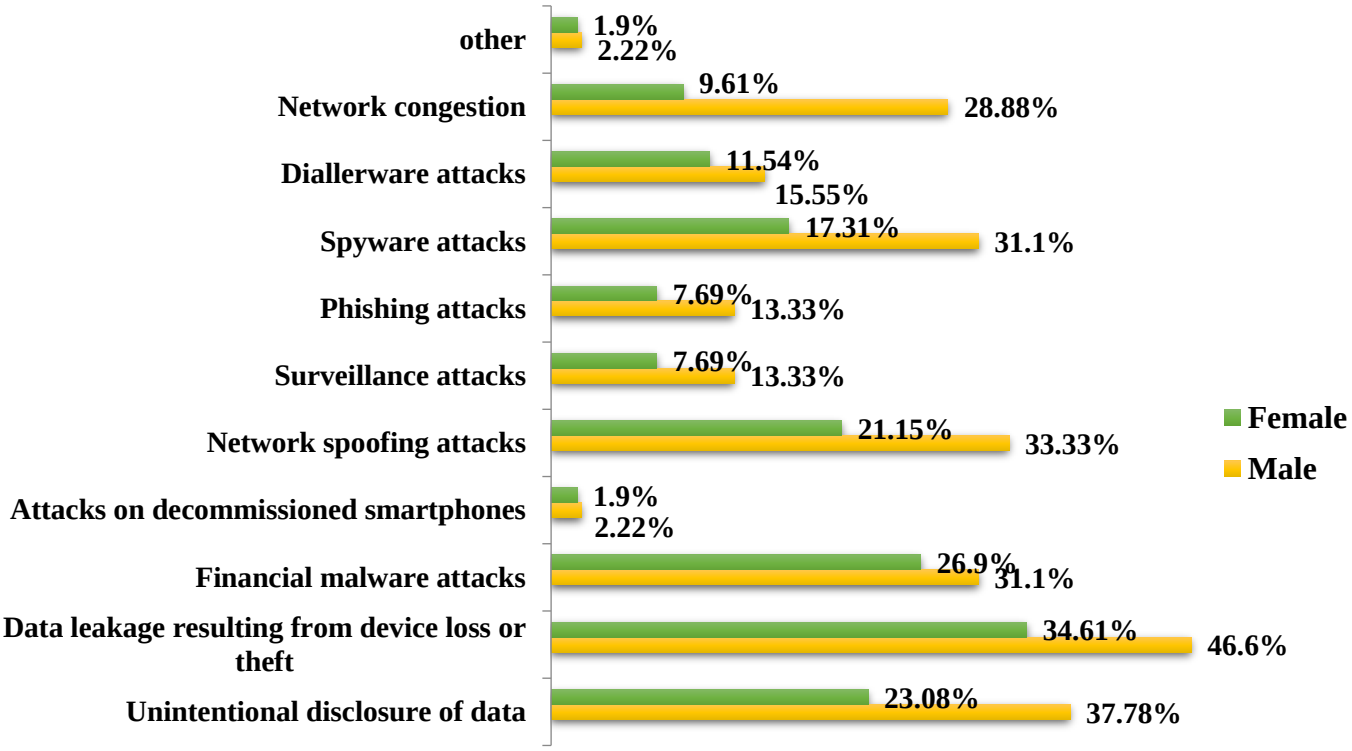

Figure :- 6 Security risks faced by the male and female students by using smartphone

Approaches towards harmful behaviour

The study also attempted to investigate the various approaches followed by the participants towards harmful behaviours (RQ3). The data in Table 2 shows that male participants (35.55%) always tend to switch off their data connection compared to female(7.69%). 58 female participants never switch off their data connections. More than half of both male(55.55%) and female(57.69%) participants did avoid downloading apps from unknown sources. Nearly half of both male (44.44%)and female (40.38%)participants have a habit of logging out their applications to stay safe. More than half of male(57.78%) and nearly half of female(46.15%) respondents configure automatic locking. A good number of male(53.3%) and female(42.3%) participants sometimes avoid connecting to public Wi-Fi networks.22.55 % of male and 9.63% of female participants never updated to systems and applications. Nearly half of the male participants(44.4%) and a good number of female participants(36.5%) blocked their own identity sometimes to stay away from harmful activities.

Table:-2 Approaches towards harmful behaviour

Responses	Always		Sometimes		Never	
	Male	**Female**	**Male**	**Female**	**Male**	**Female**
Switch off data connections	56 (35.55)	14 (7.69)	84 (53.3)	112 (61.54)	20 (11.12)	58 (30.77)
Check permission authorization	32 (20)	50 (26.9)	114 (71.11)	96 (51.9)	14 (8.89)	38 (21.2)
Avoid downloading apps from unknown sources	88 (55.55)	106 (57.69)	46 (28.88)	48 (26.9)	26 (15.57)	30 (15.41)
Logging out of applications	70 (44.44)	74 (40.38)	82 (51.11)	88 (48)	6 (4.45)	22 (11.62)
Configure automatic locking	92 (57.78)	84 (46.15)	56 (35.5)	64 (34.6)	12 (6.72)	36 (19.25)
Avoid using location services	52 (33.33)	56 (30.77)	92 (57.7)	78 (42.3)	16 (26.7)	50 (36.55)
Avoid connecting to public Wi-Fi networks	32 (20)	38 (21.1)	84 (53.3)	78 (42.3)	44 (26.7)	68 (36.55)
Updates to systems and applications	70 (44.44)	88 (48.07)	84 (53.3)	78 (32.69)	36 (22.5)	18 (9.63)
Block one's identity	60 (53.3)	64 (34.6)	70 (44.4)	66 (36.5)	30 (22.27)	54 (28.89)

Approaches in useful phone settings and add-on utilities

Students were asked to express settings and add-on utilities activated on their smartphones (RQ4). According to Table 3, 52 participants always deploy updates on their smartphone. While 48 participants never update their smartphone. It is also clear that a good number of male(11.2%) and female(11.24%) participants never installed anti-virus software or application to protect their data on the phone. The majority of both male(66.6%) and female(67.3%) participants disable their Wi-Fi as a precaution tool to stay away from attacks. The number of respondents who disable Bluetooth is also high.55.5% of male 30.7% of female always disable their Bluetooth. Nearly half of the participants sometimes disable their GPS. While a good number of female respondents(34.32%) never disable. It is also seen that majority of male (68.8%)and female (57.7%) participants use data/device encryption. It is understood that 52 participants never modify their privacy settings of the phone. Even though the majority of male (68.8%)and female(57.7%) participants install apps for privacy protection/permission management.

Table: - 3 Approaches in useful phone settings and add-on utilities

Responses	Always		Sometimes		Never	
	Male	**Female**	**Male**	**Female**	**Male**	**Female**
Deploy updates	38 (24)	14 (7.6)	102 (64.4)	142 (76.9)	20 (11.6)	28 (15.5)
Installation of anti-virus software or application	36 (22.2)	74 (40.4)	106 (66.6)	88 (48.38)	18 (11.2)	22 (11.24)
Disable Wi-Fi connection	32 (20)	34 (19)	106 (66.6)	124 (67.3)	22 (13.4)	26 (13.7)
Disable Bluetooth	88 (55.5)	56 (30.7)	50 (31.1)	110 (59.6)	22 (13.4)	18 (9.7)
Disable GPS	68 (42.2)	32 (17.3)	78 (48.8)	88 (48.38)	14 (9)	64 (34.32)
Modify privacy settings of the device	46 (28.8)	56 (30.7)	78 (48.8)	96 (51.9)	36 (22.4)	16 (17.4)
Avoid rooting the device	42 (26.6)	32 (17.3)	88 (55.5)	106 (57.69)	30 (17.9)	46 (25)
Use data/ device encryption	38 (24.4)	64 (34.6)	110 (68.8)	106 (57.7)	12 (6.8)	14 (7.7)
Use apps for privacy protection/permission management	38 (24.4)	64 (34.6)	110 (68.8)	106 (57.7)	12 (6.8)	14 (7.7)

Approaches for disaster recovery

When sought information regarding the major approaches that the respondents adopted for recovering the disaster(RQ5), it is found that 40% of male and only 9.6% of female participants always back up their data stored in their smartphone. While 8.88% of male and 13.5% of female respondents never tried this for recovery. It is also clear that only 22 male and 14 female participants would block their devices after they it lost. More than half of the female participants(57.71%) never block their device once it went missing. participants are not interested to insure their phone as the majority of the male (71.12%) and female (75.06%) participants never take out insurance to cover the loss of their smartphones.

Table: - 4 Approaches for disaster recovery

Responses	Always		Sometimes		Never	
	Male	Female	Male	Female	Male	Female
Data backup	64 (40)	16 (9.6)	82 (51.1)	142 (76.9)	14 (8.88)	26 (13.5)
Blocking the device after losing it	22 (13.33)	14 (7.69)	88 (55.55)	64 (34.6)	50 (31.12)	106 (57.71)
Take out insurance	14 (8.87)	8 (3.84)	32 (20)	38 (21.1)	114 (71.12)	138 (75.06)

Misplacement of smartphone

Respondents were also asked whether they misplace phones and the responses were analysed. According to Figure 7, male participants tend to misplace their phones compared to female. 28.88% of the male participants cited that they would misplace smartphones while it is 15.38% of female. The misplacement always leads to loss of the device and it was found from the previous table that most of the students never blocked their device once it loses it.

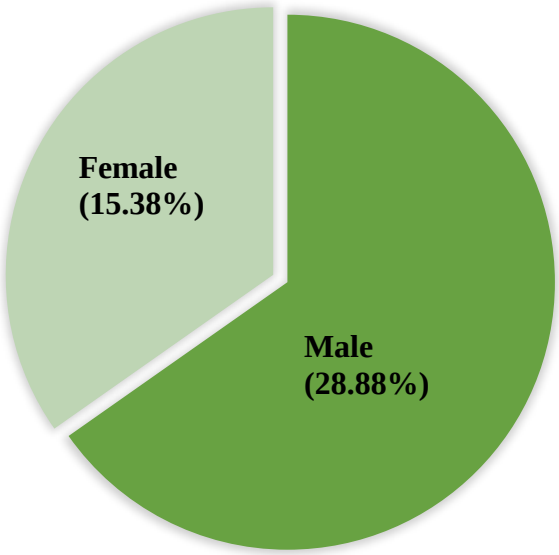

Figure 7 -Misplacement of smartphone

Concern about the safety and security of information stored in the smartphone

Finally, we wanted to know to what extent the students are concerned about the safety and security of the information stored in their smartphone and a separate question was included in the questionnaire to measure it. As per Figure 8, 35% of male and 29.35% of female participants are not worried about the safety and security of the information stored in their smartphones. Nearly half of male(40%) and female(47.83%) participants are a bit worried. There are 13.75% of male and 5.44% of female who are enough worried about their data stored in smartphones. It is also seen from the table that a few males (11.25%) and female participants (17.39%) are much worried.

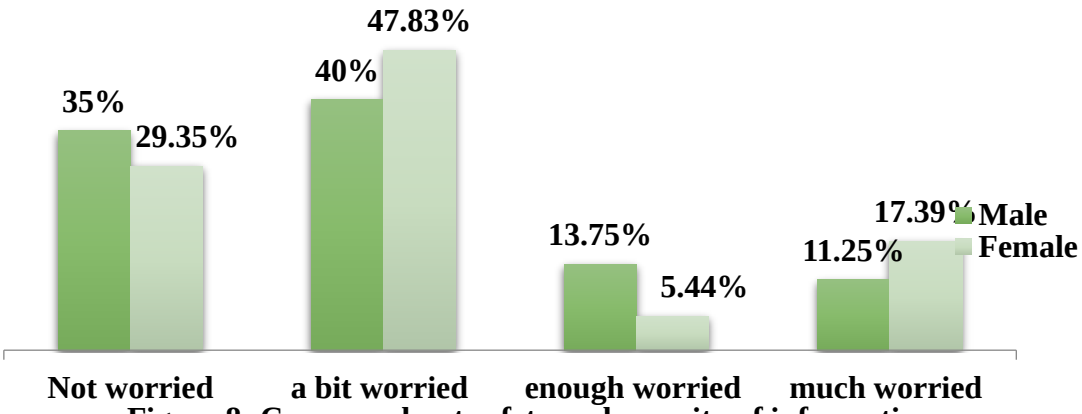

Figure 8 -Concern about safety and security of information

Findings, Conclusion and Recommendations

This research attempt to investigate the information security practices of postgraduate students at the University of Calicut. The study mainly embarked on the information security practices on the smartphone. The study findings reported the scanty knowledge of the participants regarding the issues and risks associated with smartphones. 25% of female & 31.25% of male participants was having insufficient knowledge regarding the dangers associated with the smartphone. Female students were lacking knowledge about IMEI compared to male. Even though, majority of the students were aware of the security practices on smartphone and were not concerned or worried much about the safety and security of information stored in their device. The tendency of students to store their sensitive and secret data on their device was reported as alarming. The majority of both genders used their smartphone device for storing secret information like email password, ATM password, bank and credit card details. The major risk faced by the respondents was data leakage. The number of participants who connected to public WI-FI also found high. Many of them never updated their systems and applications. It was found that still, a good number of participants were yet to install anti-virus software or application to protect their data on the smartphone device. It was interesting to see that the number of students who used to misplace their device was high. Adding to this, 156 participants never blocked the device once it went missing.

Cyber threats continue to grow at an exponential rate. The need for imparting proper awareness and training programs to the students has become mandatory which is far beyond the information technology college courses (Slusky & Partow-navid, 2014). Various security issues like spyware, network spoofing and phishing attacks are surging and the application developers should better their security system even though the users have adequate knowledge but reported laxity in adopting. Connecting to public free wi-fi would let the hackers intrude to the device easily which should be avoided maximum. The privacy setting of the device to be updated frequently and back up of data can be done. Smartphone users can also insure their device to compensate against the risk of loss or damage.

Following recommendations are proposed

- Academic institutions should impart cyber-security awareness and training programs for the students.
- The students are suggested not to store any secret and sensitive information on their smartphones.
- The security facilities which are available in the smartphone devices to be recalibrated.
- Be very vigilant while connecting to public free networks and always try to use a safe network.

References

Abbas, M. (2019). Cyber Security Awareness Among College Students. *Advances in Intelligent Systems and Computing*, 79–89. https://doi.org/10.1007/978-3-319-94782-2

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information and Knowledge Management*, *15*(1). https://doi.org/10.1142/S0219649216500076

Al-Jerbie & Jali, M. Z., S. I. (2014). A second look at the information security awareness among secondary school students. In *The International Conference on Information Security and Cyber Forensics (InfoSec2014)* (pp. 88–97).

Al-Menayes, J. (2015). Dimensions of Social Media Addiction among University Students in Kuwait. *Psychology and Behavioral Sciences*, *4*(1), 23. https://doi.org/10.11648/j.pbs.20150401.14

Androulidakis, I., & Kandus, G. (2011). Mobile Phone Security Awareness and Practices of Students in Budapest. In *ICDT 2011, The Sixth International ...* (pp. 18–24). Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=icdt_2011_1_40_20110

Ariel, Y., Elishar-Malka, V., Avidar, R., & Levy, E. C. (2017). Smartphone usage among young Israeli adults: a combined quantitative and qualitative approach. *Israel Affairs*, *23*(5), 970–986. https://doi.org/10.1080/13537121.2017.1345422

Azizi, S. M., Soroush, A., & Khatony, A. (2019). The relationship between social networking addiction and academic performance in Iranian students of medical sciences: A cross-sectional study. *BMC Psychology*, *7*(1), 1–8. https://doi.org/10.1186/s40359-019-0305-0

Bagga, T., Sodhi, J. S., Shukla, B., & Qazi, M. A. (2017). Smartphone security behaviour of the Indian smartphone user. *Man in India*, *97*(24), 333–344.

Chiu, S. I. (2014). The relationship between life stress and smartphone addiction on taiwanese university student: A mediation model of learning self-Efficacy and social self-Efficacy. *Computers in Human Behavior*, *34*, 49–57. https://doi.org/10.1016/j.chb.2014.01.024

Dukic, Z., Chiu, D. K. W., & Lo, P. (2015). How useful are smartphones for learning? Perceptions and practices of Library and Information Science students from Hong Kong and Japan. *Library Hi Tech*, *33*(4), 545–561. https://doi.org/10.1108/LHT-02-2015-0015

Fan, K. Y. K., Lo, P., Ho, K. K. W., So, S., Chiu, D. K. W., & Ko, E. H. T. (2020). Exploring mobile learning needs amongst performing arts students. *Information Discovery and Delivery*, *48*(2), 103–112. https://doi.org/10.1108/IDD-12-2019-0085

Hamid, A., Alam, M., Sheherin, H., & Pathan, A. K. (2020). Cyber Security Concerns in Social Networking Service. *International Journal of Communication Networks and Information Security*, *12*(2), 198–212.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, *53*(2), 22–30. https://doi.org/10.1080/08874417.2012.11645611

Kohar, A., Riadi, I., & Lutfi, A. (2015). Analysis of Smartphone Users Awareness Activities Cybercrime. *International Journal of Computer Applications*, *129*(2), 1–6. https://doi.org/10.5120/ijca2015906449

M. Alfawareh, H., & Jusoh, S. (2014). Smartphones usage among university students: Najran University case. *International Journal of Academic Research*, *6*(2), 321–326. https://doi.org/10.7813/2075-4124.2014/6-2/B.48

Masika, M. M., Omondi, G. B., Natembeya, D. S., Mugane, E. M., Bosire, K. O., & Kibwage, I. O. (2015). Use of mobile learning technology among final year medical students in Kenya. *Pan African Medical Journal*, *21*, 1–12. https://doi.org/10.11604/pamj.2015.21.127.6185

Muhirwe, J., & White, N. (2016). Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users. *Issues in Information Systems*, *17*(Ii), 183–192.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *Journal of Information Assurance & Cybersecurity*, *2017*, 1–13. https://doi.org/10.5171/2017.800299

Pearson, C., & Hussain, Z. (2016). Smartphone Addiction and Associated Psychological Factors. *Addicta: The Turkish Journal on Addictions*, *3*(2). https://doi.org/10.15805/addicta.2016.3.0103

Peker, Y. K., Ray, L., Silva, S. Da, & Gibson, N. (2016). Raising Cybersecurity Awareness among College Students. *Journal of The Colloquium for Information System Security Education (CISSE)*, (September), 1–17.

Raj, M., Bhattacherjee, S., & Abhijit, M. (2019). Usage of Online Social Networking Sites among School Students of Siliguri, West Bengal, India. *Indian Journal of Psychological Medicine*, *40*(5), 452–457. https://doi.org/10.4103/IJPSYM.IJPSYM_70_18

Slusky, L., & Partow-navid, P. (2014). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security*, 37–41. https://doi.org/10.1080/15536548.2012.10845664

Srivastava, S. R., Dube, S., Shrivastaya, G., & Sharma, K. (2019). Smartphone Triggered Security Challenges - Issues, Case Studies and Prevention. *Cyber Security in Parallel and Distributed Computing*, 187–206. https://doi.org/10.1002/9781119488330.ch12

Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science*, *126*, 1271–1280. https://doi.org/10.1016/j.procS.2018.08.070

Tikadar, S., & Bhattacharya, S. (2019). How Do They Use Their Smartphones: A Study on Smartphone Usage by Indian Students. In *IFIP Conference on Human-Computer Interaction* (pp. 132–151). https://doi.org/10.1007/978-3-030-29387-1_8

Vaidya, D. A., Pathak, V., & Vaidya, A. (2016). Mobile Phone Usage among Youth. *International Journal of Applied Research and Studies*, *5*(3). https://doi.org/10.20908/ijars.v5i3.9483

Vijayakumar, P. . (2016). Growing cyber crimes in India: A survey. In *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*. Retrieved from https://ieeexplore.ieee.org/abstract/document/7684146

Wai, I. S. H., Ng, S. S. Y., Chiu, D. K. W., Ho, K. K. W., & Lo, P. (2018). Exploring undergraduate students' usage pattern of mobile apps for education. *Journal of Librarianship and Information Science*, *50*(1), 34–47. https://doi.org/10.1177/0961000616662699