Man In India, 97 (24) : 333-344

SMARTPHONE SECURITY BEHAVIOUR OF THE INDIAN SMARTPHONE USER

Teena Bagga[1], JS Sodhi[2], B. Shukla[3] and Mir Arsalan Qazi[4]

Various researches have revealed that users are complacent regarding smartphone security behaviour. This is paradoxical, because users perceive information stored on their smart devices to be privileged and worth protecting. Conventionally, not much consideration is given to human aspects compared to technical security mechanisms (like firewalls and antivirus), but there is an essential requirement to study human factors as technology in itself is inadequate in delivering comprehensive security solutions. The core objective of this research was to study the usage patterns of smartphone users, determining whether a general level of security complacency exists amongst smartphone users. The study was undertaken in an Indian context (a multi-cultural developing nation) and incorporated demographics as a variable in evaluating any disparities in smartphone security awareness amongst population groups. A structured questionnaire was deployed online to gather responses. A survey of 150 users assessed trust in smartphone application repositories, users' contemplations while installing new applications, and their usage of security mechanisms (security controls). The results shows that, smartphone users are aware of various security threats as well as the security software available. They also showed a high level of trust in official application repositories. In addition, there found to be a significant relationship between a user's level of information security knowledge and their behaviour. The most interesting finding from this research reveals that despite of being knowledgeable and aware of various security aspects generally people are causal in attitude and rarely protect their devises.

***Keywords*:** Smartphone, Security Awareness, Mobile Security

Introduction

The first smartphones were launched around the year 2007 by Apple and Google and ever since then, they have become nearly pervasive in the modern world. They exist in countless varieties and have become increasingly affordable over the recent few years. The features offered by them are of immense help for private daily tasks as well as for business assignments. Smartphones provide a broad range of connectivity options and can be online around the clock, presenting up-to-date information any time of the day, while also providing the likelihood to send arbitrary information to virtually anyone at the same time. Nowadays smartphones possess the same processing power that normal PCs had a decade ago but are small enough to fit into everybody's pocket. Their popularity is also due to the vendors who make certain that users have straightforward access to new applications and, consequently, be able to realise new use scenarios for their smartphones. Although

[1] Associate Professor, Amity Business School, Amity University Uttar Pradesh

[2] Vice President & CIO-Amity Education Group

[3] Professor of Entrepreneurship and Leadership, Amity University, Noida, Uttar Pradesh

[4] Student-MBA, Amity Business School, Amity University Uttar Pradesh.

some apps are paid and need to be purchased before they can be installed on a smartphone, the majority can be installed and used free of charge which has turned out to be a contributing factor to the smartphone's ever increasing popularity.

It has been seen that smartphone users have a habit of ignoring security messages that are prompted to them (Mylonas *et al.*, 2013). This is a vulnerability that disrupts the trust model of smartphone security. It has also been known that users seldom consider privacy and security when installing new applications and also do not sufficiently protect themselves by implementing smartphone protection mechanisms (Ophoff and Robinson, 2014). This is true even for younger, technology-savvy generations which have had access to mobile devices at an early age. Studies conducted on students showed that they did not pay considerable attention to smartphone protection mechanisms (Park and Drevin, 2016). In the Indian context, research has found that students pursuing higher education are not unaware about security issues, but are not informed about all the security risks and practices (Pramod and Raman, 2014). While there are numerous free security applications available on the application repositories to secure mobile devices, they are not pervasive among smartphone users (Alkaldi and Renaud, 2016).

Information Security

Information security or InfoSec is a collection of guidelines for managing the processes, tools and policies essential to avert, detect, document and counteract threats to digital and non-digital information. Infosec tasks consist of establishing a set of business processes that will safeguard information assets irrespective of how the information is formatted or whether it is in transit, is being processed or is at rest in storage. Infosec programs are constructed around the fundamental objectives of the CIA triad: preserving the confidentiality, integrity and availability of IT systems and business data. These points guarantee that sensitive data is only revealed to authorised individuals (confidentiality), avoid unauthorised alteration of data (integrity) and guarantee the data can be retrieved by authorised parties when demanded (availability). According to Peltier (2013), people are the biggest threat to information security. Peltier also describes how awareness can be made to happen and gives a set of information security skills required for a particular awareness program namely; the job, the environment, group culture and management.

Smartphones

Smartphones are mobile computational devices that merge the functionalities of traditional cell phones and contemporary portable computers. In addition to having a connection to mobile phone networks, smartphones can be categorised as mobile devices having a large screen, sufficient processing power and memory, and an operating system that is extensible with third-party software or applications. The

usage of smartphones is consistently growing along with the number of smartphone third-party applications or "apps". These applications can be downloaded and installed in a very small number of steps through so called "App stores". These app stores deliver applications in a centralised manner from app repositories or app markets. The app repositories can be either official, i.e. provided by the smartphone platform (e.g. Google Play), or unofficial (e.g. Amazon App store for Android). Although there have been many devices which have been touted as the "first" smartphone, however Apple which, in early 2007, introduced the iPhone, was one of the first smartphones to utilise a multi-touch interface. The iPhone was noteworthy for its usage of a large touchscreen for direct finger input as its main method of interaction, in place of a stylus, keyboard, or keypad, characteristic for smartphones at the time. In October of 2008, the first phone to run Android, known as the HTC Dream (also called the T-Mobile G1) was released. Ever since then, smartphones have evolved at a rapid pace and the technology involved in these devices has progressed by light years. Nowadays, a typical smartphone has the same computational power that a supercomputer possessed in the 1980s.

Smartphone Security Mechanisms

Hoffman (2014) described a set of security mechanisms for a smartphone which are given as:

> ***User Authentication:*** Similar to a normal PC, users normally must authenticate in some way before the smartphone can be used. Most of the time users authenticate with a secret PIN and unlock the SIM card in order to get access to the SIM provider's telephony services. There exist several login mechanisms, but the major smartphone operating systems typically offer at least one of the following: (1) Patterns (2) PIN (3) Passphrase (4) Fingerprint Lock
>
> ***Sandboxing:*** Most mobile operating systems additionally run applications in some sandbox which further delegates access to some API functions and adds additional security checks. Android for example runs most applications under a separate user id and inside the Android Runtime (ART) which provides a complete API for applications and delegates necessary functionality to system libraries or the kernel while performing (additional) security checks.
>
> ***Permission System:*** The operating systems typically restrict access to services which could be exploited by attackers and where misuse could have negative effects for the user. This includes all functionality which occur costs, such as sending a SMS or establishing a phone call. Functionality related to sensitive or private information is also often controlled by permissions, e. g., serial numbers or databases storing contacts or chat messages etc. Access to certain hardware devices is also usually protected, e. g., the camera or the GPS sensor.

Knowledge, Attitude and Behaviour of Smartphone Users

Studies have shown that privacy, as well as security knowledge and global data privacy concern, are significantly influential for mobile protection behaviour. It has also been seen that low knowledge and low global information privacy concern can function as predictors for the non-usage of protection methods, while high knowledge and high concern can help in predicting the usage of smartphone protection mechanisms (Kraus *et al.,* 2014). Recent studies have also shown that smartphone users are capable of recognising a reasonable collection of threats and mitigations related to smartphone use (Kraus *et al.*, 2015). While smartphone users are concerned about security for their device, wanting added security, yet they do not engage with the security mechanisms that already exist (Clarke *et al.,* 2016). Other studies have discovered that smartphone users are complacent when it comes to information security, exhibiting high levels of trust for smartphone application repositories, seldom taking into thought privacy and security considerations when installing new applications and, additionally, not sufficiently protecting themselves through implementation of smartphone protection mechanisms (Ophoff and Robinson, 2014). Research has also found peculiar differences in security knowledge as well as attitude between genders (Pramod and Raman, 2014) (Ophoff and Robinson, 2014).

Rationale of the Study

Typically, human aspects of information security are not given considerable thought compared to technical security mechanisms. It is a must to study the human aspects as security cannot be complete without taking them into consideration, because technology alone cannot deliver comprehensive security solutions. Increasing a user's knowledge may lead to an increase in compliance with effective security habits (Kraus *et al.,* 2014). Also, for instructors and educationalists to make helpful security awareness resources, they should have a detailed understanding about users' pre-existing behaviours, knowledge, misunderstandings and general attitude with regard to smartphone security. The purpose of this study is, therefore, to analyse the behaviour that smartphone users exhibit when using their smartphones, with respect to information security. It attempts to gain an insight into their knowledge about information security, attitude towards information security and, finally, their behaviour while using their smartphones.

Demographic Profile

Table 1 presents the demographic profile of the respondents' which shows that the majority were male students below the age of 25 years, with an annual income of less than ₹ 5 lakhs per annum. The second largest age group was between the range of 25 and 35 years with none of the respondents being above the age of 55 years. It is also pertinent to mention here that forty percent of the respondents were

TABLE 1: DEMOGRAPHIC PROFILE OF RESPONDENTS

	Frequency	*Percent*	*Cumulative Percent*
	Gender		
Male	93	62	62
Female	57	38	100
	Age		
Below 25	73	48.7	48.7
25 to 35	66	44.0	92.7
35 to 45	8	5.3	98.0
45 to 55	3	2.0	100.0
	Occupation		
Employed Full-Time	60	40.0	40.0
Employed Part-Time	13	8.7	48.7
Unemployed	4	2.7	51.3
Student	73	48.7	100.0
	Annual Income		
Below ₹ 5 Lakhs	109	72.7	72.7
₹ 5 Lakhs to ₹ 10 Lakhs	26	17.3	90.0
₹ 10 Lakhs to ₹ 15 Lakhs	3	2.0	92.0
₹ 15 Lakhs to ₹ 20 Lakhs	1	0.7	92.7
Above ₹ 20 Lakhs	11	7.3	100.0
	Computer Experience		
Beginner	7	4.7	4.7
Average	101	67.3	72.0
Expert	42	28.0	100.0
Total	**150**	**100**	

employed full-time, whereas none of the respondents was retired. However, four of the respondents reported to be unemployed. Also, as expected, the largest number of respondents, close to seventy percent, perceived themselves to have average computer experience and over a fourth of them believed that they were experts. Only seven respondents thought that they were beginners at computers.

Ownership, OS and Usage Characteristics

TABLE 2: OWNERSHIP, OS AND USAGE CHARACTERISTICS

	Frequency	*Percent*	*Cumulative Percent*
	Ownership		
Smartphone	146	97.3	100
Tablet	37	24.7	100
PC/Laptop/Netbook	116	77.3	100
Total	297	199.3	
	PC Operating System		
Mac OS	13	8.7	8.7
Microsoft Windows	131	87.3	96.0
Linux	1	0.7	96.7
I Don't Know	1	0.7	97.3

contd. table 2

	Frequency	*Percent*	*Cumulative Percent*
Other	4	2.7	100.0
Total	150	100	
Smartphone Operating System			
Android	88	58.7	58.7
Apple iOS	54	36.0	94.7
Windows Mobile	2	1.3	96.0
Blackberry OS	2	1.3	97.3
Other	4	2.7	100.0
Total	150	100	
Smartphone Usage in a Day			
From 1 to 2 hours	15	10.0	10.0
From 2 to 3 hours	25	16.7	26.7
From 3 to 4 hours	34	22.7	49.3
More than 4 hours	76	50.7	100
Total	150	100	
Installation of New Applications			
Frequently	19	12.7	12.7
Occasionally	29	19.3	32.0
Sometimes	63	42.0	74.0
Rarely	38	25.3	99.3
Never	1	0.7	100.0
Total	150	100	

Table 2 shows the ownership of other devices such as PCs and tablets in addition to smartphones as well as the PC operating system as well as the operating system of the smartphones used by the respondents. It also shows smartphone usage characteristics such as the number of hours spent in a day while using smartphones and also the frequency of installation of new applications.

In Table 2, we can see that a large majority of smartphone users also own a PC or Laptop. However, not many respondents own a tablet. When it comes to the operating system of their devices, the majority of respondents reported to have Microsoft Windows on their PCs and Android on their smartphones. It is pertinent to mention here that Android and iOS together consisted of close to 95% of the respondents which goes on to show that these smartphone operating systems have overwhelmed the competition and are the only two competing players in the smartphone arena. Coming to the number of hours spent using a smartphone in a day, close to three-quarters of the respondents reported to be spending more than three hours a day using their smartphones and over half of the total respondents spent well over four hours a day on their smartphones. Only 10% of the respondents reported to be spending no more than two hours a day using their smartphones. This goes on to show that smartphones have become an essential part of peoples' lives and they spend a substantial duration of their time using them. Now, when it comes to installing new applications on their smartphones, the majority reported

that they "sometimes" installed new applications i.e. a few times a month. Over a quarter of responded with "rarely" (about once a month) while there were only close to 13% of respondents who installed new applications "frequently" i.e every other day.

Usage of Security Software

TABLE 3: USAGE OF SECURITY SOFTWARE

Device	*Frequency*	*Percent*	*Cumulative Percent*
Smartphone	78	52	100
Tablet	26	17.3	100
PC/Laptop	106	70.6	100
None of the above	18	12	100

Table 3 shows the usage of security software by respondents on various devices that they own. This was a multiple-choice question and respondents were free to choose as many options as they wanted with the exception of the "none of the above" option which, for obvious reasons, could only be selected exclusively. From the responses to this question, it was observed that only a little over half of the smartphone users reported to have been using security software on their smartphones, with the percentage at 52%. The highest usage of security software was observed to be on PCs with 70.6% of the respondents reporting that they used security software on their PCs or laptops. It also came to light that 12% of the respondents did not use security software on any of their devices.

Knowledge, Attitude and Behaviour

TABLE 4: MEAN VALUES FOR KNOWLEDGE, ATTITUDE AND BEHAVIOUR

	Frequency	*Mean*	*Standard Deviation*
Knowledge			
Applications in the official repository are secure for installation on my device	150	3.64	1.045
I think that applications in the official repository have undergone security application testing before I have download them	150	3.54	1.001
I am aware of the existence of smartphone malicious software (worms, viruses, etc.)	150	4.02	0.886
I am aware of the existence of smartphone security software (firewall, antivirus, etc.)	150	3.93	0.913
I am aware of all the security features available on my smartphone	150	3.81	1.054
Attitude			
I am concerned about the privacy and protection of my personal data	150	4.48	0.953
Smartphones are more secure than PCs or Laptops	150	2.83	1.163

Contd. table 4

	Frequency	*Mean*	*Standard Deviation*
Smartphone software security is essential	150	4.31	0.741
Security features add hassle to my smartphone experience	150	3.27	0.919
The information stored on my smartphone is important	150	3.97	0.976
Behaviour			
I pay attention to the security prompts that appear during the installation of a new application on my smartphone	150	3.65	1.069
I prefer installing a pirated version of a paid application instead of buying the original	150	3.11	1.185
I have searched the application repository for free smartphone security software	150	3.37	0.959
I store personal data on my smartphone	150	3.56	1.052
I store business data on my smartphone	150	3.31	1.164

Table 4 showcases the various statements regarding knowledge, attitude and behaviour of smartphone users which were rated by respondents on a Likert scale where 1 stood for "strongly disagree" and 5 meant "strongly agree". It is pertinent to mention here that 3 stood for "undecided". Keeping this in mind, the mean value of all the responses for a particular statement was calculated. This mean value was then used to determine the level of agreeableness or disagreeableness of respondents towards a particular statement.

It is interesting to note that respondents agreed that they were aware of smartphone malicious software as well as the security software for smartphones. They also strongly agreed that smartphone software security is essential yet believed that smartphones are not more secure than PCs. Also, they perceived the information stored on their smartphones to be important and were concerned about the privacy and protection of their personal data. When it came to the behaviour of respondents, it was seen that they paid attention to the security messages that appeared during the installation of new applications but not necessarily enough since the mean was calculated to be 3.65. Furthermore, respondents also reported to have installed pirated applications on their smartphones and searched the application repository for free smartphone security software.

For further analysis, the average mean for each category of statements i.e. knowledge, attitude and behaviour was calculated and was used to determine the differences among different groups of respondents with respect to these factors.

An independent sample t-test was conducted to determine if there is any significant difference between males and females when it comes to their knowledge, attitude and behaviour. Various earlier studies had conflicting views on this subject (Ophoff, J. and Robinson, M., 2014) (Pramod, D and Raman, R. 2014) since some showed differences while others didn't. From the results of current research it is

evident that there is a significant difference between the knowledge level of males (mean :3.67) and females(mean: 4.02) when it comes to smartphone security whereas they are same in terms of their attitude and behaviour towards information security. Further, no significant difference found among the respondents of various age group based on the ANOVA test.

Difference Between Males and Females Regarding Perceived Level of Security

TABLE5: INDEPENDENT SAMPLE T-TEST FOR MALES AND FEMALES REGARDING PERCEIVED LEVEL OF SECURITY FOR SMARTPHONE PROTECTION MECHANISMS, DF: 143

Mechanism	*Male Mean*	*Female Mean*	*t-value*	*Significance*
File Encryption	3.69	3.08	3.679	.000
Device Password Lock	3.42	3.75	2.235	.027
Device PIN	3.39	3.65	1.669	.097
Biometric Lock	4.20	3.12	6.013	.000
Remote File Deletion	3.18	3.15	0.176	.860
Device Locator	3.69	3.35	1.881	.062

An independent sample t-test was conducted to determine if there is any significant difference between males and females when it comes to the perceived level of security for various smartphone protection mechanisms. From the results of Table 5, it can be inferred that the significance level for file encryption, device password lock and biometric locks is less than .05. This leads us to conclude that there is a significant difference between males and females when it comes to the perceived level of security for smartphone protection mechanisms. Male tend to use more of File Encryption and Device PIN and Female prefer Device Password Lock as security measure.

Relationship Between Knowledge of Smartphone Users and Their Behaviour

TABLE 6: MODEL SUMMARY

Model	*R*	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	.307[a]	.094	.088	1.111

(Constant: Knowledge of Smartphone Users)

TABLE 7: ANOVA

Model		*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig.*
1	Regression	18.965	1	18.965	15.377	.000b
	Residual	182.529	148	1.233		
	Total	201.493	149			

(Dependent Variable: Behaviour of Smartphone Users)

TABLE 8: COEFFICIENTS

Model		*Unstandardized Coefficients*		*Standardized Coefficients*		
		B	*Std. Error*	*Beta*	*t*	*Sig.*
1	(Constant)	.600	.575		1.044	.298
	Knowledge_Mean	.588	.150	.307	3.921	.000

(Dependent Variable: Behaviour of Smartphone Users)

The regression model with knowledge as a predictor of behaviour produced R square = .088, $F(1,148) = 15.377$, $p<.05$, indicating that there is a regression rate of 8% which shows the impact of knowledge of smartphone users on their behaviour.

The result indicated in Table 6,7 and 8 shows that there is a significant relationship between the knowledge and behaviour of smartphone users, leading to knowledge affecting the security behaviour of users when using their smartphones. This is an important result to consider because it goes on to show that knowledge affects the behaviour of smartphone users when information security is concerned and that augmenting a user's knowledge about information security can lead to better behavioural practices when it comes to smartphone security risks and threats. However, the low value of R square suggests that this change in behaviour may not be consistent across all the users as it may lead to a considerable change in the behaviour of one user, while not substantially affecting the behaviour of another user. Therefore, this relationship needs to be further explored and it needs to be examined that to what degree the security behaviour of smartphone users changes in accordance with increase in their knowledge.

Key Findings

Many findings were generated with the help of this research report which helped gain an insight into the information security knowledge, attitude and behaviour of Indian smartphone users. First and foremost, it came to light that smartphone users use their smartphones for long durations on any given day, suggesting that they consider their smartphones a part of their daily lives and cannot get by with doing their daily tasks without a smartphone on their person. Another observation was that Android and Apple iOS are the only two dominant smartphone operating systems in the market today and any other operating systems are only an insignificant minority. As for the awareness level of smartphone users regarding various security threats and security software available, there is a reportedly high level of knowledge in case of both threats as well as security software available. Users also showed a high level of trust in official application repositories and believed that applications in the said repositories underwent security testing and were secure for installation on their devices. Users also showed concern about the data stored in their

smartphones because they believe that the data stored on their smartphones is important and also because they think that smartphones are not as secure as PCs or laptops. When it comes to the behaviour of smartphone users, it was observed that more users store personal data on their smartphones than business data. Another interesting observation was that users also reported installing pirated applications on their smartphones instead of buying them off official application repositories.

On further analysis, it was found that males and females varied significantly when it came to their level of information security knowledge. However, there was no significant variation in either attitude or behaviour. Also, it was observed that different income groups were significantly varied when it came to their level of knowledge as well as behaviour. However, attitude towards security was not found to be significantly varied. Moreover, no significant difference was found for the knowledge level, attitude as well as the behaviour between different age groups. Moving further, it was also found that there was a significant difference between males and females when it came to expected level of security while performing various tasks on their smartphones. Different income groups also exhibited a significant difference in this case. Additionally, when it came to the perceived convenience and security level of different smartphone protection mechanisms, again, males and females showed a significant difference but income groups only showed a significant difference in case of perceived level of security and not for convenience. Lastly, the relationship between the knowledge level of users and their behaviour was examined and it was observed that there is a significant relationship between a user's level of information security knowledge and their behaviour in the context of security when using their smartphone. However, this relationship was not proved to be consistent as there were implied variations when it came to the degree of the relationship. Perhaps, the most enlightening finding from this research was that in spite of users being knowledgeable and aware of smartphone threats and security software, perceiving the data stored on their smartphones to be important, being concerned about the privacy and protection of their personal data, and believing smartphone security to be essential, only about half of the users employed security software on their smartphones.

Conclusion

This research attempted to quantify the factors affecting the behaviour of smartphone users in India with respect to information security and made an effort to learn how those factors affected the said behaviour. In addition to gain insight into the security behaviour of smartphone users and from the obtained results, implications can be derived which can help people such as instructors in designing course material for security programmes. One of the major results i.e. the lack of usage of smartphone security software in spite of the adequate knowledge should tell application developers that they need to better their software because users may perceive them

as adding hassle to their smartphone experience, as users value convenience a lot when it comes to employing smartphone protection mechanisms. They tend to use simple, less secure mechanisms over complicated, more secure ones. Therefore, there is a need to integrate convenience and security so that users find smartphone software easy to use. Also, the significant differences between gender and income groups regarding the knowledge level of users, as well as the perceived level of security regarding various smartphone protection mechanisms needs to be studied in more detail as it can provide to be useful in further exploring the effect of knowledge on the behaviour of smartphone users, as well as help in perfecting the smartphone protection mechanisms to better suit the needs of users. Finally, the magnitude of the effect of information security knowledge imparted and the subsequent effect on smartphone users' needs to be examined further as this study found a significant relationship between the level of knowledge and the behaviour of smartphone users, albeit with high variability.

References

Alkaldi, N., & Renaud, K. (2016). Why Do People Adopt, or Reject, Smartphone Password Managers?. In *1st European Workshop on Usable Security, Darmstadt* (Vol. 18, pp. 1-14).

Hoffmann, J. (2014). *From Mobile to Security* (Doctoral dissertation, PhD thesis, Ruhr-Universitt Bochum).

Kraus, L., Fiebig, T., Miruchna, V., Möller, S., & Shabtai, A. (2015). Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy. *S&P. IEEE*.

Kraus, L., Wechsung, I., & Möller, S. (2014). A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. In *Workshop on Privacy Personas and Segmentation* (p. 2014).

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

Ophoff, J., & Robinson, M. (2014). Exploring end-user smartphone security awareness within a South African context. In *Information Security for South Africa (ISSA), 2014* (pp. 1-7). IEEE.

Park, M., & Drevin, L. (2016). An investigation into the security behaviour of tertiary students regarding mobile device security.

Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security.

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security.