ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse285952020.pdf
https://doi.org/10.30534/ijatcse/2020/285952020

Cybersecurity Behavior of Smartphone Users in India: An Exploratory Sequential Mixed Methods Approach

Pintu R Shah[1], Anuja Agarwal[2]
[1]SVKM's NMIMS Mukesh Patel School of Technology Management & Engineering, India, pintu.shah@nmims.edu
[2]SVKM's NMIMS Mukesh Patel School of Technology Management & Engineering, India, anuja.agarwal@nmims.edu

ABSTRACT

India is experiencing tremendous growth in the smartphone market, and mobile data usage is increasing. As India moves towards a digital economy, it is required that the Indians securely access digital services. Hence, it is essential to understand smartphone users' attitude, behavior, and security practices in India. Limited research is available about smartphone users' cybersecurity behavior in India, as the majority of research in this domain is done in the western country. This article reports the results of an exploratory sequential mixed method design. The main patterns of the qualitative user study are: (1) interviewed users' are aware of cybersecurity threats; (2) interviewed users' are motivated to protect their smartphone and data but lack the ability to do so; (3) difference in security behavior of digital natives and digital immigrants. A quantitative user study further validated these patterns.

Key words: Cybersecurity behavior, Human aspect, India,Mixed method approach,Smartphone user, User behavior

1. INTRODUCTION

The smartphone has become the most popular personal device because of mobility, portability, and increasing capability. There is a worldwide growth in the number of smartphone users including India.It is estimated to reach 974 million by 2025 in India [1]. Mobile banking is the fastest growing digital platform [2]. With the increased smartphone usage, sensitive data like contacts, emails, photos, and videos are stored and processed on it. This makes the smartphone an attractive target for hackers [3, 4].

Citizens of developed countries have more experience in the usage of Information and Communication Technology(ICT). Their journey started with using desktops, followed by laptops and tablets, and then graduated using ICT through their smartphone. In this journey, they learned the vulnerabilities associated with the security of data communication and devices such as virus attacks, hacking, etc. as technology stepped up. In contrast, the smartphone is first computing device for many Indians. They lack the experience of handling cyber-related threats. Hence, there is a need to study the cybersecurity behavioradopted by smartphone users in India for securing their smartphones and data. This study attempts to answer the following questions:

1. Are smartphone users aware of cybersecurity threats to their device and data?
2. Are they motivated to use recommended cybersecurity measures to protect their smartphone and data?
3. Is there a difference in the cybersecurity behavior of a person who grew up using digital devices from a very young age (referred to as digital native) and people who have adopted some aspects of new technologies (referred to as digital immigrants)?

The main contributions of this study are:

1. To the researchers' knowledge, this is the first study to use exploratory sequential mixed methods research design for understanding the cybersecurity behavior of smartphone users in India.
2. This study provides insights into the adoption and awareness of various cybersecurity practices of smartphone users in India. Such an understanding of smartphone users' behavior in India may be considered for the development of the SETA program and default settings on the smartphone.

2. BACKGROUND AND RELATED WORK

Cybersecurity is complex involving technology, people, and processes. Technical controls are not sufficient to achieve cybersecurity. A substantial percentage of cybersecurity incidents involve human errors [5]. Literature suggests that humans are the weakest link [6, 7]. Cyber hygiene exhibited by the human user will improve cybersecurity. A considerable amount of research is conducted to understand cybersecurity behavior and practices followed by smartphone user, their motivation, attitude, and ability to protect smartphones and data from cyber-threats [8, 9, 10, 11]. However, the majority of such research is done outside India. Not much research

studies on the cybersecurity behavior of smartphone users in India are available [12, 13]. Culture plays a role in decision-making when avoiding cybersecurity risk [14]. Hence, there is a need to study cybersecurity behavior exhibited by smartphone users in India, a culturally different country.

3. RESEARCH METHODOLOGY

Qualitative research methods are useful for understanding user needs and behaviors and evaluating the use of technology in context[15]. A qualitative method can reveal new information and provides insights into users' experience, beliefs, thoughts, and motivations. Face-to-face, semi-structured interviews were considered the most suitable primary data collection tool to access this knowledge and enable flexible, in-depth exploration of the issue. Quantitative methodologies are useful to answer questions that addresscausality, generalizability, or magnitude of the effect. Mixed methods research draws on the strengths of both qualitative and quantitative research [16].

Quantitative empirical research is the dominant research methodology in studying information security awareness and behavior, whereas very little qualitative empirical research is conducted [17, 18]. Hence, to get the advantage of both types of research methodology, an exploratory sequential mixed method design is used in this study to understand the cybersecurity behaviorof the smartphone user. The researchers started with the qualitative method, followed by the quantitative method. The researchers used this strategy to see if data from a small set of individuals (in the qualitative phase) can be generalized to a large sample of the population (in the quantitative phase). The study flow is shown in figure 1.

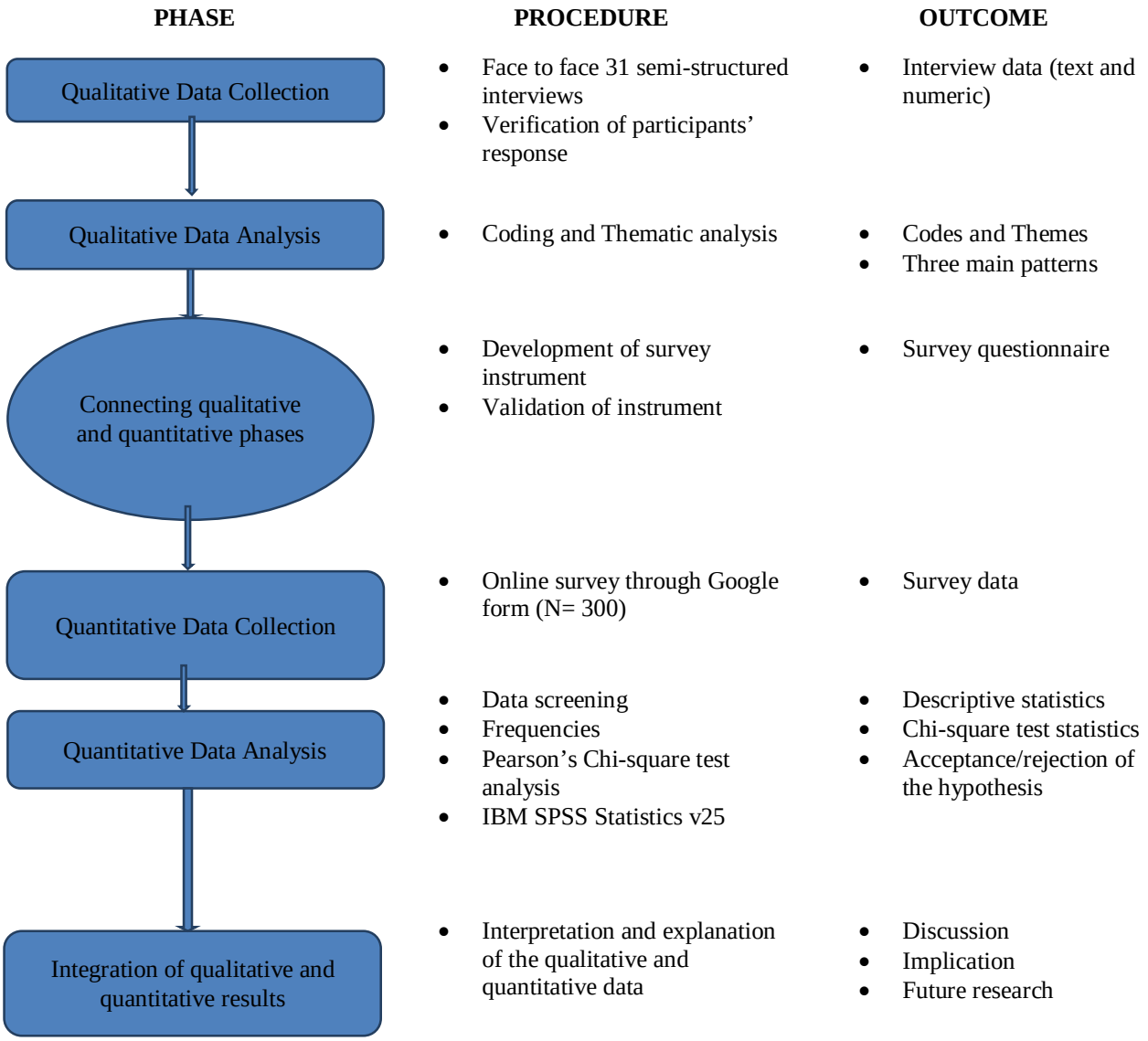

Figure 1: Study Flow

The number of participants in the qualitative phase was decided based on: (1) the objective of the study; and (2) theoretical saturation [15]. Participants were selected using a convenient sampling method. The researchers verified participants' responses on their smartphones wherever possible. One of the researchers conducted semi-structured interviews with 31 users to understand their security behavior and practices. Interviews were conducted in multiple languages. Interview questions were divided into two parts. The first part focused on demographic information like gender, age, marital status, occupation, education, and work experience. The second part focused on various cybersecurity practices and behavior. The most common cybersecurity threats and recommended countermeasures were identified based on the literature review. The researchers identified malware, phishing, unauthorized access to smartphone devices, and data stored on it because of lost or stolen smartphone and data loss as the most prominent threats[19, 20, 21, 22]. The researcher asked the participant to show their smartphone setting so that the researcher can verify the user's responses. The researcher also looked at the user's social network application for location-based updates. To understand the user's level of awareness about security threats, the researchers asked them to explain terms like ransomware, phishing, malware, hacker, identity theft, etc.

Three patterns were identified after an analysis of the data collected during the qualitative phase. A quantitative methodology was used to validate the identified trends. The survey questionnaire was developed based on identified cybersecurity behaviors and practices. The reliability of the questionnaire was tested using Cronbach alpha. The Cronbach alpha coefficient for 28 items in the questionnaire was 0.761, which is accepted as reasonable [23]. Table 1 gives the respondents' demographic profile in phase 1(Qualitative) and phase 2 (quantitative) of the study. Responses were analyzed using statistical software for frequency analysis and other statistical tests.

Table 1: Count for demographic variables

Demographic Variables		Quantitative Phase (N=31)	Qualitative Phase (N=300)
Gender	Male	22	175
	Female	9	125
Age	<=25	12	153
	26-40	15	102
	>40	4	45
Marital Status	Married	15	184
	Unmarried	16	116
Occupation	Businessman	7	25
	Housewife	1	19
	Student	12	149
	Employee	11	107
Education	High School and Diploma	2	11
	Undergraduate	20	186
	Post Graduate and above	9	103
Work Experience	<=1 year	12	143
	2 to 10 years	4	87
	more than 10	15	70

4. RESULT ANALYSIS AND DISCUSSION

This section presents the result and analysis of the qualitative and quantitative phases. The objective of this research is to validate the trends emerging from the qualitative analysis with quantitative analysis. Major patterns emerging from the semi-structured interviews are presented along with supportive evidence from quantitative analysis. Three main findings of the semi-structured interviews are: (1) users' are motivated to protect their smartphone and data but lack the ability to do so; (2) users' are aware of cybersecurity threats; (3) differences in security behavior of digital natives, and digital immigrants.

Users' are motivated to protect their smartphone and data but lack the ability to do so:

The majority of the participants said that they are motivated to protect their smartphones and data. One of the participants said that *"it is the user's responsibility to protect data and phone*." Another participant expressed it as "*My actions are the key for security of my phone and data. Security features of the phone can provide security only if I use it correctly"*. Table 2 shows the percentage of participants who were aware of and/or adopted cybersecurity-related behaviors.

Table 2: Cybersecurity behavior adoption

Behavior	Quantitative Phase	Qualitative Phase
Auto Update	48.39%	41.67%
Authentication	74.19%	87.67%
Noting IMEI Number	61.29%	46.00%
Remote Track	61.29%	51.33%
Remote Lock	32.26%	39.33%
Remote Wipe	35.48%	35.00%

The researchers can infer from table 2 that the users adopted popular security measures like authentication. However, other cybersecurity measures were poorly adopted. Figure 2 shows the percentage of the breakup of the authentication mechanism used by the participants. Figure 3 shows the motivation rating of the participants.

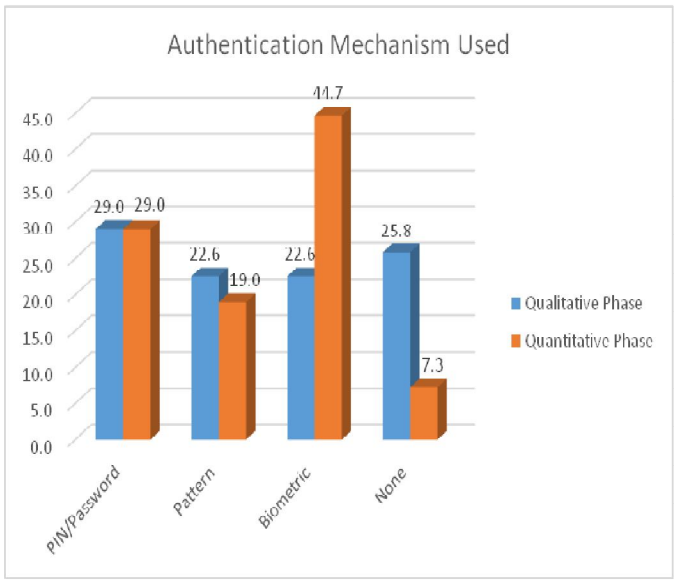

Figure 2: Authentication mechanism used by participants

Users' are aware of cybersecurity threats but do not deploy protection mechanisms: To understand user perception and awareness about cybersecurity threats, the researchers asked participants to describe various cybersecurity threats like ransomware, virus, phishing, identity theft, etc. The majority of the participants were aware of the meaning of ransomware, virus, phishing, etc. The main sources of information about cybersecurity threats were newspapers, TV news, friends, and colleagues through WhatsApp, social media, etc. Figure 4 shows the percentage response of the participants to a question on awareness.

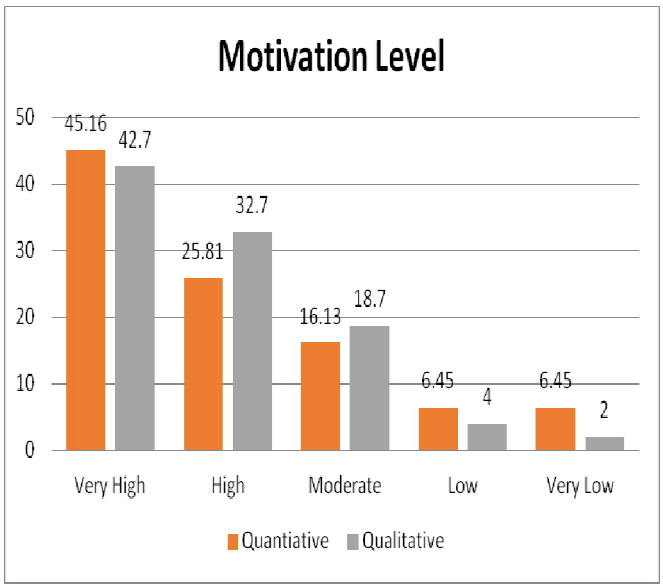

Figure 3: Motivation rating by participants

Researchers observed that the digital natives were very much aware of the security threats and had adopted some of the recommended cybersecurity controls. However, participants with 30 years or more were aware but complacent in adopting cybersecurity controls.

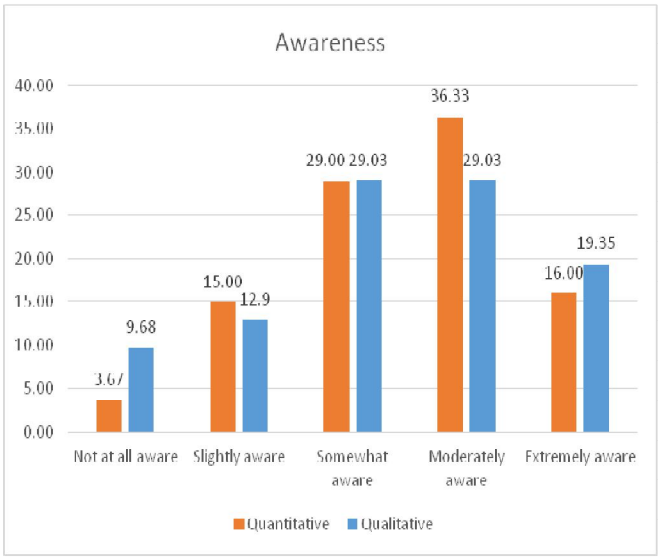

Figure 4: Threat awareness of participants

The difference in the security behavior of digital natives and digital immigrants: The researchers were able to see the difference between the cybersecurity behavior of digital natives and digital immigrants[24]. Digital natives refer to the person grown up using computers and the Internet from a very young age. In contrast, digital immigrants are the people who have adopted many aspects of new technologies. Digital natives refer to the student participants in this study, and digital immigrants are all other participants. To meet Chi-Square test requirements the age variable was divided into two categories: (1) smartphone users less than or equal to 24 years of age; and (2) smartphone users greater than 24 years. The researchers conducted a chi-square test and found a significant difference ($\chi 2$ (1, N=300) =16.658, $p<0.001$) in the security control adoption score.

5. CONCLUSION

The results of the study show that users do not adopt many of the recommended security practices. Sometimes they are not aware of how to enable a specific security feature of a smartphone. Nevertheless, they state to be motivated and take responsibility for securing their device and data. Most of the security features can be easily enabled on the phone and are not time-consuming or difficult to use. This raises a question: *Why smartphone users in India do not adopt recommended cybersecurity controls when they state to be motivated to secure their smartphones and data?* This gap requires further investigation. The quantitative analysis validated the trends identified in the qualitative phase.

The results of this study cannot be generalized to the entire population of India because of its diversity and population of smartphone users. Instead, the results are the interpretation of some users' cybersecurity experiences in India. The

researchers used an exploratory sequential mixed method research design to understand the attitude, behavior, and the cybersecurity practices adopted by smartphone users in India. The security behavior of smartphone users in our study is similar to the users in other countries. Smartphone users in our study are complacent and have not adopted recommended security practices. The main patterns of the study are (1) users are motivated to protect their smartphone and data but cannot do so; (2) users are aware of cybersecurity threats; (3) there is a difference in the cybersecurity behavior of digital natives and digital immigrants. The patterns emerging of qualitative analysis were validated by quantitative analysis. This study's findings may be useful for the development of the cybersecurity awareness campaign.

REFERENCES

1. Statistica, “Number of smartphone users in India,” 2 October 2020. [Online]. Available: https://www.statista.com/statistics/467163/forecast-of-smartphone-users-in-india/.
2. RBI, “RBI Bulletin,” 6 April 2018. [Online]. Available: https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/43T10032018BD9C4CDD1050B489B94AF71C911936395.PDF.
3. R. Unuchek, “Mobile Malware Evolution 2017,” 7 March 2018. [Online]. Available: https://securelist.com/mobile-malware-review-2017/84139/. [Accessed 24 October 2018].
4. RSA, “RSA Quarterly Fraud Report: Q1 2020,” RSA, Bedford, MA, 2020.
5. IBM, “2019 Cost of Data Breach Study,” Ponemon Institute Research Report, IBM Security, 2019.
6. B. Schneier, Secrets and Lies, Digital Security in a Networked World, New York: John Wiley & Sons, 2000.
7. J. Green and P. Dorey, The Weakest Link, New York: Bloomsbury, 2016.
8. J. Ophoff and M. Robinson, “Exploring end-user smartphone security awareness within a South African context,” in Proceedings of the Conference on Information Security for South Africa (ISSA), 2014, Johannesburg, South Africa, 2014.
9. Das and H. U. Khan, “Security Behaviors of smartphone users,” Information and Computer Security, pp. 116-134, 2016.
10. X. J. Zhang, Z. Z. Li, and H. Deng, "Information security behaviors of smartphone users in China: an empirical analysis,” The Electronic Library, pp. 1177-1190, 2017.
11. F. Calderwood and I. Popova, “Smartphone Cybersecurity Awareness in Developing Countries: A Case of Thailand,” in Second EAI International Conference, Benin, 2019.
12. K. Gajjar and A. Parmar, “A Study of Challenges and Solutions for Smart Phone Security,” in Shetty N., Prasad N., Nalini N. (eds) Emerging Research in Computing, Information, Communication, and Applications, New Delhi, 2016.
13. P. R. Shah and A. Agarwal, "Cybersecurity behavior of smartphone users in India: An Empirical Analysis," Information and Computer Security, vol. 28, no. 2, 2020.
14. L.-C. Chen and D. Farkas, “An Investigation of Decision Making and the Tradeoffs Involving Computer Security Risks,” in AMCIS 2009 Proceedings, San Francisco, California, 2009.
15. Blandford, “Semi-structured-qualitative-studies,” 14 04 2018. [Online]. Available: https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/semi-structured-qualitative-studies.
16. J. Creswell and D. Creswell, Research design: qualitative, quantitative, and mixed methods approaches, Los Angeles: Sage, 2018.
17. B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, “Employees' Information Security Awareness and Behavior: A Literature Review,” in 46th Hawaii International Conference on System Sciences, 2013.
18. M. Silic and A. Back, “Information security Critical review and future directions for research,” Information Management & Computer Security, pp. 279 - 308, 2013.
19. M. A. Harris, S. Furnell, and K. Patten, "Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals," Journal of Information Privacy and Security, p. 186–202, 2014.
20. Z. Tu, O. Turel, Y. Yuan and N. Archer, “Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination,” Information & Management, pp. 506-517, 2015.
21. B. z. Markelj and I. Bernik, “Safe use of mobile devices arises from knowing the threats,” Journal of Information Security and Applications, pp. 84-89, 2015.
22. R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach and A. Shabtai, “Taxonomy of mobile users’ security awareness,” Computer & Security, pp. 266-293, 2018.
23. M. Tavakol and R. Dennick, “Making sense of Cronbach's alpha,” International Journal of Medical Education, pp. 53-55, 2011.
24. M. Prensky, “Digital Natives, Digital Immigrants Part 1,” On the Horizon, pp. 1-6, 2001.