ORIGINAL RESEARCH PAPER

Management

PERCEPTION ANALYSIS ON USING COMPUTER APPLICATIONS-A STUDY ON AAROGYA SETU APP

KEY WORDS: Mobile phones, Smart Phones, Computer applications, Cyber security risks, Financial frauds, Privacy, Covid 19, Aarogya Setu App

Dr. Hema Doreswamy	Professor-Finance Welingkar Institute of Management
Dr. Madhavi Lokhande*	Dean- Bangalore campus Welingkar Institute ofManagement*Corresponding Author
Prof. Radhika Uttam	Assistant Professor - Research Welingkar Institute of Management

ABSTRACT

Smart phone usage and various computer applications has become part and parcel of daily life of millions of individuals in India and across the globe. These apps help in doing day to day tasks in an efficient manner, it saves time and they are very user friendly. Be it financial transactions, online shopping, online education and so on, users find them extremely useful. Going forward, we can expect more and more people adopting smart phones and start using different types of applications. But, using apps also brings in considerable amount of risk for the users. If the users are not aware of such risks, they are exposed to considerable amount of risk and may become victims of financial frauds, hacking, privacy issues and other cyber security crimes. This research is conducted to understand the users' perception towards using applications and cyber security risks. The study is based on primary data and analysis is done with regards to Aarogya Setu app. This app was made mandatory by the government of India during the COVID-19 pandemic to track covid cases. The data collected through a questionnaire is analyzed using different tools and based on the analysis findings and suggestions are offered.

Introduction:

The usage of smart phones has changed the lifestyle of people over two decades. Smart phones are our best friend's replacing cameras, calculators, calendars, alarm clocks etc. The applications that we download for different purposes suchascommunication, socialization, business, finance, and shopping, gaming, entertainmenthave made life so easier than before. According to a research conducted by Similar web solutions some of the popular apps downloaded by people in India in the past two years are as follows: 1) Communication – Whatsapp, Messenger, True caller, Telegram, Google chrome, UC browser, Gmail etc. 2) Social: Facebook, Twitter, Instagram, helo, sharechat, snapchat etc. 3) Business: Whatsapp business, Zoom meeting, Google meet etc. 4) Finance: Google pay, Phonepay, Paytm etc. 5) Shopping: Amazon, Flipcart, Bigbasket, Jio mart etc. 6) Gaming: Candy crush, Pubg, Subway surfers etc. 7) Entertainment: You tube, Amazon Prime, Zee5, Hotstar etc.

"Every individual using a Smartphone is being watched". In order to use various applications a Smartphone user keeps his mobile data on or sometimes when there is wifi available a user will make use of it to access different apps not having enough knowledge how their information is being misused. Smartphone keeps a track of all the activities of the user through these third party applications; the places visited, meal had a restaurant, a facebook post liked, monetary transactions made, a movie watched in a multiplex or on OTT, conversations had with friends and family and the like.

The impact of Smartphone on our lives is severe. Apart from the benefits we derive from the usage there are certain threats. As Smartphone users we download third-party applications without considering the risk associated with it *(Mylonas A. 2013).*Smartphone are said to be vulnerable for several reasons, especially when a third party application is downloaded on it: a)personal data gets stored in it which possibly creates a chance for hackers through malwares *(Daojinghe2015)*b) the app developers get access to location which is used for future advertising but leads to privacy concerns of the users *(PritiJagwani 2015)* c) security threats could also be caused due to lack of awareness and understanding of security issues by few developers of the applications*(Miller 2011)*d)Most of the Smart phones don't have security software to protect data stored in it and also the operating systems don't get updated frequently like a PC *(J. Wright 2012).* However, users have to grant permissions requested by a particular app before downloading. It is users' choice to download or not to download an app. Therefore, privacy level of requested permissions would influence the users in deicing to download an app *(Hsiangchu La 2018).* Some apps demand more permissions than required that creates a susception for misuse of the personal information of the user *(Min Peng 2017).*Suchapps could be malicious apps.

Health care applications:

The Smartphones have also extended its utility in health care sector. The mobile health applications have gained lot of importance because of health awareness or consciousness among people.Majorclassification of these applications can be: a) Application for health care professionals b) Applications for medical students c) Applications for patients *(Mohammad Mosa 2012).* All these applications store customer's data and use the same for rendering them the required services. Suppose a customer/ user wants to order medicines through a mobile health app, he has to enter every information about his health along with the doctor's prescription and only then the order would be processed. Data security concern in this case would be a medical identity theft where the medical record of an individual could be altered or stolen and used to avail false medical treatments or purchase drugs to sell on the black market*(Adhikari 2014).* Recently, during the outbreak of COVID 19 pandemic many countries have launched a mhealth app for tracking COVID cases and control the spread of the disease. COVIDsafe app in Australia, COVID-19 Smart Management System (SMS) in South Korea, Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) in Germany, Trace together in Singapore, Arogyasetu in India etc., tracks users' location through Bluetooth and gives regular updates regarding the spread of the pandemic.

About Arogyasetuapplication

Arogyasetumeaning 'bridge to health 'is an application developed and launched by Government of India during the outbreak of the pandemic COVID-19. Some of the important features of the app are:

a) It updates users about the number of positive cases in the nearest proximity with the help of Bluetooth and GPS location.
b) Self assessment test can be taken by the user to detect the symptom of the disease.
c) Updates about the confirmed, recovered and deceased cases state wise are also available.Some of the best practices that could be followed to avoid the spread of virus can be found in the app.
d) Emergency helpline to help users in case of emergency.
The app is mainly useful in identifying the potential corona hotspots around user's location which acts as an intervention to control the spread.

Argoyasetu was launched on 2nd April 2020 replacing 'Corona Kavach' and had more than 50 million downloads within 13 days. The app is said to have become viral in India in a short span mainly because of the purpose of its launch 'tracking COVID cases' and also for it varied features making it user friendly.

Though the initiative is appreciated by WHO and World Bank some countries like Germany, Italy, and Singapore are not in favor of it. The main reason is the 'privacy of data' stored in app's server. There is no assurance from the government that the personal data of the citizens would not be used for any other purpose other than tracking COVID cases. The data security concerns of the citizens have emerged mainly due to two reasons:

a) The government had made it mandatory for all the citizens to download the app :
Few days after the launch of the app government had made it mandatory in workplaces (both public and private), travel through flight or train and any other public place all over the country. But after the controversies, it decided to be flexible and made it optional.

b) The app requires the user to keep Bluetooth on 'always on' mode: Through Bluetooth the app keeps a track of the user's location which leads to clear violation of someone's privacy. Those who are using the app are being watched 24/7.

Controversies on Aarogya Setu App:

The Software Freedom Law Centre, a consortium of lawyers, technology experts and studentshas expressed their view on the app. The data collected through Arogyasetu app is given to medical authorities who in turn make use of it for various interventions. There are high chances of data being transferred to other hands in the process and that brings in trust issues of people with the government. The government also declares that it cannot be held liable for the data leakage which is against the provisions of the IT Act. Therefore, if there is a breach of data the users are solely responsible for their act. **Pukhraj Singh,** Cyber-intelligence specialist, has recounted on several incidences where the data held by the government was being leaked or hacked and so he calls the app risky in that case.

Another concern of experts is the lifespan of the data stored in the app. The personal and sensitive information of individuals saved in the app gets deleted after 45 days. But there is no confirmation message sent to the user after deletion.Major risk arises when people download and install fake apps. Hackers have also come up with apps which looks similar to 'Arogyasetu'. When users download it and enter their personal information the data gets uploaded in their server and can be misused in several ways.

Though the 'Arogyasetu' app is beneficial in tracking the COVID cases and helped in inventions ithas been controversial in case of data security and privacy of the users. In this paper, we have tried to analyze the perception of users of various apps and specifically with regards to Aarogya Setu app which is made mandatory in several locations by the Government of India.

Methodology:

This study is conducted to understand the perception of users towards downloading and using different apps and in particular with reference to Aarogya Setu app. The study is conducted based on the data collected through a questinonnaire. Sample size of the respondents are 208 and the study was conducted in the city of Bengaluru. The questionnaire had 19 questions and respondents represented both males and females with different age groups and educational qualifications. The data collected is alanysed to bring out findings by using various statistical tools.

Objectives of the study:

1. To study mobile phone and smartphone usage pattern of the respondents
2. To analyze the awareness of smartphone users with regards to cyber security risk
3. To study the perception of respondents for Aarogya Setu app.
4. To analyse the relationship between qualification and perception of users towards cyber risk

Hypothesis:

Null Hypothesis (H0): There exists a significant relationship between qualification of the respondants and app usage awareness components like cyber risk and app downloading mechansism etc.

Alternate Hypohtesis (H1): There exists no significant relationship between qualification of the respondants and app usage awareness compnents like cyber risk, and app downloading mechansism etc.

Data Analysis tools applied: Data collected through questionnaire is analysed and interpreted by using percentage analsysis, chi-square test, graphs and charts.

Analysis and Results

Profile of the respondants:

- Primary data was collected through a questionnaire and a total of 208 respondants data is used for the analysis. Out of the total respondants 52% fall into the age group of 18 to 25 years, 26% belong to 26 to 35 years, 13% represent age bracket of 46 to 55 years and the rest belong to above 55 years age bracket.
- 52% of the respondants represent qualification between 12th and graduation, 42% are post graduates and 6% above post graduation.
- 60% of the respondnats have non-science/non-engineering background, 19% have engineering background and 21% have science background

Mobile phone and smart phone usage analsyis:

Usage of mobile and smart phone with regards to number of years by respondands is as mentioned in the below table. As it can be observed, smart phone usage has been there since 10 years and has grown exponentially ove the years.

Table 1 showing duration mobile phone and smart phone usage

Years of Usage	Numer of Respondants	
	Mobile phone	Smart phone
0-5 years	24	75
6 to 10 years	101	133
11 to 15 years	51	NA
more than 15 years	32	NA
Total	208	208

(Source: Primary Data)

Analysis of various Apps used by the respondants:

Most of the respondants acknowledge that they use various apps like social media apps, online shopping apps, apps for financial transactions, gaming apps etc. Being connected to family and fri neds was the most popular option chosen by the respondants followed by news/entertainment and knowledge/learning. Respondants also mentioned online shopping and online banking too as advantages of using smart phones. Few other things mentioned by the respondants are checking office mails, Google search, and maps. The below mentioned table provides the details (Note: Respondants were allowed to choose multiple options)

Table 2 showing Advantages of using smart phone from respondnats perspective

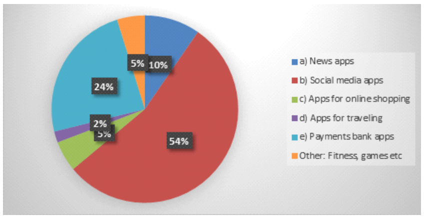
Advantages of using a smart phone	Number of responses
a) Connecting with family and friends	190
b) News and entertainment	167
c) Knowledge and learning	163
d) Online shopping	139
e) Online banking	141

(Source: Primary Data)

Different Types of Apps used by the respondnats:

54% respondants use social media apps on a regular basis followed by payment bank (24%) and news apps (10%). Other type of apps include apps for traveling, online shopping, games, fitness etc.

Chart 1 Showing different types of Apps used by the respondants



(Source: Primary Data)

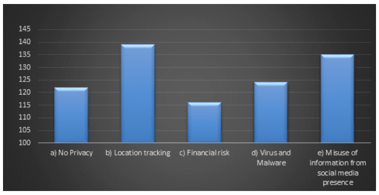
Analysis of Cyber Risk awareness of respondants:

- Whenever an app is downloaded, certain permissions are sought like access to location, camera, photos and so on. 43% of the respondnats said they read the full details, 23% said they don't read and 34% respondants responded maybe.
- 73% respondants said they are aware of the cyber security risk while downloading an app, where as 13% said they are not aware and 13% said maybe.

Analysis of cyber security risk factors:

When asked what kind of cyber risks respondants anticipate, respondants chose location tracking, misuse of information from social media platforms, virus and malware, no privacy and financial risk. (Note: Respondants were allowed to choose multiple options)

Chart 2 showing Cyber Secrity risks anticipated by the respondants



(Source: Primary data)

Analysis of Data on Aarogya Setu App:

- 69% of the respondants mentioned they have downloaded the app where as 31% said they have not downloaded the app. Reasons for not downloading app are no space in phone, cyber security risk, not much use and being on a national data base is riskier.
- Out of the respondnats who have downloaded the app, 53% mentioned they downloaded the app in the beginning itself where as 47% said they downloaded after it was made mandatory
- Out of the total respondants who downloaded the app, 63% upgraded the app after Bluetooth proximity feature was added, where as 37% did not upgrade the app.
- User status and self assessment is the most used feature in aarogya setu app (62%) followed by recent contact option (25%) and lastly to check covid updates (13%)
- 64% of the respondants feel Aarogya setu app serves the purpose of fighting against Covid and keeping safe where as 36% feel appl is of no use.

Analysis of relationship between Qualification and Cyber Security risk Awarness:

Hypothesis:

Null Hypothesis (H0): There exists a significant relationship between qualification of the respondants and app usage awareness components like cyber risk and app downloading mechansism etc.

Alternate Hypohtesis (H1): There is exists no significant relationship between qualification of the respondants and app usage awareness compnents like cyber risk, and app downloading mechansism etc.

1.Qualification * Are you aware of cyber security risk in downloading an app?

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.668[a]	4	.796
Likelihood Ratio	1.754	4	.781
Linear-by-Linear Association	.540	1	.462
N of Valid Cases	208		

2 cells (22.2%) have expected count less than 5. The minimum expected count is 1.75.

From the above table the sympotic significance of Chi Square independence test is found to be 0.796 which is greater than the required level of significance (0.05) Hence we are unable to reject null hypothesis which means that there exists a significant relationship between qualification and awareness about cyber risk factors while downloading an app.

2. Qualification * Whenever an app is downloaded, certain permissions are sought like access to location, camera, photos and so on. Do you read it in detail before installing an app?

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.878[a]	4	.928
Likelihood Ratio	.905	4	.924
Linear-by-Linear Association	.029	1	.864
N of Valid Cases	208		

a. 2 cells (22.2%) have expected count less than 5. The minimum expected count is 2.94.

From the above table the sympotic significance of Chi Square independence test is found to be 0.928 which is greater than the required level of significance (0.05). Hence we are unable to reject null hypothesis which means that there exists a significant relationship between qualification and understandig/comprehending the risks while installing an application.

Suggestions:

Cyber security risk is unavoidable when smart phone and multiple applications are being used. Using these applications makes various difficult tasks very easy, affordable and it saves time too. Going forward we can see more and more people using smart phones. At the same time it creates considerable amount of risks, especially if the users are not aware of such risks. The only way to be safe is to have a complete understanding of the various kinds of risks associated and also by learing to manage the same. The data collected and analysedshows that majority of the users are aware of such risks which is a good thing. To manage the same some important steps users can follow to are:

- Not downloading too many applications
- While downloading an app, reading and understanding carefully all the permissions sought
- Periodically evaluating all the apps and deleting apps which are not being used for a long time
- Taking precautions while doing financial transactions. For e.g. Protecting all payment gateway apps with 2 to 3 passwords, not linking the main bank account of the user with the payment gateways, changing the passwords regularly, using just one payment gateway app instead of havig multiple apps, not saving the passwords and so on
- Being cautious while sharing personal information/ photographs on social media
- Increasing awareness about cyber security risks by reading relevant blogs/materials or watching experts speak on the issue and by following govt. initiatives on user eduationand creating awareness programs
- Keeping the internet/data of the phone off when not in use.
- Learing and adopting technological innovations/new cyber security tools.

Conclusion:

Cyer security risk is going to be the biggest risks to all kinds of stakeholders in the society such as banks/financial institutions, government, individuals and so on. All users must contribute towards fighting this. The repucurssions of a cyber attack is very dangerous rnging from loss of business and finances, losing privacy, unlawful use of data etc. Product and service providers take adequate measures in putting proper systems in place to protect the users and government/ regulatory bodies will bring in adequate regulation to put things in place. Being individual users, it is everyone's responsibility to be safeby adopting safety measures and to follow the guidelines issued by the government and regulatory frameworks. Adopting new technological innovations too will help in understaning the risk perception in a better way.

REFERENCES :

1. https://www.similarweb.com/apps/top/google/store-rank/in/all/top-free/
2. Miller, C. (July–Aug. 2011). Mobile attacks and defense. IEEE Security and Privacy Magazine, 9(4), 68–70. doi:10.1109/MSP.2011.85, p.68.
3. Daojinghe, S. Andmohsenguizani. (February 2015), "Mobile Application Security: Malware Threats and Defenses" . IEEE wireless communications.
4. Adhikari, R., Richards, D., & Scott, K. (Dec 2014), security and privacy issues related to the use of mobile health apps. MHealth app privacy and security issues. 25th Australasian Conference on Information Systems.
5. Mylonas A., Kastania A., GritzalisD., (2013), "Delegate the smartphone user? Security awareness in smartphone platforms", Computers &Security(to appear).
6. Wright, J., Dawson, M. E., Jr., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smart phones. Cyber Security and Mobile Threats: the Need For. Antivirus Applications for SMART Phones, 5(14), 40–60.
7. Mosa, A. S. M., Yoo, I., & Sheets, L. (2012). A systematic review of healthcare Applications for smart phones. BMC Medical Informatics and Decision Making, 12, 67. doi:10.1186/1472-6947-12-67
8. Lai, Hsiangchu, Hsu, J. S.C., & Wu, M.-X. (2018). The Impacts of Requested Permission on Mobile App Adoption: The insights based on an experiment in Taiwan. Proceedings of the 51st Hawaii International Conference on System Sciences. ISBN: 978-0-9981331-1-9.
9. Peng, M., Zeng, Guanyin, Sun, Z., Huang, J., Wang, H., & Tian, G. (2018). 'Personalized app recommendation based on app permissions', Topical Collection: special Issue on Security and Privacy of IoT. World Wide Web, 21(1), 89–104. doi:10.1007/s11280-017-0456-y.
10. Jagwani, P., Kumar, R., & Sharma, G. (2015). Security issues in mobile apps. International Journal of Computer Science and Network, 4(3). ISSN (Online) : 2277-5420.
11. https://www.livemint.com/ai/artificial-intelligence/how-aarogya-setu-app-works-and-how-it-helps-fight-covid-11594512597402.html.
12. https://github.com/nic-delhi/AarogyaSetu_Android.
13. https://www.livemint.com/ai/artificial-intelligence/how-aarogya-setu-app-works-and-how-it-helps-fight-covid-11594512597402.html
14. https://www.financialexpress.com/industry/technology/govt-discontinues-corona-kavach-aarogya-setu-is-now-indias-go-to-covid-19-tracking-app/1919378/
15. https://news.jagatgururampalji.org/download-aarogya-setu-app/
16. https://www.indiatoday.in/india/story/aarogya-setu-not-mandatory-govt-softens-stance-in-lockdown-4-0-guidelines-1679029-2020-05-17
17. https://www.bbc.com/news/world-asia-india-52659520
18. https://economictimes.indiatimes.com/tech/software/legal-experts-point-out-liability-concerns-with-the-aarogya-setu-app/articleshow/75561944.cms
19. https://www.hindustantimes.com/india-news/aarogya-setu-protection-or-threat/story-QmpSP3H60ohkLV3l5ywhBI.html
20. https://www.huffingtonpost.in/entry/aarogya-setu-app-privacy-issues_in_5eb26c9fc5b66d3bfcddd82f