The Study of Security and Privacy Related Concerns Associated with Smartphones

Sumeet Gupta , Prof. Shravani Pawar

Master of Computer Applications

Bharati Vidyapeeth's Institute of Management&
Information Technology

Sector 8, C.B.D.Belapur,

Navi Mumbai. 400614.

Abstract

Smartphones are nowadays part in our day- to-day life. Smartphones are something which are an essence to store our personal and professional information.as it holds sucha lot of value and importance in our life, it is necessary to make sure both privacy and security of smartphones. Although, the addition of latest features makes smartphones smarter, on the opposite hand security and privacy related threats also increases relatively. Our research is to gaugethe notice of Smartphone users areconscious of security and privacy. Our study deals with a survey of Smartphone users to assess their level of awareness about security. From survey we conclude that the majority users are conscious of their smartphone security and privacy but on the opposite hand they are unaware the way to ensure for an equivalent. secondly, we have described certain smartphone problems and their impact, respectively. Also, we have suggested certain common measures to reinforce and make sure the privacy andsecurity in smartphones.

Keywords: ***awareness, privacy, security, smartphones, survey.***

1. Introduction

The use of smartphones has increased immensely over the earlier couple. We humans tend to heavily depend on it as we store all the personal as well as professional information in it. And henceforth, privacy and security tend to major factors as well as challenges. With increase in use of smartphones, security and privacy related threats have also increased. So, it is important to be aware of security and privacy and in turn ensure in it our smartphones. When it comes to smartphones privacy, the basic security measures we use is encrypting our phones with patterns, fingerprint lock, face lock, pin etc. Users also protect their phones using antivirus and other measures. But still, there are attacks which are inevitable.

According to global smartphone penetration data, there are now over 9.42 billion mobile connections worldwide, which surpasses the current world population of 7.75 billion implied by UN digital analyst estimates. Hackers attack every 39 seconds, on the average 2,244 times each day. Over the past five years, security breaches have increased by 67%, according to Accenture’s global survey. Symantec’s internet security threat report 2019 states that number of attacks using destructive malware have increased 25% in the last few months.

Our paper is organised as follows: In the upcoming section we have described various smartphone problems and their impact on smartphones. In third section, we have put forward literature review, the next section goes ahead with methodology and survey result And we wind up our research with conclusion and references.

2. Smartphone problems

2.1. Access permissions

When you install any applications like Instagram, WhatsApp etc., there are certain access permissions, that should be agreed. Also, there may be certain policies or regulations which should also be agreed.by doing, so we are giving the applications full access permissions to our privacy factors. For example, after installing Instagram, there are access permissions to locations, gallery etc.by agreeing them we are giving them full access to photos and locations.

2.2. Installing Third party applications

It is not safe to put in third party apps. So many hackers or companies use these third-party apps to fetch your personal information. There are some google policies issues in these apps, which is why these apps aren't available live Store.

For e.g., google play store ban 13 apps from play stores as they were malicious.

2.3. Spyware

Whether your employees have an iOS or Android device, their devices are targets for threats focused on mining user data and your private corporate data. **For example,** Apple realized it had three zero-day vulnerabilities that left its devices open for spyware attacks. Pegasus spyware was discovered back in August 2016 and was used to hack into Apple devices and survey users. Apple had to release a patch with updates that might protect users against the Trident iOS vulnerabilities.

2.4. No password protection

With all the ways to secure mobile devices, it would be shocking to understand that 34% of individuals do not use a password to lock their phones. If these devices are lost or stolen, it gives thieves quick access to all or any the knowledge stored within the phone. For people that do undergo the trouble of making a password or PIN, they typically default to codes that are easy to crack. Like 0000, 1234 or birthday month and day.

2.5. Botnets

Depending on the site's employees visit on their mobile devices, malware can be downloaded onto mobile devices that are not protected by antivirus software or a mobile security app. This gives hackers full access to the device in order that they will control affected devices remotely. All devices with the malware on them are added to a network of other affected devices — called a botnet — that allow hackers to send spammy emails and other click fraud campaigns that spread the malware to even more devices.

2.6. Lost or stolen device

Not all attacks happen in the digital world. Losing a phone or tablet is one among the toughest threats to fight against since it gives hackers direct access to the info, they are after.

Hackers can see what sites your employees visit on their devices and which apps are linked to your corporate data and personal communication. Most times users are logged onto the apps on their devices so hackers will not need to find out passwords to unlock the info.

Impact of these attacks on smartphones

Attack name	Threat to smartphones
Access Permissions	1) Interference in smartphone operations 2) Confidential information can be leaked.
Installing Third Party Applications	Personal information can be hacked
Spyware	1) Makes security of smartphone weak 2) Data may be hacked
No Password Protection	1) Sensitive information can be accessed. 2) Biggest threat to privacy.
Botnets	1) Spams can be added via emails. 2) Decrease smartphone internet speed 3) Mail can be hacked.
Lost or Stolen Device	1) Physical access to data 2) Leakage of information

3. Literature review

3.1. Lock Screen

A new phone will become a treasure trove of personal data very quickly, so you ought to take a couple of basic steps to form sure it keeps your data secure. Always confirm you configure a secure lock screen, ideally with a robust password. Android phones with fingerprint sensors will not force you to type that in whenever, but it ensures nobody are going to be ready to brute force your phone. you will also close lock screen notification snippets to form sure your messages aren't revealed. Likewise, confirm Smart Lock (automatic phone unlocking supported connected devices, locations, then on) is disabled unless you are extremely confident in your other security practices.**Steps:** Go to Settings ◊ Security, and attend ScreenLock. then you will set either pin lock, password, or fingerprint sensor.

3.2 Prevent unauthorized applicationsfrom installing.

Unlike iPhones, android devices can run third-party content outside of the Google Play app store. this will open a tool to malware attacks. the simplest thanks to make sure that only verified and malware- checked apps are often installed on your phone or tablet is by getting to Settings then Security and ensuring that the Unknown sources option is turned off.

3.3 App Permissions

Introduced several years ago, Android's app permission model allows you to block apps from accessing certain system features. When apps open for the primary time, many of them will invite permissions (storage, camera, microphone, location, then on). you will deny them at that point, but some apps might refuse to start out if you deny necessary permissions.

Android also makes permissions accessible within the app settings (under the most system settings). Each app info page includes toggles for all its permissions. So, you will close Facebook's location tracking albeit you mistakenly allowed it within the past. There also are apps like Bouncer that clear permissions after each app use.

3.4. Install a Security App

You would not let your computer run without antivirus, so why leave your phone unprotected? It does not matter what OS your mobile device runs or how secure its manufacturer says it is: Â if you access the web with it, your phone is susceptible to attack.

There are many anti-virus and anti-malware apps available for each sort of device. Firewall apps also are handy to form sure no apps are sending or receiving information you are not conscious of.

4. Methodology

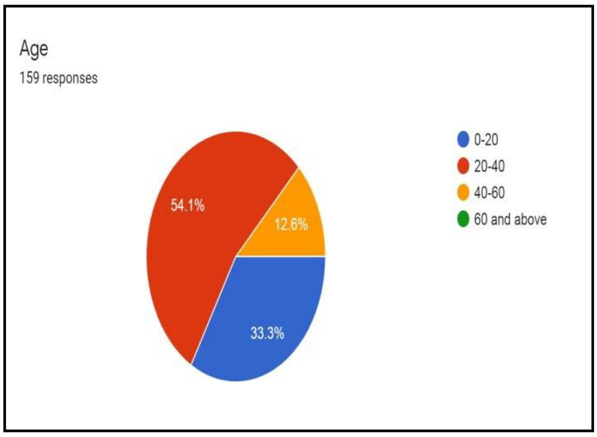
The aim of this research paper is evaluating what proportion the smartphone users are aware of security and privacy related functions in their phones. In our study we have used Questionnaire methodology to seek out the conclusion for our research. Atfirst, we created google form during which we set the questionnaires associated with security and privacy related issues in smartphones to seek out what proportion users are conscious of these functionalities. By using google forms, we have taken the survey of smartphone users of our society and that we have stored the end in spreadsheet. The target population of this study was smartphone users, especially youngsters and teenagers of our society. The responses we got from smartphone users helped use for evaluating the notice of security and privacy among them and for better research. consistent with the number of responses, we have made the graphs to present our survey result for better understanding of our research.

Survey Result

We have taken the survey of 159 respondents through a google form. The aim of this survey is to check how smartphone users are aware about security and privacy in their phones.

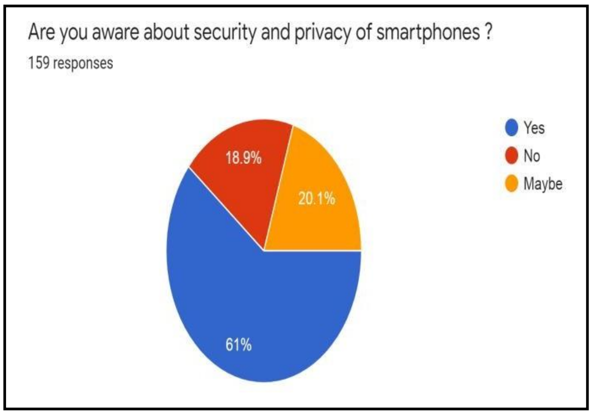
Evaluation of Research Questions

Fig.1: From the above figure there are 54.1% respondents are between ages 20-40,



33.3% between 0-20,12.6% between 4-60.

Fig.2: From the above figure there are 61% respondents said that they are aware about it, 18.9% are unaware about it and 20.1 % are aware about it.



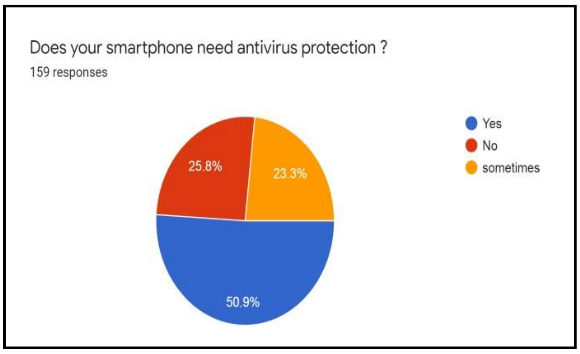


Fig.3: From the above figure 50.9 % respondents said Yes ,25.8 % said No, and 23.3 % said Sometimes.

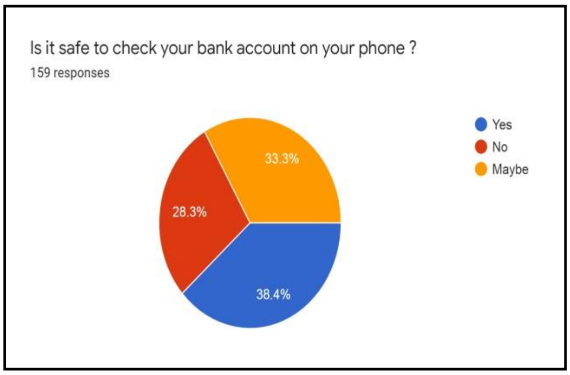


Fig.4: From the above figure 38.4 % respondents said that it is safe ,28.3% said that it is unsafe, and 33.3 % said that it is safe.

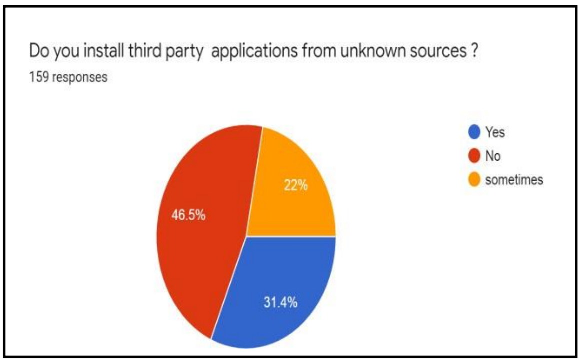


Fig.5: From the above figure, 31.4 % respondents said Yes, 46.5 % said No, and 22 % said Sometimes.

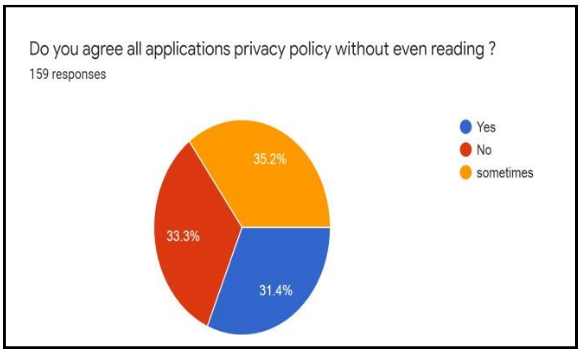


Fig.6: From the above Figure, 31.4 % respondents said Yes, 33.3 % said No, and 35.2 % said Sometimes.

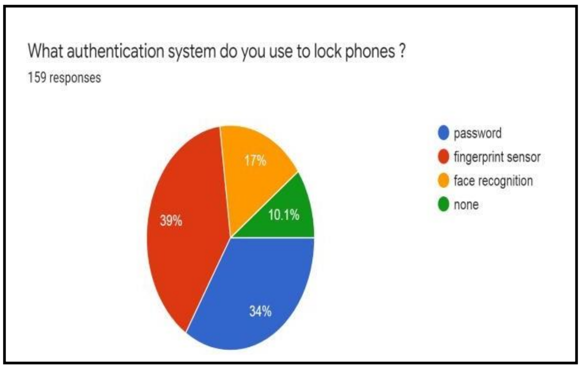


Fig.7: From the above figure 39 % respondents uses fingerprint sensor, 34 % uses password, 17 % uses face recognition, and 10.1 % are not using any system

Considered options for questions

Question	Safe option	Unsafe option
Do your smartphone needs antivirus protection?	Yes	No Sometimes
Is it safe to check your bank account on phone?	No	Yes Maybe

Do you install third party applications from unknown sources?	No	Yes Sometimes
Do you agree with all applications privacy policy even without reading?	No	Yes Sometimes
What authentication system do you use to lock phones	Password Fingerprint sensor Face recognition	None

Solution

The word smartphone itself suggest that the phone is now smarter. The free apps are the major contributor in this type of manipulation. When you have given access to your privacy to any app. If you are not using it or you just uninstall it without dropping the account. Then also your account is using and collect the data that has been saved in your phone. When we are surfing the web, we are catching viruses for our phone. When we put any information on web it gives chunks to the hackers to go for it. I have been through such fraud with my friend. It not only hacks the phone. The phone data is the by-product of your personality. So, it indirectly hacking your personality. People are learning hacking courses. Because they think hacking is the future. Companies hire people with hacking knowledge to get access to the data available on the web and use it for their purpose. They hire people too for their information safety. They need hackers to save from hacking. Like iron cuts iron. Less awareness about security. People are not aware about thetrouble they are ignoring and thinking we donot have anything to hide from family. But you are giving all your information to the scammer to defraud you. Apps are using diverse ways to confirm that the device is supported by a user. The had started a new way for confirmation. Instead of sendingOTP they by default using your phone SMS to send the confirmation message to the app. You are getting phones at cheaper prices because the companies are linked with each other. They are hungry for your information. Data can be manipulative because we are taking views of the people present in your community. Those are just an inappropriate data. The people in villages are unawareabout security and they are ignorant about the effect that technology made in their life. This advertisement companies are a stepahead in all terms of threat. They are readingpeople's mind. Phone have become smarter.They know about you more than any of your family members does. The data we are taking as an average. We should have at least 1% of the population in the survey. From diverse backgrounds to get the genuine results. Now a days phones are University, bank, electricity connection gas connection. Groceries, basic needs, food, everything is available online. They help people to scammer to make a blueprint of you. When we are using our password in any app Google ask us can we save your password. This shows that what technologymade human. In 21st century. Trust is the thing that people got deceived for. They are trusting the app with bigger name without any inspection that any app can be a means for the manipulation of your data. There are tons of craps are available on the web. They have sold their morality for money. They gave permission without inspection that they are showing add of the genuine advertiser or they are just playing with innocent people's trust. We cannot trust privacy policy too. Because a sentence you are learning can have different meaning. So, assume every scenario of that permission and they take the decision. Not every phone has the hard level security. Most phone do not have fingerprint or face lock.

They must use the password or the pin or pattern. But according to a survey most people cannot afford a phone of a higher price range. They usually afford phones from 7000 to 10000. Those phones cannot have that level of security. So, it is important to make people aware about the security and the apps which are useful, and which are harmful. Out of smartphones, only 10% phones have face lock or fingerprint lock. Smartphone are getting smarter, and people are getting dumb. This is becoming reality. We are moving in an era in which people will only think what smartphones allow them to think.

There are some ways to spread awareness.

- At the time of buying a phone. The seller should give 30 min representation. About security to everyone.

- Everyone should follow at least one technology related YouTube channel and be updated to the changes that take place day by day. This helps them to find genuine apps which help them to save their phones from getting hacked.

- We should do awareness programs in school and college so that the children themselves will be aware and will also teach the elders of their house the proper use of smartphones.

- We can also use social media for awareness program. We can create a WhatsApp link or group through which we can make people aware.

- Nowadays short videos apps are showing rapid growth. Even in villages people are crazy for watching short videos. We can use that 30 sec video for the purpose of their betterment. It will be easy for them to grasp the knowledge about security in chunks.

Conclusion

The research aims at evaluating the extent of awareness of smartphone users in terms of privacy and security. during this study we have taken survey of users and that we have found that on a mean most of the users are conscious of their smartphone security and privacy, but they are unaware of the way to make sure that level of security and privacy. therefore, we have also suggested measures in literature review to make sure the privacy and security in smartphones. Smartphones are something which are part for our living, our dependency thereon increases the danger of privacy and security. therefore, small steps like encrypting phones with password, locks, securing with antivirus enhance the safety of smartphone and protects it from unauthorised access and other things. Following certain measures to make sure security would always be beneficial as prevention is best than cure.

References

- https://thesai.org/Downloads/Volume10No9/Paper_64-Security_and_Privacy_Awareness.pdf
- https://www.appknox.com/blog/the-hidden-dangers-of-using-a-third-party-mobile-app
- https://us.norton.com/internetsecurity-mobile-the-risks-of-third-party-app-stores.html
- https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/
- https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf
- https://www.ijrte.org/wp-content/uploads/papers/v7i4s/E2001017519.pdf
- https://www.csoonline.com/article/3241727/7-mobile-security-threats-you-should-take-seriously-in-2019.html
- https://www.123helpme.com/cell-phone-privacy-preview.asp?id=285551
- https://gradesfixer.com/free-essay-examples/mobile-security/
- https://www.sciencedirect.com/science/article/pii/S1877050915017044
- https://www.privacypolicies.com/blog/protect-mobile-privacy/
- https://www.sciencedirect.com/book/9780128046296/mobile-security-and-privacy#book-description
- https://www.internetsociety.org/resources/ota/2017/mobile-app-privacy-security/
- https://www.kaspersky.co.in/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
- https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/
- https://us.norton.com/internetsecurity-mobile-types-of-common-mobile-threats-and-what-they-can-do-to-your-phone.html
- https://www.esecurityplanet.com/mobile-security/10-trickiest-mobile-security-threats.html
- https://searchsecurity.techtarget.com/definition/botnet
- https://www.researchgate.net/publication/309675787_Research_Paper_for_Mobile_Devices_Security
- https://thesai.org/Downloads/Volume7No4/Paper_26-A_Survey_on_Security_for_Smartphone_Device.pdf