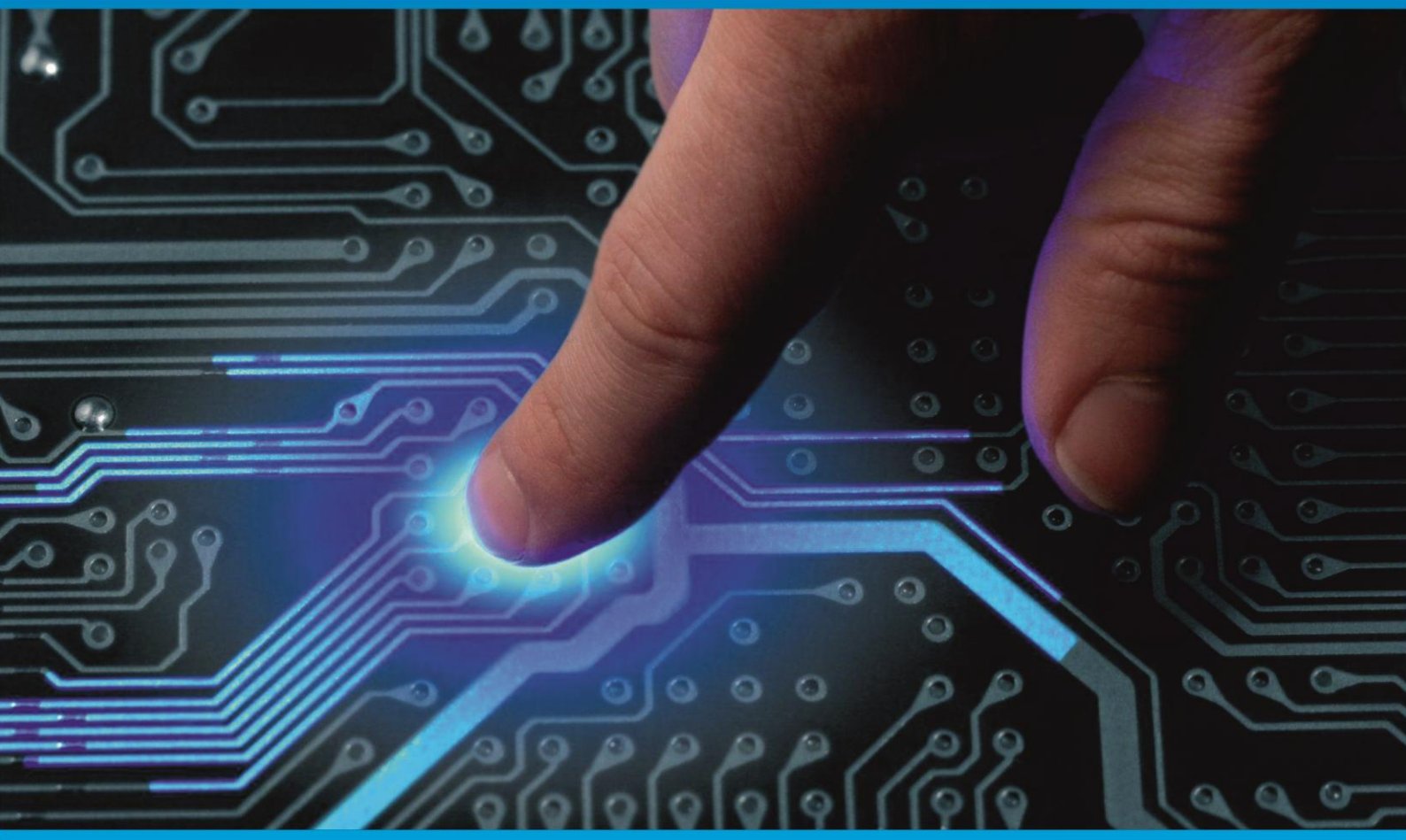
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905040 |

Review of Anti Malware in Smartphones

Atharv Gaikwad [1], Tulsi Naidu[2], Prof. Rajeshwari Gundla[3]

U.G Student, School of Engineering, Ajeenkya D.Y Patil University, Pune, Maharashtra, India [1,2]

Assistant Professor, School of Engineering, Ajeenkya D.Y Patil University, Pune, Maharashtra, India[3]

ABSTRACT: Now a Day's popularity and growth of Android or mobile device is increase. with them the risk and challenges are also increased. There are a lot of apps are there on internet or on google for entertainment, banking, shopping etcSome of those are used to spread viruses in android devices. To protect from such apps and threads challenges in antimalware software are also increased. In this paper, we evaluate types of threats, the anti malware or antivirus software in the market and what we can do to fight back. such an evaluation is including Application-based threads, malicious apps, spyware, phishing attackers etc.

KEYWORDS: Mobile, Android Device, Viruses, Antimalware, Antivirus, Application-based Threats, Spyware, Malicious Apps, Attackers.

I. INTRODUCTION

Mobile computing devices such as smartphones and tablets are becoming increasingly popular. Unfortunately, this popularity attracts malware authors too. In reality, mobile malware has already become a serious concern. It has been reported that on Android, one of the most popular smartphone platforms [1], malware has constantly been on the rise and the platform is seen as "clearly today's target" [2], [3]. With the growth of malware, the platform of antimalware software with the range of fees are also available in app market, Google play.
In this paper, we evaluate types of malwares and some antimalware platforms and what can we do for mobile security, example Bitdefender Mobile Security offers excellent protection for your Android device, with a raft of features including anti-theft, and top-notch antivirus capabilities[11].

II. LITERATURE SURVEY

ANDROID ANTIMALWARE
Android Antimalware nowadays is a very important thing to protect your device, drives and bank info. Lot of malware sides and applications are used to damage your devise performance, to steal your data and information. To protect from such malwares and malicious apps there are a lot of antimalware available in the app market.
There are some threads that can harm your device 4 of them are:

1. Application Based Threats
2. Web-Based threats
3. Network-based threats
4. Physical threats.

Let's have a quick idea of them:

I. **Application Based Threat** happens when people download apps that look legit but actually skim data from their device. Examples are spyware and malware that steal personal and business information without people realizing what's going on [11].

II. **Web-based threats** are subtle and tend to go unnoticed. They happen when people visit affected sites that seem fine on the front-end but in reality, automatically download malicious content onto devices [11].

III. **Network-based threats** are especially bad because cybercriminals can steal unencrypted data while people use public Wi-Fi networks [11].

IV. **Physical threats happen** when someone loses their mobile device or has it stolen. Because hackers have direct access to the hardware where private data is stored or where they have access to data, this threat is especially dangerous to enterprises [11].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905040 |

Below mentioned are the other apps and combinations of these types of threats.

1. **Malicious Apps**
   - It's important to know all the choices and specs of the code you put in on a laptop or mobile device before it gets put in [12].
   - The long list of checkbox choices, which frequently get unnoticed, ought to be scrutinized. Checking a box might approve doubtless malicious applications to be downloaded [12].
   - Not technically malware, these applications will represent direct access for a cybercriminal and send browsers to malicious sites or unwanted web content [12].
   - This type of browser hijacking or hacking will modification home page settings and add toolbars that are troublesome to get rid of. they'll conjointly serve scareware to the system and install unwanted computer cleaners and performance optimizers [12].
   - The potentially malicious application might take over a digital camera, as an example, and deliver malware bots providing remote access to a cybercriminal wanting personal money info and personal information. If you see read associate unknown app on your laptop or mobile device, delete it [12].

   - 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 [11].
   - 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 would protect users against the Trident iOS vulnerabilities [11].

2. **Public WIFI**
   - As more companies offer remote work options, access to unsecured WiFi is becoming more widely available in public places. Be it coffee shops, co-working spaces or the library, public Wi-Fi is convenient, but the downside is that the devices your employees use are vulnerable to attacks sent through these networks [13].
   - Instead of connecting directly to a network, people are tricked into accessing a network that looks authentic but is actually controlled by a hacker. Figure 1 below explains the following:

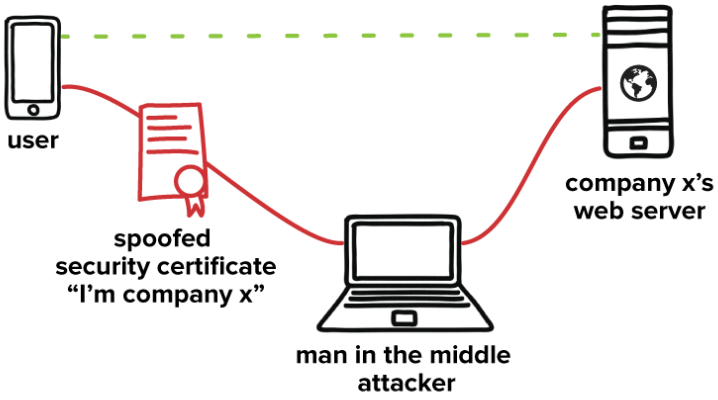


Fig.1 Network controlled by hacker Inactive apps

   - Google and Apple remove apps from their stores on a regular basis, but the thing is, they don't offer much explanation about why. We can assume, though, that these occasional purges have something to do with security threats and privacy breaches [11].
   - In Google's case, they found apps that forced users to click on ads by making it hard to use the app otherwise. When a user clicks on the ad, it runs in the background without the user knowing while the ad accumulates automated clicks to generate income for the app developer [11].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905040 |

3. Botnets

- Depending on the site's employees visit on their mobile devices, malware can be downloaded onto mobile devices that aren't protected by antivirus software or a mobile security app. This gives hackers full access to the device so that they can control affected devices remotely [13].
- 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 [13].

4. IoT mobile security threats

Mobile devices are branching out from cell phones and tablets to include wearable tech, like smart watches or devices in the office, like video conferencing tools. Basically, anything that's used to improve workplace efficiency, productivity and service quality has a product for that purpose [12].

5. Lack of end-to-end encryption

A recent study found that only 5.5% of mobile app development budgets go towards security. This is shocking considering the amount of information uploaded to apps. Depending on the platform's employees use to access corporate data on their phones, a lack of mobile app security doesn't bode well for you [12].

For example, a lot of communication happens electronically. You send, share and receive countless amounts of data every day, so leaving that unencrypted leaves the door open for anyone to look at what's being said or done in your company [12].

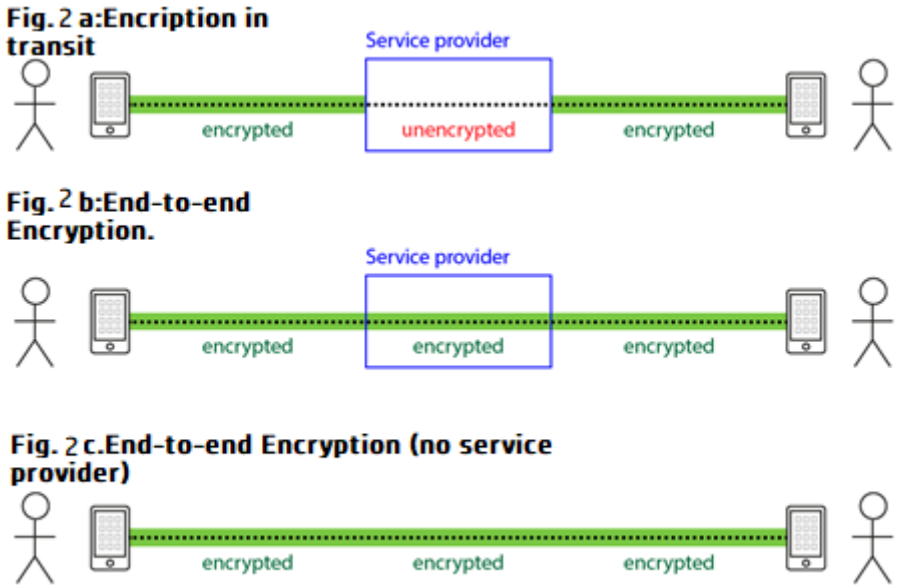


Fig.2 Encryption in transit

6. Phishing attacks.

This happens all too often in enterprises where hackers send what look like legit emails or SMS to get employees to hand over private information [13].

Following are some Anti Malware software and apps are present in app market.

1. Bitdefender Mobile Security

- Bitdefender Mobile Security offers excellent protection for your Android device, with a raft of features including anti-theft, and top-notch antivirus capabilities. In fact, this android antivirus mobile app got full marks in the latest AV-Test roundup, and AV-Comparatives (the other major independent antivirus test lab) observed a protection rate of 99.9%. That's impressive indeed.
- Mobile Security gives you real-time protection for Google's Chrome browser, and an autopilot feature that claims to be capable of making intelligent recommendations for security actions depending on your system and typical usage pattern [8].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905040 |

- There's also a nifty privacy advisor tool that adds a layer of security to your smartwatch via its Wear On technology, which alerts you if you accidentally leave your phone behind - clever stuff [8].
- Another interesting extra is a bundled VPN, although don't get too excited. The provided version is restricted to extremely light use at just 200MB daily, but still, that could be useful in a pinch.
- As mentioned, there are anti-theft capabilities here, and Bitdefender Mobile Security allows you to remotely locate and lock your device, or send a message to the phone or tablet (which could be very useful if you've lost it). It's also possible to completely wipe the device remotely if you so choose [8].
- There are a lot of features on offer here, then, and the asking price is more than reasonable to cover a single Android device for a year (plus if you want to give the app a spin before you buy, there's a 14-day free trial available) [8].

2. Norton Mobile Security

- Norton Mobile Security for Android offers a wealth of features, including an App Advisor which is powered by Norton Mobile Insight, and vets' apps for any possible privacy risks, or other unwanted behavior like being overly taxing on your battery (you can even get these evaluations before you install an application, which is very handy) [10].
- This mobile security suite also gets top marks for the protection its antivirus engine delivers going by AV-Test's findings (the other main test lab didn't evaluate Norton recently) [10].
- Other features include call blocking to protect against spam phone calls, Wi-Fi security that alerts you when you connect to an insecure wireless network, plus anti-theft features that allow you to remotely lock a stolen (or lost) device, or wipe all your data [10].
- All this adds up to an impressive level of protection for your Android device – but are there any downsides here? Well, the app is pricey, or at least the recommended asking price is, but given the discount on offer at the time of writing, it's actually the same price as Bitdefender above (making it an excellent buy currently, given that you get coverage for three Android devices, not just one) [10].
-

3. Avast Mobile Security

- Antivirus giant Avast has produced another quality app which goes above and beyond being a mundane scanner, although that said, it does virus scanning very well, and is highly rated by the independent test labs [7].
- Avast Mobile Security's nifty features include an anti-theft system allowing you to track and remotely lock (or wipe) your Android device if it's stolen, or if you lose it. There are also some interesting performances enhancing features including a junk cleaner to free up storage space, and a 'RAM boost' which aims to speed up your device [7].
- The app used to be paid but is now free, albeit supported by ads. You can pay a small monthly or yearly premium to remove the adverts if they annoy you, though. Another very useful premium feature is 'in-app locking' whereby your device will ask for a PIN before opening certain apps. This prevents malware from launching apps such as internet banking automatically [7].

4. AVG Antivirus Free

- AVG Antivirus Free is another high-quality app for securing your Android device, and it delivers an impressive level of protection at no cost whatsoever. In fact, it uses the same well-liked antivirus engine as Avast above (remember that Avast bought up AVG back in 2016) [6].
- This isn't the same product, though, and it doesn't have some of the features you'll find in Avast's freebie offering. It is, however, still built around very robust core antivirus protection, plus anti-theft features which allow you to locate, lock or wipe a stolen (or lost) phone. Also like Avast, this app is ad-supported, but by upgrading to the premium version you can get rid of those adverts [6].
- The paid Pro version of AVG comes with a whole load of extra features, including extended anti-theft capabilities (such as the device locking itself if the SIM card is replaced, and sounding an alarm), a Photo Vault to secure your photos, an app lock, Wi-Fi security scanner, and additional privacy settings, such as for blocking callers [6].
- There are also a host of other features such as performance enhancement measures, which aim to kill unnecessary processes, turn off battery-draining settings, as well as deleting junk files such as those commonly found in temp and cache folders [6].
- Note that you can try out all these Pro features for free, at least for the first two weeks when using AVG Antivirus Free; but after that, you have to pay [6].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905040 |

- With so many features bundled in the Pro version, it's no wonder this app is the most popular antivirus when you search for one in the Google Play store, with more than 100 million downloads, over 6.5 million reviews and an average score of over 4.5 [6].

5. Kaspersky Internet Security

- Kaspersky has a reputation up there with the big players like Bitdefender, so perhaps unsurprisingly the free version of its security app has some smart features, including top-notch malware detection (going by the ratings from independent test labs) [6].
- Not only do you benefit from Kaspersky Internet Security, but there are also some heavyweight anti-theft capabilities, allowing you to find the location of your Android device if it has been lost or stolen. You can also remotely lock the phone, or wipe the data on it, or even snap a photo of the person currently using the device (which could be really useful if they're a thief). An alarm can be remotely set off, too (that might be handy if you've lost the phone) [6].
- Another impressive feature is support for Android Wear which simplifies security management, plus this app is free, as we already mentioned, which is always a major boon. There is a paid version, mind, and some important features are reserved for this [6].
- If you fork out for Kaspersky Internet Security for Android (Premium) you also get automatic antivirus scans (as opposed to having to start them manually), as well as anti-phishing protection to keep you safer online, and a few extra benefits. Still, the freebie version gives you good malware defenses for the princely sum of nothing at all! [6]

6. Trend Micro Mobile Security

- The Trend Micro Mobile Security app not only scans new apps for malware before they are downloaded and installed, it prevents newly installed apps from accessing other applications, which can be useful for device admins and parents [5].
- There's also a built-in privacy scanner for Facebook which warns you if your profile settings are displaying sensitive personal information. Indeed, there are a huge number of features here, which include web protection, anti-theft, a Wi-Fi checker for making sure any wireless networks you connect to are safe, plus system tuning utilities, a full suite of parental controls, and Pay Guard ensures that any online banking or shopping transactions are fully secure [5].
- Furthermore, both independent testing labs rated Trend Micro Mobile Security as protecting against 100% of threats, making it top of the tree in this respect at the time of writing [5].
- There's a lot to like here, then, but the downside is that the asking price is rather steep compared to many of the alternatives on this page. That said, you're getting a lot for your money, and there's a free version of the app which allows you to have the full run of all [5].

III. FUTURE SCOPE AND DISCUSSION

In the future maybe a lot of people start using Android anti malware to protect their devices. Maybe companies will preinstall antimalware to users in order to secure their device and to maintain performance. In future maybe it will become more necessary to have android antimalware in your device.

IV. CONCLUSION

Mobile devices face a lot of threats but there's a lot you can do to protect yourself, your data and your employees. Follow these guidelines and you'll be well on your way to protecting yourself through your mobile security journey.
The key is to educate employees and give them the tools and information they need to make the right choices. The more they understand what's at risk, the safer yours and their data will be.
Talk about mobile security regularly so that it becomes standard practice and so that you can feel confident that your corporate data is safe and secure.
As we move further into the digital age, it's important that we do as much as possible to protect devices and the information they give us access to.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905040 |

REFERENCES

[1] Rastogi, Vaibhav, Yan Chen, and Xuxian Jiang. "Catch me if you can: Evaluating android anti-malware against transformation attacks." *IEEE Transactions on Information Forensics and Security* 9, no. 1 (2013): 99-108.
[2] McAfee, "MacAfee threats report: Third quarter 2011," http://www. mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf.
[3] F-Secure, "Mobile threat report Q3 2012," http://www.fsecure.com/static/doc/labs global/Research/Mobile%20Threat% 20Report%20Q3%202012.pdf.
[4] Sen, Sevil, Emre Aydogan, and Ahmet I. Aysan. "Coevolution of mobile malware and anti-malware." *IEEE Transactions on Information Forensics and Security* 13, no. 10 (2018): 2563-2574.
[5] Jarabek, Chris, David Barrera, and John Aycock. "Thinav: Truly lightweight mobile cloud-based anti-malware." In *Proceedings of the 28th Annual Computer Security Applications Conference*, pp. 209-218. 2012.
[6] Jang, Jae-wook, Jaesung Yun, Jiyoung Woo, and Huy Kang Kim. "Andro-profiler: anti-malware system based on behavior profiling of mobile malware." In *Proceedings of the 23rd International Conference on World Wide Web*, pp. 737-738. 2014.
[7] Walls, Jason, and Kim-Kwang Raymond Choo. "A review of free cloud-based anti-malware apps for android." In *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 1053-1058. IEEE, 2015.
[8] Distefano, Alessandro, Antonio Grillo, Alessandro Lentini, and Giuseppe F. Italiano. "SecureMyDroid: enforcing security in the mobile devices lifecycle." In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, pp. 1-4. 2010.
[9] Li, Qing, and Greg Clark. "Mobile security: a look ahead." *IEEE Security & Privacy* 11, no. 1 (2013): 78-81.
[10] Faruki, Parvez, Ammar Bharmal, Vijay Laxmi, Manoj Singh Gaur, Mauro Conti, and Muttukrishnan Rajarajan. "Evaluation of android anti-malware techniques against dalvik bytecode obfuscation." In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 414-421. IEEE, 2014.
[11] https://www.techradar.com/in/best/best-android-antivirus-app accessed on 28 Feb 2021
[12] https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/ Accessed on 28 Feb 2021
[13] https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/ Accessed on 28 Feb 2021

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details