Journal of Multidisciplinary Engineering Science Studies (JMESS)
ISSN: 2458-925X
Vol. 8 Issue 7, July - 2022

Smart Phone Security Threats And Risk Mitigation Strategies

Ozuomba Simeon[1]
Department of Electrical/Electronic and Computer Engineering, University of Uyo, Akwa Ibom, Nigeria
simeonoz@yahoomail.com
simeonozuomba@uniuyo.edu.ng

Akpasam Joseph Ekanem[2]
Department of Electrical and Electronic Engineering, Akwa Ibom State University Mkpat Enin, Akwa Ibom State

Gloria Ngozi Ezeh[3]
Information Technology Department, School of Information and Communication Technology, Federal University of Technology Owerri.
gloriaezeh2014@yahoo.com

***Abstract*—In this paper, smart phone security threats and risk mitigation strategies are presented. Brief overview of some selected cybersecurity threats applicable to smart phones are presented. The cybersecurity threats discussed include spyware attack, direct cyber-attack, drive-by download, exploit, keylogging, Malvertising, malware, phishing, ransomware, social engineering, spam, Trojan, virus (computer virus), and zero-day virus. Specifically, each of the smartphone cybersecurity threat category is described briefly along with description of how smartphone users' activities can make them vulnerable to such threat. In addition, smartphone cybersecurity risk mitigation strategies are presented. The cybersecurity risk mitigation strategies presented is twelve layers of protection approach which is based on recently developed cyber security best practices for mobile devices and applications. The detailed sequence of instructions for implementing some of the security mitigation strategies are also presented. The essence of this paper is to intimate the smartphone users with contemporary smartphone security threats and the best practice strategies for mitigating smartphone security risk.**

***Keywords*— Security Threats, Smart Phone, Security Risk, Malware, Risk Mitigation Strategies, Cybersecurity**

1. Introduction

As smart phones and their application market is growing, there is a serious battle between cyber-attackers and defenders. Furthermore, with the advent of the emerging technology of 5G networks and its infrastructure, cybercrime will be on the increase [81]. Presently, smart phone users are always subjected to diverse malicious activities. However, many users of smart phones are not really aware of the numerous security threats and the implications of so certain actions they perform with their smart phones. Also, many of the users do not know that that smart phones can also be hacked. As such, often times, smart phones contains even more important information than the personal computers; such information includes, phone numbers, photos, location data and history and stored credit card information. Notably, according to [30], a greater percentage of organizations had a data breach as a result of employees using their mobile phones to access the company's data.

Malware is any software used by cyber criminals to disrupt computer operations, gather sensitive information and/or unlawfully gain access to private information in computer systems without the knowledge of the system user [35, 39, 40]. Computer viruses, worms, rogue security software, Trojan horses, ransomware, spyware, adware, scareware are different forms of malware which is a common name used to for all malicious software. Executable codes and active contents, as well as executable scripts and other software are the various means of spreading malware. Nowadays, with the rapid adoption of mobile devices like smart phones, the rise of malware targeted at smart phone users has also increased. Malware software are often disguised or embedded in non-malicious files, such as .jpeg, .exe, .mp3, .gif, .mpeg and so on[74]. According to the statistics of mobile ad fraud and malware report for 2021[82], about 21% of the most malicious apps were in the games category, 17% were in entertainment and lifestyle category while 20% were in tools and personalization category .

Although smart phone app giants like Google and Apple scan the applications in their app stores for malware, but users are still exposed to different kinds of attacks because of their online activities. According to [34], information security market is expected to reach $170.4 billion in 2022 and most threats according to [30, 35-38] includes data leakage, malware, direct hackers attack, phishing and social engineering attacks, as well as, communication interception and spoofing attacks, stolen and lost of phones [41,42]. According to the research conducted by Kaspersky [83], the report on the categories of mobile malware detected in 2021, shows that adware which is a form of spyware attack represent 42% of all detected mobile malware in 2021. Accordingly, in this paper, several categories of smart phone security threats and risk mitigation strategies are presented. The essence of the paper is to intimate the smartphone users with contemporary smartphone security threats and the best practice strategies for mitigating smartphone security risk.

2 Overview of selected cybersecurity threats

Today, numerous cybersecurity threats are already in existence, new threat categories are also being created while the existing threats categories are also evolving and giving rise to different versions or variants of each given threat category. In this section a brief overview of some selected cybersecurity threats applicable to smart phones are presented. The cybersecurity threats discussed include

spyware attack, direct cyber-attack, drive-by download, exploit, keylogging, Malvertising, malware, phishing, ransomware, social engineering, spam, Trojan, virus (computer virus), and zero-day virus. Specifically, each of the smartphone cybersecurity threat category is described briefly along with description of how smartphone users' activities can make them vulnerable to such threat.

2.1. Spyware attack

Spyware is a form of malicious software that is capable of gathering personal information of an internet user, without their permission. The information it collects is then sent to a third party without the information owner's consent [39,40].There are 4 main different types of spyware, namely; system monitors, Trojans, adware and tracking cookies. Spyware is mainly used for tracking a user's movement online and serving dangerous pop-up ads.

Smartphone users can get infected with spyware by visiting certain websites, by responding to pop-up messages that ask them to download an application or program, and also through security holes in the browser or in other software, etc.

Generally, spyware is always hidden and can be difficult to observe. Individuals might notice a spyware infection when the virus starts using their system's resources and slows it down.

2.2 Direct cyber-attack

A cyber-attack is an offensive action by cyber criminals to deploy malicious code into systems with the intention of destroying, altering, stealing or taking any other advantage from this action [43]. The target of cyber-attacks includes all categories and sizes of information and communication technology (ICT) infrastructure, whether they are for individual or organization devices or networks.

Direct cyber-attack can occur in any of the following instances:

i. A system user uses an infected secondary storage device like flash drive on his/her system or mobile device
ii. A mobile device or system user visits a malicious website using an outdated application, system or programming software or click on phishing links
iii. Someone browses the internet using an unsecured public wi-fi etc.

2.3 Drive-by download

According to [44, 45, 46, 47, 48, 49], a drive-by download can refer to two things:

i. A download which a user authorized but without understanding the consequences (example: downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).
ii. The unconscious download of malicious software into a computer or mobile device.

Drive-by downloads can happen when a smartphone user visit some malicious websites, when reading an email or by clicking on a deceptive pop-up window. This type of attack usually affect a browser, an app or operating system that is obsolete and has bugs or other security flaws that has not been patched [44, 45, 46, 47, 48, 49]. Outdated applications are risk and hack tools used by cybercriminal for malicious purposes. This is why it is important to constantly maintain software updated.

2.4 Exploit

An exploit is a piece of software, a chunk of data, or a set of commands that takes advantage of a bug, glitch or vulnerability for malicious purposes. Exploits can cause disruptions in the behavior of computer software, hardware, or something electronic (usually computerized) [35,39,40]. By using exploits, cyber criminals can gain control of our computer or smartphone and carry out malicious activities.

One of the ways to protect smartphone user from exploits is to keep the smartphone software updated at all times and also take all essential security measures [58].

2.5 Keylogging

Keylogging attack is a form of attack where a cybercriminal uses malicious software to record or log the keys that a computer or mobile device user strikes on keyboard in order to get confidential information about the user in a concealed manner. The information stolen could be passwords, addresses, debit/credit card details and so on [72, 84].

People can intentionally install key loggers in systems for malicious purposes. Cyber criminals can also install keyloggers on systems remotely without the knowledge of the system owners.
Although many anti-spyware applications can detect some software-based keyloggers and quarantine, disable or cleanse them, but there is no solution that can claim to be 100% effective against this type of threat [72].

2.6 Malvertising

Malicious advertising otherwise known as Malvertising a form of adware attack whereby malware is spread through online advertising.Cyber criminals inject malicious or malware-loaded code into online advertising networks or legitimate websites, which then infect your systems through clicking, redirection or drive-by downloads [73].
Since online ads are managed by online advertising networks, even a legitimate website may host an infected web banner, although the website itself remains uncompromised [73].

Some key mechanisms used by cyber criminals to spread Malvertising include drive-by downloads, hidden iframes, pop-up adverts as well as web widgets and malicious banners. Another key mechanism used to spread Malvertising include third-party applications, specifically, the use of help desk, customer relation systems, and forums. [73].

2.7 Phishing

Phishing is another form of attack that cyber criminals use in order to steal sensitive information such as usernames, passwords, and credit card details. The attackers often times pose as a trustworthy or ligitimate entity and uses emails messages, social media and other forms of electronic communication to deceive innocent people. Phishing links are risk and hack tools. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability aspects of current web security technologies [41].

Phishing is done through emails, instant messaging apps or social media posts (on Facebook, Twitter, LinkedIn, etc.) [75].

2.8 Ransomware

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom [76]. Ransomeware attack locks user out of his/her computer or mobile device by either encrypting files on the hard drive or by locking down the system and displaying messages that can extort individuals into paying the attacker to remove the restrictions by providing a decryption key.

When one is attacked by a ransomeware, the chances of retrieving data are slim, except one is willing to pay the ransom. This is why having a data back-up in a secure location is good [59]. The attacker will promise to either decrypt the files, or send an unlock code that can decrypts the files/system once the ransome is paid but there is no guarantee that this happening. Trojan-ransom is responsible for most ransomware attacks on mobile devices

Ransomware which spreads like worm could infect systems through downloaded files or other vulnerabilities in a network service [76].

2.9 Social engineering

Social engineering is a form of attack which relies on the psychological manipulation of the victim and persuading the victims to perform certain actions or divulge confidential information [42].

Cyber criminals attack information system using impersonation, blackmails and lies, as well as bribes, threats and tricks. Also, they use social engineering attacks which includes phishing, whaling, pretexting, baiting, spear phishing and scareware [85]. Some instances includes cases where cyber criminals deceives their victims into revealing confidential information relating to their companies by pretending t be firefighting marshals, plumbers, contractors or other agents that require such information. [77]

2.10 Spam

Spam refers to unsolicited emails and other forms of messages that fill our inboxes. But recently spam has spread to instant messaging apps, texting, blogs, forums, search engines, file sharing and social media [39].

Spam messages sometimes looks safe but can also spreads viruses, worms and other types of threats. It can also promote deceptive marketing.

2.11 Trojan

A Trojan horse is a form of malicious software that conceals itself as a normal application or file to deceive a computer user into downloading and installing malware. The different types of Trojan for mobile devices includes Trojan-spy, Trojan-dropper, Trojan-banker, Trojan-SMS and Trojan-ransom

A Trojan can do many dangerous things to your system, like give cyber criminals unauthorized, remote access to your infected computer [40]. Once that happens, cyber criminals can:

- Steal login informations and debit/credit card information
- Install more malware, modify files,
- Monitor user's activities through screen watching, keylogging and so on.
- Use the computer in botnets (i.e collection of Internet-connected programs communicating with other similar programs in order to spread malware),
- Encrypt files, like in the case of ransomware
- Crash user's computer system
- Format system hard disks and destroying all the contents on the device, etc [78].

There are plenty of ways in which your system can become compromised by a Trojan [78]:

- through email attachments
- software or music downloads
- unsafe instant messages
- peer 2 peer downloads
- filling of online forms
- drive-by downloads, etc.

2.12 Virus (Computer Virus)

A computer virus is a form of malware that is capable of replicating itself and spreading to other computers and data files. Viruses attach themselves to other programs and execute code when the infected program is launched. They can be used to harm computer system, steal information, create botnets, log keystrokes and so on[79].

Viruses can also spread through web applications, downloaded documents, active-X files and cross-site scripting files. Often times viruses install themselves without the knowledge of the system user because cyber attackers uses software vulnerabilities, bugs, exploit etc to gain access to computers. Viruses can reside in executable files, data files and boot sector of hard drive. Furthermore, the polymorphic nature of some viruses makes it difficult for them to be detected with an anti-virus software [79].

2.13 Zero-Day virus

The flaws in a software can be discovered by a cyber criminals and at they can exploit it, in this case, the software developer or vendor has zero-day to fix the flaw. That is why such attach is called 'zero-day' attack. They exploit that vulnerability, launching an attack that users cannot defend themselves against. Antivirus programs rely upon signatures to identify malware, but the signature for this new breed of malware or virus is not in their database, because it is new and has not been sampled. So an-tivirus solution is not very effective against Zero-Day attacks. Additional security solutions to protect users from advanced zero-day attacks is needed[80].

Zero-Day viruses can be gotten through :

- drive-by downloads
- malvertising
- spam
- through email attachments
- software or music downloads
- unsafe instant messages
- peer 2 peer downloads

The difference is that, once you get infected, there is very little you'll be able to do to stop the infection and mitigate its effects [80].

3. Mitigation Strategies for Mobile Security Risks

Smartphone cybersecurity risk mitigation strategies are presented in this section. The cybersecurity risk mitigation strategies presented is twelve layers of protection approach which is based on recently developed cyber security best practices for mobile devices and applications [50-55].

3.1. First layer of protection: activate a screen lock

The first layer of protection for mobile devices, tablets and laptops is activation of automatic screen lock after a short period of inactivity (for example, 30 seconds) [56, 57]. In addition, automatic wiping of the device after 5 failed login attempts is also very important.

There is always the possibility of loosing mobile devices, tablets and laptops. As such, the choice of approach for implementing screen lock on mobile devices, tablets and laptops is important. Using PIN code for screen lock is not advisable; it is the easiest one to breach through shoulder surfing attack. Rather, using a unique password that is long and mixed with letters, digits, numbers and symbols is recommended. Also, one can combine patter and fingerprint to wake up the phone and also to lock the phone. Biometric is another means of authentication because it is difficult to breach or replicate. Fortunately, Android and other smartphones have the biometric screen locking facility. Putting this layer of protection in place, keylogging and some form of physical engineering attacks can be mitigated.

3.2. Second layer of protection: Mobile applications security (apps)

3.2.1 App Security Settings

In the past decade, there were huge innovations regarding the mobile phone market but now

Generally, smartphones are designed to run operating systems which can accommodate several mobile applications. Both the smartphone operating systems and the application programs are liable to have bugs and are inevitably subjected to different forms of security vulnerabilities **[58, 67].** Consequently, the way smartphone users deploy mobile applications and enforce the privacy layers is important.

This layer of protection can mitigate spyware, direct cyber, drive-by download, exploit, keylogging, malvertising, malware, ransomware, phishing, Trojan, zero-day, virus and some other forms of attack.

Two of the App Security Settings strategy presented are:

i. Use official app stores to download and install an app and disable the option to allow installation of third party applications
ii. Check and set the permissions settings for the apps

Use official app stores to download and install an app and disable the option to allow installation of third party applications

In order to decrease the possibility of being infected, mobile application users should always use official app stores to download and install an app and disable the option to allow installation of third party applications. Most third party applications carry malware that can harm mobile devices.

For Android phones, users can disable the option to allow installation of apps from sources other than the Play Store. This can be achieved using this sequence of menu selection on Android phone: from Settings → Security → Unknown sources, slide the button to turn off as presented in Figure 1.

Check and set the permissions settings for the apps

However, this does not mean that an app or game from the official store is 100% secure , sometimes, even popular apps, with more than 5 million downloads, can prove to be infected.

In addition, check the permissions for the installed apps and deny the apps access to what they are requesting for if you suspect anything malicious. For Android phone users, as presented in Figure 2, users can go to Settings → Apps → App permissions and check exactly what apps required permissions.

As presented in Figure 3, the Android smartphone user can check permissions granted for each app installed on the smartphone. This can be accomplished using the following sequence of instructions, as shown in Figure 3: go to Settings → Apps and scroll through the list of apps, click on one and individually check what permissions they requested and what you gave them access to [59, 64, 65].

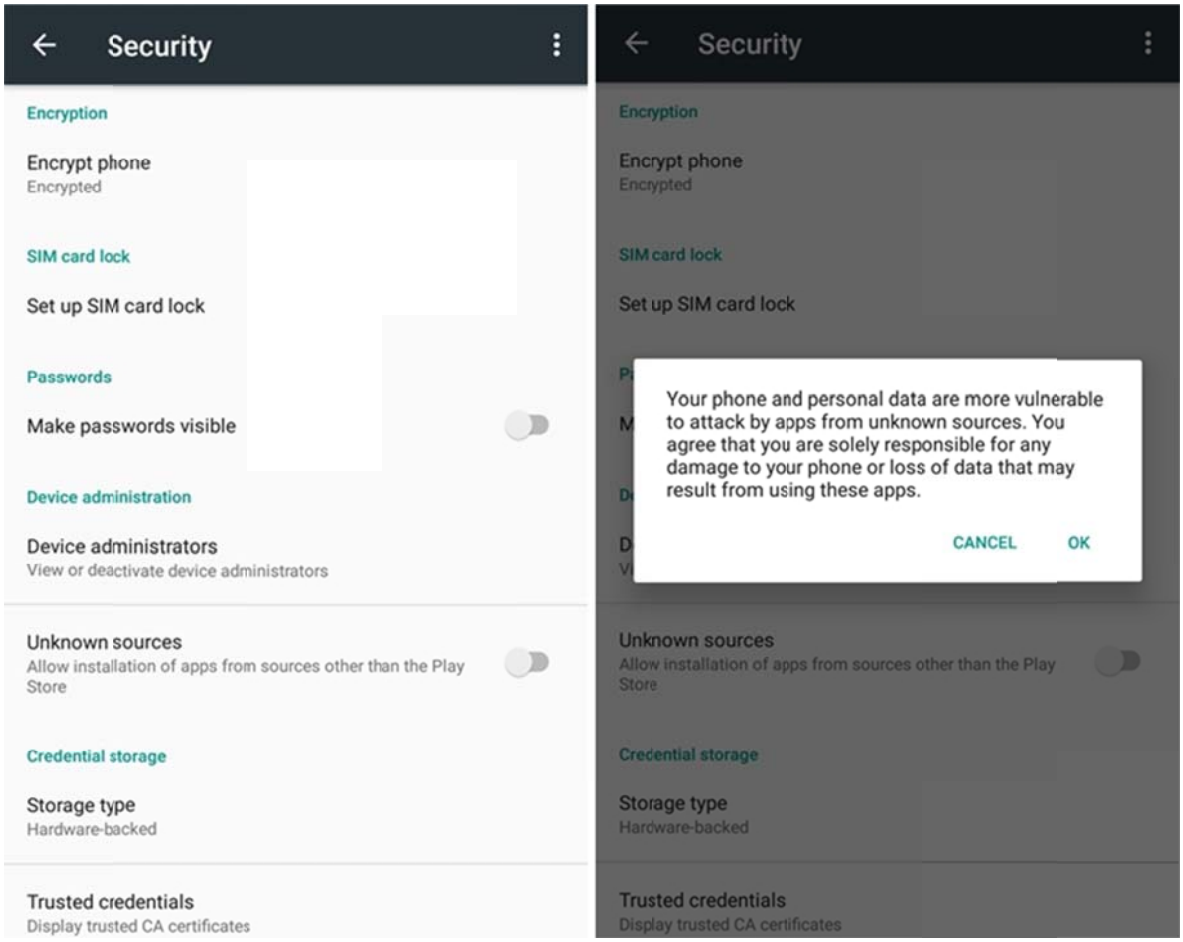


Figure 1 How to disable option for third party app installation

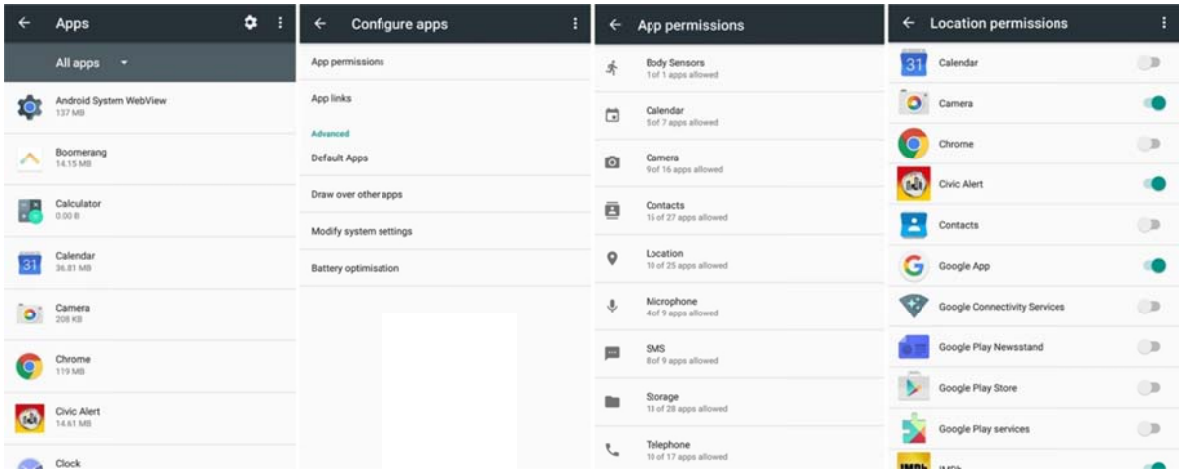


Figure 2: Setting of App permissions in Android phones

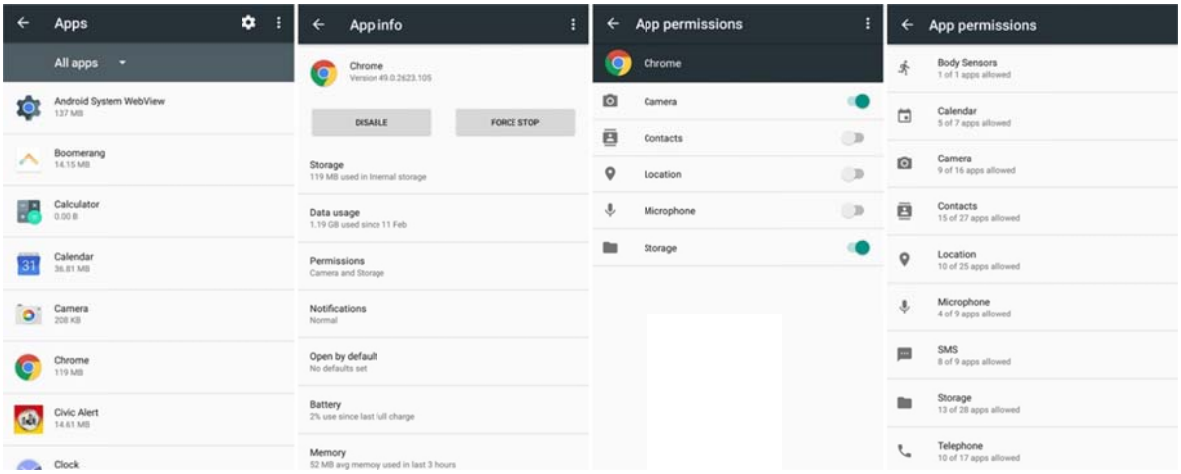


Figure 3 How to check permission of each Application in Andriod phone

3.2.2 Use of Clueful Tool

Clueful is a mobile application developed by Bit-defender and is designed to look over what permissions are requested by each app and warns the user if it is a potential threat. So, Clueful can make it easier for smartphone users to manage their app permission settings. As presented in Figure 4, clueful app knows the android and iOS operating system and the privacy risk associated with the applications installed. Also as presented in Figure 5, clueful app can also detect the mobile applications that can harm the mobile devices because of privacy issues associated with the application.

Notably, this form of protection can mitigate spyware, exploit, malware, ransomware, drive-by download, Trojan, zero-day, virus and some other forms of attack not listed here.

Figure 4 Clueful App showing iOS apps that can harm mobile devices

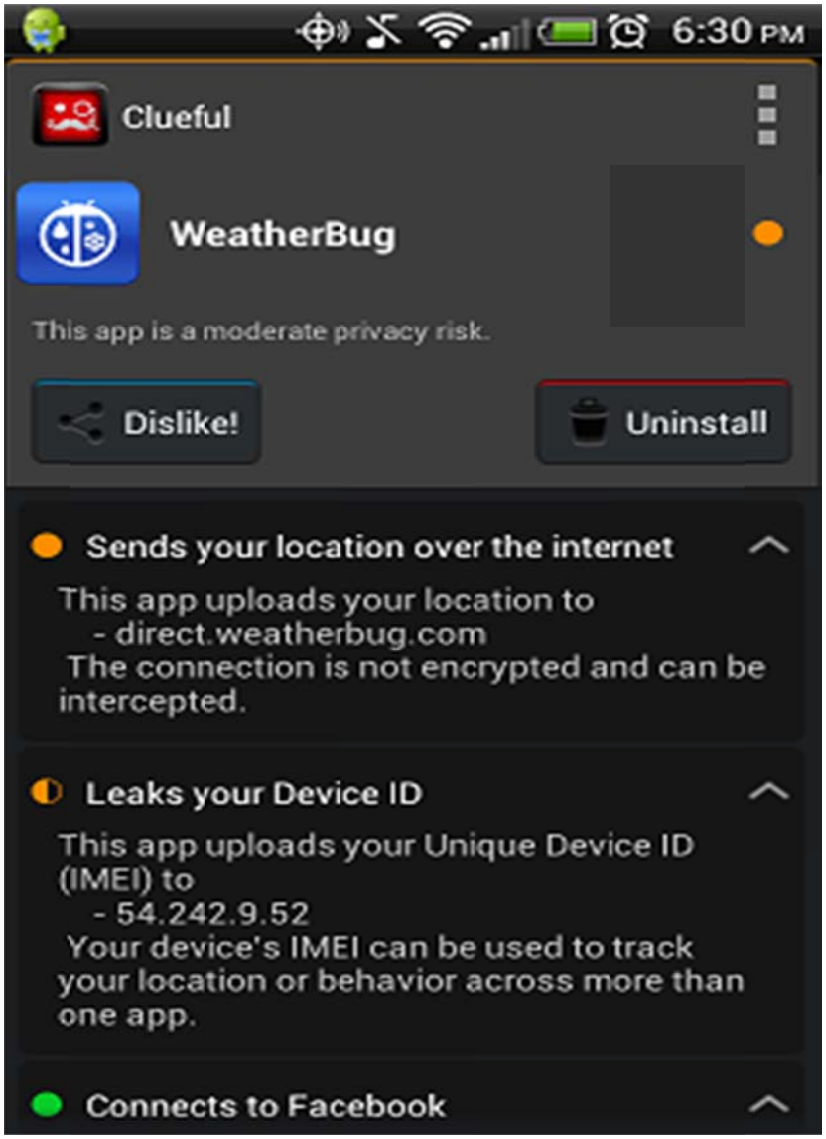


Figure 5 Clueful app showing risky apps

3.2.3 Cleanup of Apps Using Spring App Cleanup Tool

One can also do a spring cleanup of apps. It is generally known that most apps that are not in use are not always updated by the mobile user and such outdated apps are potential security risks. So, one of the security measures is to check all the installed apps and remove the ones that are not in use anymore. This form of protection can mitigate spyware, drive-by download, exploit, Trojan, zero-day, virus and some other forms of attack.

3.2.4 Battery, data and memory consumed apps

Smartphone users should regularly check out the apps that consume the most battery, data or memory, to see if there is anything suspicious about them. This way, the user can detect if the smart phones has been compromised.

3.2.5 Update Apps

Outdated apps leaves our data exposed to attacks and our smartphone are more vulnerable to security risks. As such, with each app that remains outdated, including browsers, our phones are more vulnerable to infections. Therefore, it is recommended that mobile users update their applications regularly on a daily basis. This form of protection can mitigate spyware, direct cyber, drive-by download, exploit, keylogging, malvertising, malware, ransomware, phishing, Trojan, zero-day, virus and some other forms of attack.

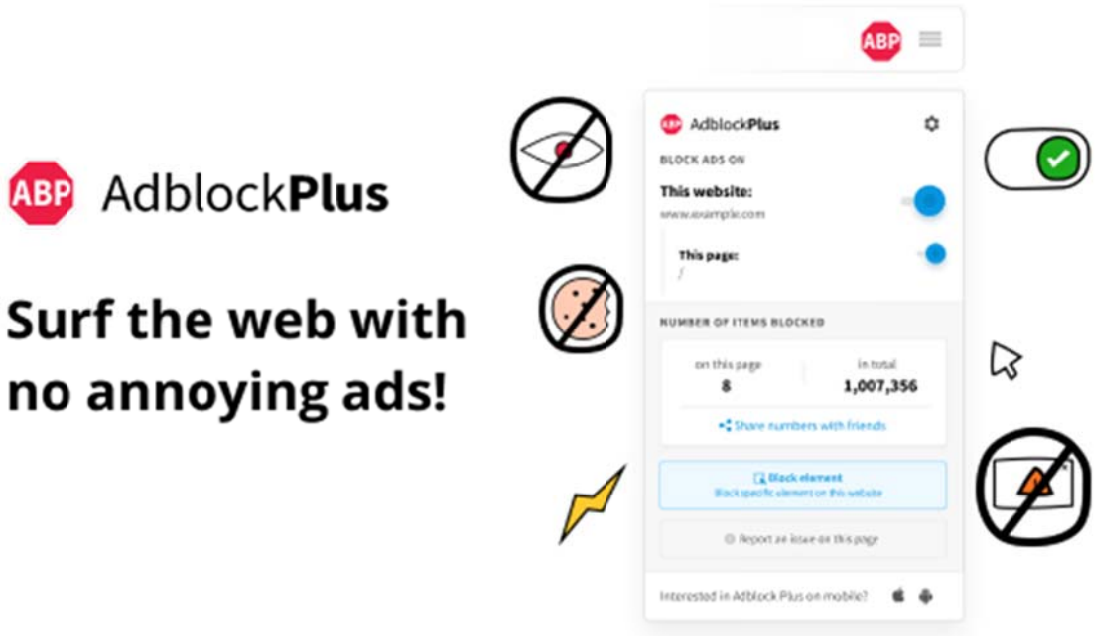
3.3. Third layer of protection: web browsing protection

3.3.1 Using Ad blocker

Ads on our smartphones can be exploited by cyber criminals. Notably, malware like Malvertising can be served right on our smart phones through ad servers – and

we do not even need to click on anything in order to get infected. As such, an ad blocker is needed on our smartphone not only because ads are intrusive but also a security measure **[62]**.

Particularly, an ad block software will help decrease the chances of infection. As presented in Figure 6, the adblock plus app is a good adblocker app that can block malicious advertising ads. The app user also has the option to select websites to block malvertising ads. This form of protection will mitigate malvertising, exploit, drive-by download, spyware, spam, Trojan and other forms not attacks not listed here.



6 Adblock plus app

3.3.2 Blocking POP-UPs

Blocking pop-ups will also help and that can be performed from the browser settings. For Firefox browser, for example, the following sequence of instructions can be followed to achieve that: Settings → privacy & security → Block Pop-ups → and make sure it is selected as presented in Figure 7. For Chrome, go to settings → privacy & security→ Site settings → pop-ups and redirect → then select Do not allow sites to send pop-ups or use redirect option, as presented in Figure 8. Similar steps can be taken for other browsers. This security measure will block drive-by download, exploit, monitors, Trojans, adware, tracking cookies and malvertising attacks.

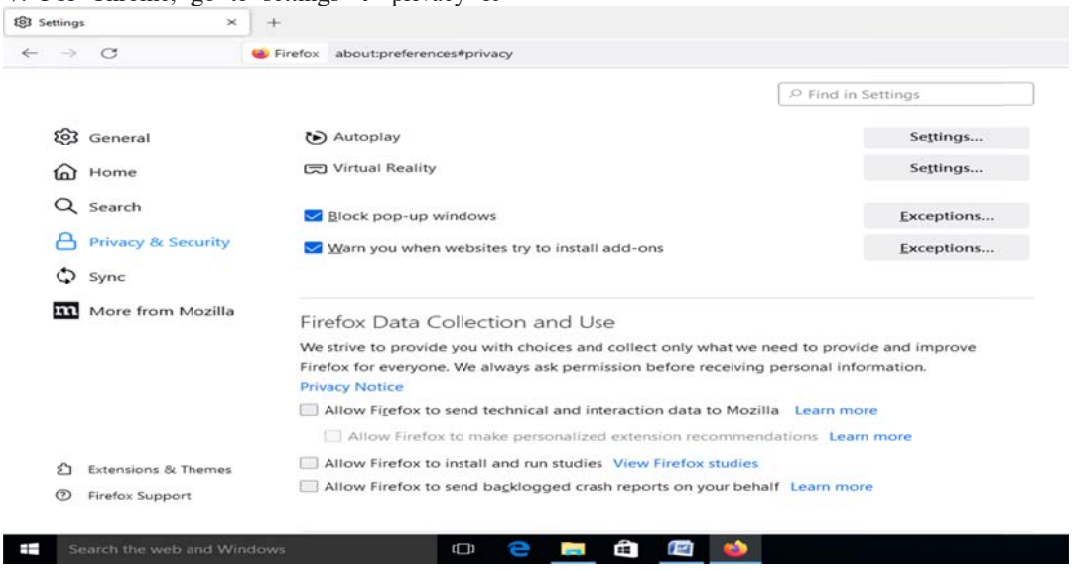


Figure 7 Blocking pop-ups apps in Mozilla Firefox browser

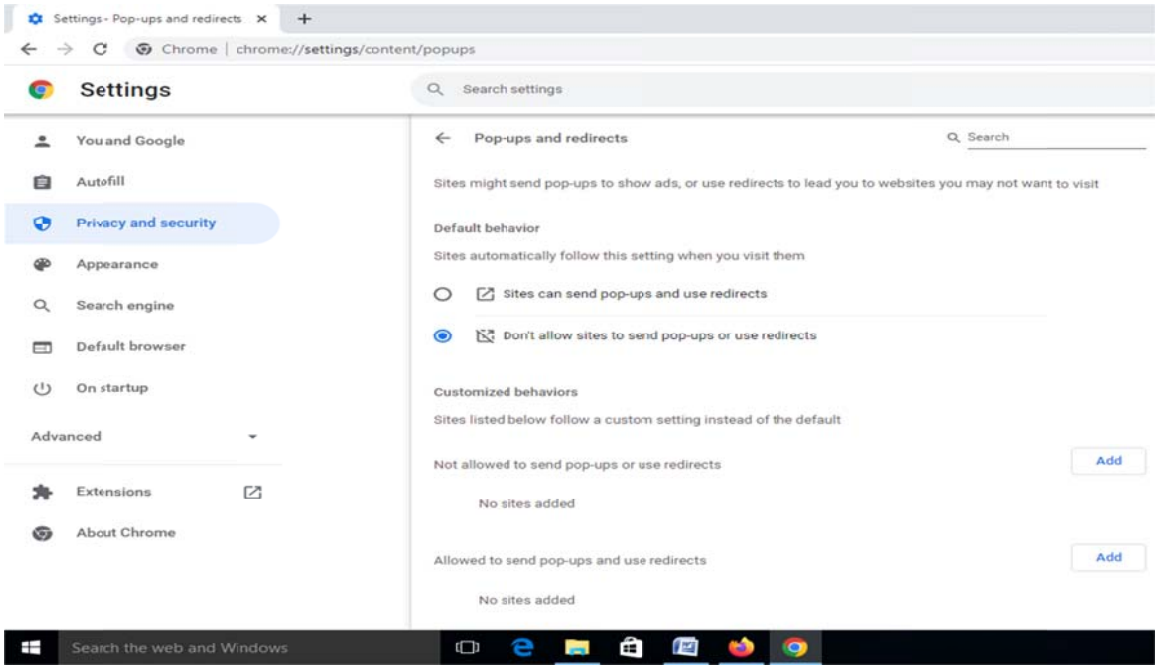


Figure 8 Blocking pop-ups apps in Chrome browser

3.4. Fourth layer of protection: beware of phishing

Cyber attackers can use phishing techniques to withdraw money from us, steal our identity, open credit card accounts in your name and much more. Phishing attack can by-pass even the strongest antivirus. A recent mobile threat called Mazar BOT – is a virus that spread via links sent in through text messages and it can give an intruder administrator rights on the victim's phone **[59, 63, 71]**. This allows the attackers to read, send and receive SMS, call people, and even erase the phone. Hence, it is the smartphone users should keep guard against phishing on all devices whether desktop, laptop, tablet or smartphone. Smartphone users should avoid clicking on suspicious links that we did not request and also be careful with those attachments we download via email or instant messaging services.

It is much harder to spot a phishing page on mobile phone than on personal computer (PC) or laptop. That is why it is important that smartphone users are advised not to click on links that the user never requested and do not know where they lead (especially short, hidden links). If somehow the user end up clicking on them and they require sign-in, the user should not give away the user's credentials. This layer of protection will mitigate phishing and other forms of social engineering attacks

3.5. Fifth layer of protection: activate remote device locator

In case our smartphone is ever lost or stolen, the easiest way to remotely locate it is by installing a dedicated app and making sure that the option to track its location is always turned on **[59,61]**. The following remote location applications are available for mobile device users: For iOS users, there is a tracking solution or application called "Find my iPhone"; for Microsoft, there is "Find my phone"; and for Android users, there is "Find my device" or "Android device manager". This layer of protection will take care of stolen or lost phones.

3.6. Sixth layer of protection: activate automatic backup

One of the smartphone security measures is to have automatic backups in cloud. This option is available on all smartphone operating systems. All the user need to do is to enable it (or not disable it, in case it is already set as default). In case the phone is lost, destroyed or stolen, we will not have to worry about the fact that we did not get the chance to backup all our data on it. The data and applications will synchronized and back up in the cloud automatically **[59, 68].**

The screenshot showing how to activate backup in android phone is presented in Figure 9 In order to backup Photos the user will have to go in the Photos app and configure it separately, the user can choose what folders to backup and at what size to upload the photos.

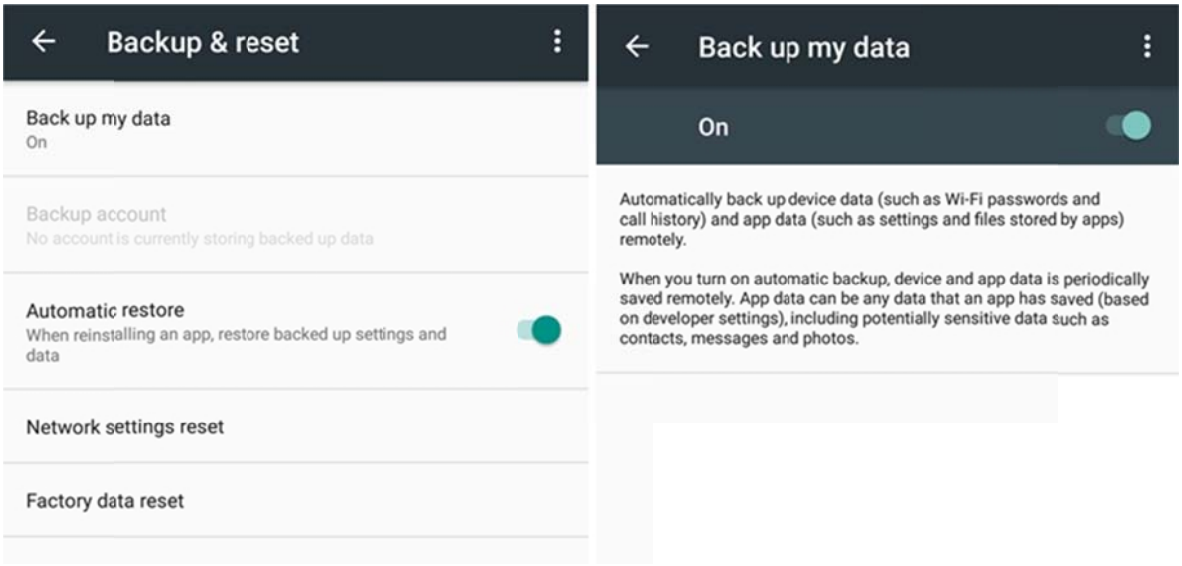


Figure 9 Screenshot showing how to activate backup in android phone

Anytime a user whose device was stolen or damaged gets a new device and set up using their credentials for Apple or Google account, all data and applications will be restored automatically. One can also set up the data to automatically backup in other accounts, such as Dropbox. This layer of protection will mitigate ransomware attack.

3.7. Seventh layer of protection: activate two-factor authentication

Irrespective of the type of account the smartphone user has, Apple, Google or Microsoft account, activating the two-factor authentication as a second layer security is important. Every time the user want to sign in on a new device or from a new location, it will require the user to verify his/her identity through a unique, time sensitive code, that user will receive via text message or using key [56, 57].

It is important that the smartphone user use different passwords for all his/her accounts. However, in case that someone manages to steal a phone, access it and find out the password, they will not be able to get through this second step of authentication. Signing in process of two step verification is presented in Figure 10. This layer of protection will mitigate keylogging and direct cyber-attack.

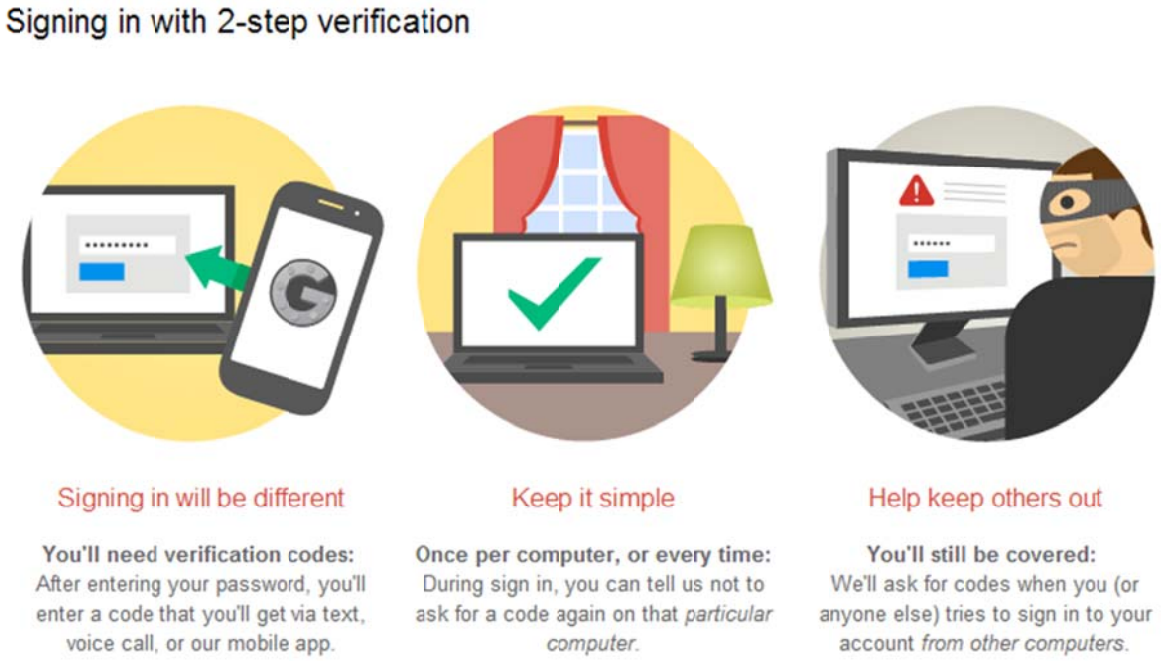


Figure 10 Signing in process of two step verification

3.8. Eighth layer of protection: turn on encryption

If a smart phone offers the option to encrypt the data on it, it is important to enable that option. In such case, full disk encryption can be implemented. Specifically, full disk encryption is a form of encryption for Android device where encryption key is used to encode all user data [60, 69]. During the encryption process, the device will ask the user to set a password to unlock the device and decrypt the data on it. If a user forgets the password, only a factory reset will grant the user access back into the system.
Unfortunately, the option to encrypt data is available for a limited number of operating systems, such as the latest Android versions and iOS. This layer of protection will handle ransomware attack.

3.9. Ninth layer of protection: install an antivirus

Another important smartphone security measures is the installation of trustworthy antivirus. Although anti-virus solutions for mobile device are not as potent as their desktop versions, but they better than not having antivirus installed. Also smartphone users need to have an antivirus product installed on our PCs. If PC is infected with a virus and phone is connected to it via USB, then the phone will also be infected **[59, 66].**

It is not a safe practice to connect smart phone to unknown computers. They might be infected with malware and end up infecting the mobile too. This layer of protection although not very effective, can mitigate spyware, direct cyber, drive-by download, exploit, keylogging, malvertising, malware, ransomware, phishing, Trojan, zero-day, virus, monitors, adware, tracking cookies and spam attack.

3.10. Tenth layer of protection: use a secure connection

Smartphone users are also advised to only use secure wireless connections. That means the user should not use free or public wi-fi, especially when accessing sensitive data. This is because on public networks information are accessible to anyone with the requisite knowledge of how to do so [60, 70]. A Virtual private network (VPN) can also protect smartphone user. VPN is a network created to protect users activities, it encrypts users internet traffic and data. Smartphone users can easily set up a VPN on today's smartphones.

Smartphone users are also advised always turn off their Bluetooths. It is not a secure way to communicate and should only be enable when necessary. This layer of protection can mitigate direct cyber, drive-by download, exploit, keylogging, malvertising, malware, ransomware, phishing, Trojan, zero-day, virus, adware, monitors and some other forms of attack.

3.11. Eleventh layer of protection: have a Factory Data Reset

If phone users plans on selling their phones, they should make sure they do not forget to do a Factory Data Reset before giving it away [58]. This way they will wipe all the data that was stored on it, including access to their accounts, system and app data and settings, downloaded apps, photos, music or any other data. This layer of protection can mitigate ransomeware attacks.

4.0 Conclusion

This paper presented some of the security threats that affect smartphone phone users and their defense mechanism. With the advent of the emerging technology of 5G networks and its infrastructure, cybercrime will be on the increase. Accordingly, cybercrime is always prevalent when the network and device users are ignorant of the security threats and the strategies that can be used to mitigate the risk. Also, many smartphone operating systems are equipped with features and settings can be enabled or disabled to mitigate many of the risks. However, ignorance on the part of the users is one of the major reasons for the rising cyber-attacks. Accordingly, in this paper, simple steps to be taken by smartphone users to mitigate many of the widespread cyber security risks are presented.

References

[30] M. Landmann, "Managing smart phone security risk," in Proceedings of the 2010 Information Security Curriculum Mobile Information Systems 13 Development Conference, pp. 145–155, Kennesaw, GA, USA, October 2010.

[34] E. Kim, D. Gardner, S. Deshpande, R. Contu, D. Kish, and C. Canales, "Forecast analysis: information security, worldwide, 2Q18 update," 2020, https://www.gartner.com/en/documents/3889055.

[35] Top 7 Mobile Security -reats in 2020, https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats- smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store, 2020.

[36] D. Emm, "Mobile malware-new avenues," Network Security, vol. 2006, no. 11, pp. 4–6, 2006.

[37] -e TOP 10 Mobile Risks of 2016, https://www.techrepublic.com/article/the-top-10-mobile-risks-of-2016/last, 2020.

[38] R. Sobers, "110 must-know cybersecurity statistics for 2020," 2020, https://www.varonis.com/blog/cybersecurity-statistics/.

[39] New MobileIron Report Details Most Common Mobile-reats and Blacklisted Apps, https://www.techrepublic.com/article/new-mobileiron-report-details-most-common-mobile-threats-and-blacklisted-apps/last,2020.

[40] A. Harkness, "Mobile malware threats," 2019, https://www.netmotionsoftware.com/blog/security/mobile-malware-threats.

[41] What Is Phishing Scam, https://usa.kaspersky.com/resourcecenter/threats/spam-phishing last, 2020.

[42] Mobile -eft Loss Report, https://preyproject.com/uploads/2019/02/Mobile--eft-Loss-Report-2018.pdf last, 2018.

[43] M. Bishop, Introduction to Computer Security, Addison-Wesley Professional, Boston, MA, USA, 2004.

[44] T. Caldwell, "Making security awareness training work,"Computer Fraud & Security, vol. 2016, no. 6, pp. 8–14, 2016.

[45] N. Gerber, B. Reinheimer, and M. Volkamer, "Home sweethome? Investigating users' awareness of smart home privacy threats," in Proceedings of the An Interactive Workshop on the Human Aspects of Smarthome Security and Privacy (WSSP),Baltimore, MD, USA, August2018.

[46] K. O'Loughlin, M. Neary, E. C. Adkins, and S. M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression," Internet Interventions, vol. 15, pp. 110–115, 2019.

[47] A. Przybyłek and D. Kotecka, "Making agile retrospectives more awesome," in Proceedings of the 2017 Federated Con-ference on Computer Science and Information Systems (FedCSIS), pp. 1211–1216, IEEE, Prague, Czech Republic, September 2017.

[48] A. Przybylek and W. Kowalski, "Utilizing online collabo-rative games to facilitate Agile Software Development," in Proceedings of the 2018 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 811–815, IEEE, Pozna´n, Poland, September 2018.

[49] M. H. Hussein, S. H. Ow, L. S. Cheong, M.-K. -ong, and N. Ale Ebrahim, "Effects of digital game-based learning on elementary science learning: a systematic review," IEEE Access, vol. 7, pp. 62465–62478, 2019.

[50] Webopedia, "Mobile security best practices," 2020, https://www.webopedia.com/TERM/M/mobile_security_best_practices.html.

[51] F. Stroud, "Mobile security best practices," 2020, https://www.webopedia.com/TERM/M/mobile_security_best_practices.html.

[52] H. Dowden, "-e 6 mobile device security best practices you should know in 2020," 2020, https://www.ntiva.com/blog/top-5-mobile-device-security-best-practices-2020.

[53] D. Hein, "7 essential mobile security best practices for businesses," 2020, https://solutionsreview.com/mobile-device-management/7-essential-mobile-security-best-practices-for-businesses/.

[54] S. Lerner, "Mobile device security best practices. How to protect portable technology," 2020, https://www.enterprisemobilityexchange.com/eme-security/articles/mobile-device-security.

[55] J. Mark, "8 best practices for mobile device security,"2020,https://www.jmark.com/8-best-practices-mobile-device-security/.

[56] A. D. Kent, L. M. Liebrock, and J. C. Neil, "Authentication graphs: analyzing user behavior within an enterprise net-work," Computers & Security, vol. 48, pp. 150–166, 2015.

[57] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authenti-cation," in Advances in User Authentication, pp. 185–233, Springer, Cham, Switzerland, 2017.

[58] H. Patel, "14 best practices for your mobile app security," 2020, https://www.tristatetechnology.com/blog/best-practices-to-improve-mobile-app-security/.

[59] M. Ciampa, Security Awareness: Applying Practical Security in Your World, Cengage Learning, Boston, MA, USA, 2013.

[60] K. Lab, "Best practices. Encryption," 2020, https://media.kaspersky.com/pdf/b2b/Encryption_Best_Practice_Guide_2015.pdf.

[61] L. Phifer, "Best practices for improving mobile data security,"2020, https://searchmobilecomputing.techtarget.com/tip/Best-practices-for-improving-mobile-data-security.

[62] A. S. K. Pathan, M. M. Monowar, and Z. M. Fadlullah, Building Next-Generation Converged Networks: Deory and Practice, CRC Press, Boca Raton, FL, USA, 2013.

[63] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: trends, tactics, and implications,"Technology in Society, vol. 32, no. 3, pp. 183–196, 2010.

[64] D. Burley, R. Carpinella, D. Chesebrough et al., Cybersecurity in our Digital Lives, Vol. 2, Hudson Whitman/ECP, New York, NY, USA, 2015.

[65] V. K. Velu, Mobile Application Penetration Testing, Packt Publishing Ltd., Birmingham, UK, 2016.

[66] M. E. Vermaat, S. L. Sebok, S. M. Freund, J. T. Campbell, and M. Frydenberg, Discovering Computers 2018: Digital Tech-nology, Data, and Devices, Nelson Education, Toronto,Canada, 2017.

[67] Documentation for app developers. Support In-App Up-

dates, https://developer.android.com/guide/playcore/in-app-updates, 2020.

[68] Documentation for App Developers. Data Backup Overview, https://developer.android.com/guide/topics/data/backup, 2020.

[69] D. Markuson, "Android vs. iOS: 2020 security face-off,"2020, https://nordvpn.com/pl/blog/ios-vs-android-security/.

[70] Wireless Connections and Bluetooth Security Tips, https://www.fcc.gov/consumers/guides/how-protect-yourself-online, 2020.

[71] R. Kalnins, J. Purins, and G. Alksnis, "Security evaluation of wireless networks access points," Applied Computer Systems,vol. 21, no. 1, 2017.

[72] https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/. Accessed 12th March, 2022.

[73] https://www.forcepoint.com/cyber-edu/malvertising. Accessed 12th March, 2022

[74] https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html. accessed 12th March, 2022.

[75] https://www.imperva.com/learn/application-security/phishing-attack-scam/. Accessed 12th March, 2022.

[76] https://www.cisa.gov/stopransomware. Accessed 12th March, 2022

[77] https://www.imperva.com/learn/application-security/social-engineering-attack/. Accessed 12th March, 2022

[78] https://www.kaspersky.com/resource-center/threats/trojans. Accessed 12th March, 2022.

[79] https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses. Accessed 12th March, 2022.

[80] https://www.kaspersky.com/resource-center/definitions/zero-day-exploit. Accessed 12th March, 2022

[81] W. Dixon and D. Samartsev, "3 technologies that could define the next decade of cybersecurity," 2019, https://www.weforum.org/agenda/2019/06/3-technologies-that-could-define-the-next-decade-of-cybersecurity/.

[82] https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/. Accessed 14th April, 2022

[83] https://www.techrepublic.com/article/2021-mobile-malware-evolution-fewer-attacks-escalating-dangers/. Accessed 14th April, 2022

[84] https://www.malwarebytes.com/keylogger. Accessed 14th April, 2022

[85] https://www.imperva.com/learn/application-security/social-engineering-attack/. Accessed 14th April, 2022