

Smartphone Security Issue and Cybercrime During Covid-19

Lee Zhao You¹, Intan Farahama Binti Kamsin², Zety Marlia Zainal Abidin³, Hemalata Vasudavan⁴

^{1,2,3,4}Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
¹tp066369@mail.apu.edu.my, ²intan.farahana@staffemail.apu.edu.my, ³zety@staffemail.apu.edu.my,
⁴hemalata@staffmail.apu.edu.my

Abstract— This research is to provide the solution on protect smartphone users from cybercrime. The issue to overcome is during covid-19 pandemic, the cases of cybercrime to smartphone users has increase with significant percentage compared to before covid-19. Stratified sampling will be used in this research and it categorized with the characteristic of the operating system like android and iOS, the data will be obtained through online survey. Human behavior has changed from physical working, physical classes, purchasing groceries, physical meeting and etc. to online based during pandemic. Where this behavior increases the chances of being attacks. Hence, the proposed system will help to enhance the security of smartphone, raise the awareness of protecting self-property and reduce the chances of being a victim of cybercrime.

Index Terms— Security, Smartphone, Cyber Crimes, Covid-19

1. Introduction

In today's generation, almost everyone use smartphone on daily basis. Smartphone invented on 1992 [1]. Since then, cybercrime has tied with smartphone due to smartphone can be use with multi-purpose [2]. In December 2019, SARS-CoV-2 as known as Covid-19 cause the pandemic worldwide. Hence, work from home is necessary for most of the companies to operate their business [3].

2. Literature Review

2.1. Research Domain

2.1.1. Smartphone

In countries all over the world, the used of smartphone have enable disruptions into everyone's daily life for messaging, browsing information, listening music while transport and many more [4]. Many cities in the world have officially invented their digital wallet, digital government, smart city and more to come in future [4]. In China, cash is almost no longer existed with most of the transactions performed through smartphone with digital wallet. According to a data collected by Hillhouse Capital in 2016 Alipay has 54 percent and WeChat has 40 percent, total 94 percent payment in the market are used digital payment [5]. Digital payment with smartphone certainly

brings benefits such as convenient, reduce the chances of being robbed, every transaction will be recorded for references, reduce the chances of counterfeit exist in the market and etc. [6].

Online shopping, fund transfer, digital wallet, social media and etc. all requires sensitive information such as real name, address, identification number and others [7]. Smartphone allowed users to download application that mentioned above to perform series of activity with convenient way [4].

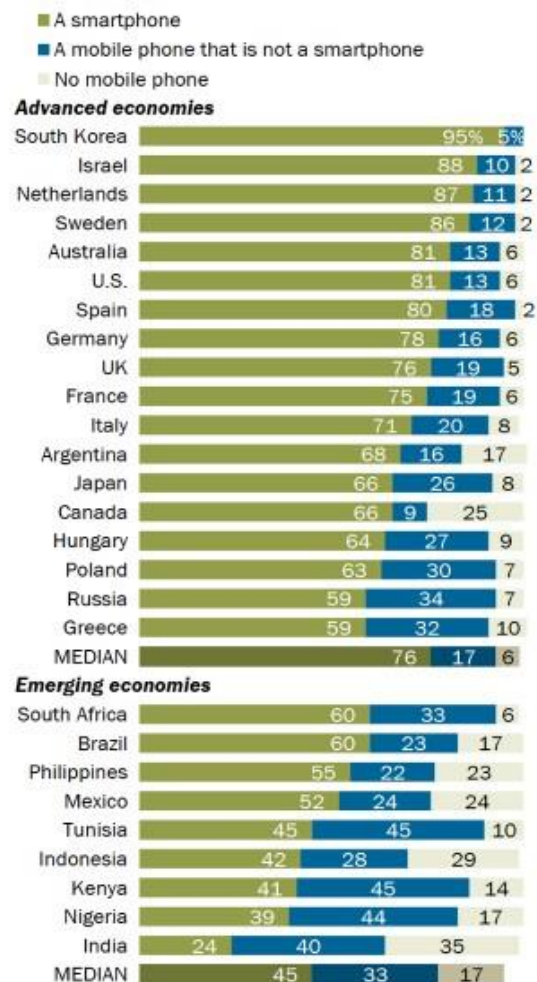


Figure 1: Percentage of Owning smartphone around the world [8]

Research conducted by Laura Silva are shown in figure 1, she is a senior researcher in Paw research center. Her research shows the percentage of owning a smartphone in a country. Those numbers in the figure1 indicates the numbers of peoples having smartphone is significate compare to those does not have a smartphone [8].

SARS-CoV-2 strikes the world on December of 2019, it causes locked down in most of the country around the world [9]. Quarantine became one of the solutions to stop the outbreak of covid-19, therefore the usage of smartphone has increase while stay at home [10].

2.1.2 Cyber-crime During Covid-19

Cybercrime has been evolving since the use of internet been widely used at worldwide [11]. During covid-19 pandemic, it causes most of the people and organization has to depend on the unsafe internet in most of the aspects [12]. Therefore, cybercrime has increase with the changed of life style that depended with internet.

According to Raghad Khweiled, Mohamad Jazzar and Derar Eleyan research, cyber-crime has increase 19.06% on phishing campaign and DDoS has increase 27.1% in between first half of 2019 to 2020. Contrast, ransomware attack has decrease 68.4% from the same time being examine with the other two crime mentioned above. The figure will be shown below:

Cybercrime	Count in H1 of 2019	Count in H1 of 2020	Relative change (%)
Phishing campaign	224556	267372	+19.06%
Ransomware	46,177,036	14,594,852	-68.4%
DDoS	3800000	4830000	+27.1

Figure 2: Comparison of cyber-crimes in first half of 2019 and first half of 2020 [12]

According to the articles, the rise of cyber-crime during covid has significant increase and huge number of peoples has their own smartphone today. The increases of the cyber-crime show the current smartphone system and the applications is not good enough to stop the attackers. Therefore, it is necessary to have an automated malware and suspicious activity scanner application to reduce the number of victims in future and enhanced the security of smartphone.

2.2. Similar Systems

2.2.1 Similar system 1 – Bitdefender

Bitdefender mobile security is created by Bitdefender where it's founded in Romania in the year of 2001 [13].

Bitdefender mobile security is a subscribed based application for one smartphone device to get the protection [14]. It requires certain requirements while installing such as android version 5.0 or later and active internet connection [14]. However, Bitdefender mobile security does not support IOS devices.

2.2.2 Similar system 2 – TotalAV Antivirus

TotalAV antivirus is created by TotalAV and it's founded in United Kingdom in 2016 [15].

Antivirus pro is a subscribe based for up to 3 devices and it support both android and iOS devices. It requires android version 5.0 and later, iOS version 9.3/iPadOS 9.3 or later [16][17].

2.2.3 Comparison Table

Product Name	Mobile Security	TotalAV Antivirus	Proposed System
Compatibility	Android	Android & iOS	Android & iOS
Real-Time Scanning	Yes	Yes	Yes
Manual Virus Scanning	Yes	Yes	No
24/7 Active Automated Scanning	No	No	Yes
Smartphone Optimizer	No	Yes	Yes
Parental Control	Yes	No	Yes
Anti-Spam	Yes	No	Yes
Email Protection	Yes	No	Yes
Chat Protection	No	Yes	Yes
Adware Prevention	No	Yes	Yes
Price(annual)	\$29.99	\$19	Free
Support multiple devices with one subscription	No	Yes, up to 3 Device	No

Table 1: Comparison between similar systems and proposed system

Table 1 shows the comparison between two similar system and proposed system. The special features and capability of each application are listed

3. Problem Statement

In daily life, most of the people consider smartphone as one of the daily important accessories, where it became a smartphone addiction for most of the people. [18]. During covid-19 pandemic, the usage of the smartphone has increased due to peoples has more free time at home [19]. Therefore, the cybercrime that related to smartphone has increase significantly due to the time spent online has increased for most of the peoples and the awareness has decrease due to peoples rely on online shopping. The personal information has been added to a lot of online platforms. Thus, it increases the percentage of leak of personal information [20].

4. Research Aims & Objectives

4.1 Aims

The aim of this research is to propose an effective automated malware and suspicious activity scanner application to enhance the security on smartphone to against cybercrime.

4.2 Objectives

- I. To develop a Malware scanner or detector application and perform scanning and detection from the database.
- II. To prompt alert for suspicious permission needed for certain application
- III. To constantly prompt users to check suspicious application and the permission.

5. Research Significance

This research will ensure that a solution is provided into helping on reducing the cybercrime through smartphone and obtain the awareness on protecting self-property. Smartphone users will gain the benefits on enhancing the security of their personal information and self-property from cybercrime during and post covid-19 pandemic. This prevents smartphone users as one of the victims of cybercrime such as scam, identity theft, blackmailing, phishing and more. The solution to overcome the existing issue is to create an automated malware and suspicious activity scanner application, an enhanced version compares to existing application that required users to manually click and run the application to scan their smartphone.

In additions, this research will help to raise the awareness of smartphone users to identify the cyber threats while using smartphone. Also, the data been collected by the application will help to improve the accuracy and speed of detections of threats

6. Research Methodology

The target users of the proposed system in this research are smartphone users that wants to had a secured smartphone environment.

Stratified sampling will be used as the sampling method in this research. The purpose of using stratified sampling is because it will get numerous of responses around the world. In Stratified sampling, the respondents will be divided in to strata and it will categorize based on the characteristic. In this research the characteristics will be based on the android and iOS. The method of collecting data will be sending out survey through online. Open and closed ended question will be provided in the survey.

7. Overview of the Proposed System

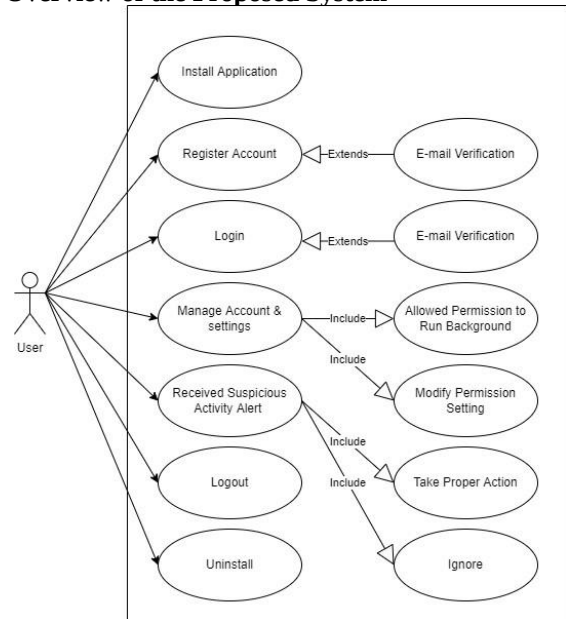


Figure 3: Automated Malware and Suspicious Activity Scanner Application Use Case Diagram

In figure 3 shows the use case diagram of proposed system. Users have to download and install application from either play store if using android device or Appstore if using iOS device. After the installation process is done, users have to register an account for login. The registration progress requires users to bind their email with the particular account and the verification email will be sent at the end of the registration progress to ensure the email is validate and prevent impersonator access. If the users already have a registered account after installation, the login option is available. User login also required email verification to prevent unauthorized access or brute forced attack. Email verification can enhance the security of the account and it act as multi-factor authentication to protect users from being attack or hacked.

After login process, users are required to give permission to the application access smartphone's run-in background, storage, contacts, file and media, location, SMS, and any required permissions. Users also can modify the permission after give

the access but it will certainly affect the application runs smoothly. The reason of requiring permission is to make sure the application works as the way it designed.

After all the setting has configured correctly, users can use the smartphone as normal. Once suspicious activity or malware has been detected, the application will rise alert to notify users. Users has two options on the alert. First option, users can take proper action such as delete the malware or take a deeper look on suspicious activity. Second option, users can choose to ignore the alert but it will increase the vulnerability of the smartphone except one circumstance that users is acknowledge on the alert is not harmful for the smartphone.

8. Conclusion

In conclusion, this research shows the rise of cyber-crime on smartphone during covid-19 due to the behavior of humans has to adapt with the serious disease now. Which the changed of behavior cause number of people became a victim of cybercrime. Users of smartphone can use the proposed system to enhanced the security of their smartphone and rise some awareness on new type of cyber-crime.

References

- [1] Tocci, M. (2019, August 19). History and Evolution of Smartphones. Retrieved from SimpleTextin: [https://simpletexting.com/where-have-wecome-since-the-first-smartphone/#:~:text=The%20first%20smartphone%2C%20created%20by,Simon%20Personal%20Communicator%20\(SPC\).](https://simpletexting.com/where-have-wecome-since-the-first-smartphone/#:~:text=The%20first%20smartphone%2C%20created%20by,Simon%20Personal%20Communicator%20(SPC).)
- [2] Zakiah Zulkefli, Manmeet Mahinderjit Singh, Azizul Rahman Mohd Shariff, Azman Samsudin. (2017). Typosquat Cyber Crime Attack Detection via Smartphone. *Procedia Computer Science*, 124, 664-671. <https://doi.org/10.1016/j.procs.2017.12.203>.
- [3] Øystein Tønnessen, Amandeep Dhir, Bjørn-Tore Flåten. (2021). Digital knowledge sharing and creative performance: Work from home during the COVID-19 pandemic. *Technological Forecasting and Social Change*, 170, 120866. <https://doi.org/https://doi.org/10.1016/j.techfore.2021.120866>
- [4] Gan, S. K.-E. (2018). The history and future of scientific phone apps and mobile devices. *Scientific Phone Apps and Mobile Devices*, 4(1). <https://doi.org/10.1186/s41070-018-0022-8>
- [5] Cheng, E. (2017, October 8). Cash is already pretty much dead in China as the country lives the future with mobile pay. Retrieved from CNBC: <https://www.cnbc.com/2017/10/08/china-is-living-the-future-of-mobilepay-right-now.html>
- [6] YAKEAN, S. (2020). Advantages and Disadvantages of a Cashless System in Thailand during the COVID-19 Pandemic. *The Journal of Asian Finance, Economics and Business*, 7(12), 385-388. <https://doi.org/https://doi.org/10.13106/JAFEB.2020.VOL7.NO12.385>
- [7] Donggen XU, Qiming GE. (2018). Rules of real name registration for internet access in China: infrastructure for cyber security. *Forensic Research & Criminology International Journal*, 6(1). <https://doi.org/10.15406/frcij.2018.06.00183>
- [8] Silva, L. (2019). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. Pew Research Center.
- [9] Wu Yi-Chia, Chen Ching-Sunga, Chan Yu-Jiun. (2020). The outbreak of COVID-19: An overview. *Journal of the Chinese Medical Association*, 83(3), 217-220. <https://doi.org/doi: 10.1097/JCMA.0000000000000270>
- [10] Serra, Gregorio&Lo Scalzo, Lucia&Giuffrè, Mario&Ferrara, Pietro&Corsello, Giovanni. (2021). Smartphone use and addiction during the coronavirus disease 2019 (COVID-19) pandemic: cohort study on 184 Italian children and adolescents. *Italian Journal of Pediatrics*, 47(1), 150. <https://doi.org/10.1186/s13052-021-01102-8>
- [11] Adam M. Bossler & Tamar Berenblum. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, 42, 495-499. <https://doi.org/10.1080/0735648X.2019.1692426>
- [12] Khweiled, Raghad and Jazzar, Mahmoud and Eleyan, Derar. (2021). Cybercrimes during COVID -19 Pandemic. *International Journal of Information Engineering and Electronic Business*, 13, 1-10. <https://doi.org/10.5815/ijieeb.2021.02.01>
- [13] Bitdefender. (2022). About Bitdefender. Retrieved from Bitdefender: <https://www.bitdefender.com/company/>
- [14] Bitdefender. (2022). mobile-security-andriod. Retrieved from Bitdefender: <https://www.bitdefender.com/solutions/mobile-securityandroid.html>
- [15] Parsons, I. (2022, 1 10). Is total AV an American company? Retrieved from parsons-technology: <https://parsons-technology.com/is-total-av-anamerican-company/>
- [16] TotalAV. (2022). TotalAV Andriod. Retrieved from TotalAV: <https://www.totalav.com/app/android>
- [17] TotalAV. (2022). TotalAV iOS. Retrieved from TotalAV: <https://www.totalav.com/app/ios>
- [18] Peter André Busch, G. I. (2021). Smartphone usage among older adults. *Computers in Human Behavior*, 121. <https://doi.org/10.1016/j.chb.2021.106783>
- [19] Tong Li, Mingyang Zhang, Yong Li, Eemil Lagerspetz, Sasu Tarkoma, Pan Hui. (2021). The Impact of Covid-19 on Smartphone Usage. *IEEE Internet of Things Journal*, 8, 16723-16733. <https://doi.org/10.1109/JIOT.2021.3073864>
- [20] Scott Monteith, Michael Bauer, Martin Alda, John Geddes, Peter C Whybrow & Tasha Glenn . (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, 2. <https://doi.org/10.1007/s11920-021-01228-w>