Chapter

Revealing Cyber Threat of Smart Mobile Devices within Digital Ecosystem: User Information Security Awareness

Heru Susanto

Abstract

In recent years, the number of mobile device users has increased at a significant rate due to the rapid technological advancement in mobile technology. While mobile devices are providing more useful features to its users, it has also made it possible for cyber threats to migrate from desktops to mobile devices. Thus, it is important for mobile device users to be aware that their mobile device could be exposed to cyber threats and that users could protect their devices by employing cyber security measures. This study discusses how users in responded to the smart mobile devices (SMD) breaches. A number of behavioural model theories are used to understand the user behaviour towards security features of smart mobile devices. To assess the impact of smart mobile devices (SMD) security and privacy, surveys had been conducted with users, stressing on product preferences, user behaviour of SMD, as well as perceptions on the security aspect of SMD. The results was very interesting, where the findings revealed that there were a lack of positive relationships between SMD users and their level of SMD security awareness. A new framework approach to securing SMD is proposed to ensure that users have strong protection over their data within SMD.

Keywords: smart mobile device, awareness, behaviour, cyber threat, cyber security, cyber crime

1. Introduction

Technology has been known to continually evolve since centuries ago, creating new innovations and infrastructures that changes how economies functions and overall improves standards of living within societies, and there have been no signs of it slowing down. One of the radical innovations within this century is the introduction of mobile phones. When mobile device was first introduced in 1973, mobile devices was a bulky communication device that was considered as a luxury good that aren't affordable to everyone and has limited features.

However, as the years goes by, emerging technology and innovation has successfully created an upgraded version of mobile phones which is known as smart mobile devices. Unlike mobile phones, smart mobile devices have more features to users, where it acts more than just a medium of communication, but as a device capable of storing data, capturing pictures of memorable moments and much more.

In other words, smart mobile devices had been delivering great number of benefits to everyone that it has deeply integrated itself within society's livelihood. Within this era of digitalization, more users are actively using their smart mobile devices to conduct activities such as paying bills online, managing their finances or do some online shopping as a direct result of the incremental upgrades that had been made which includes increased storage, power and speed. In addition, smart mobile devices are also a part of a large computing environment that encompasses a child's legacy, a user's persona and the keys to a user's home or digital life which includes any items in the house that is connected to the user's mobile device. But for every good thing that has been created, there's always a downside to it. New technology such as smart mobile devices also provides opportunities that could be reaped and exploited by malicious entities with ill intentions, hence exposing users and organisations to potential cyber threats such as hacking or data breaches [1–3]. According to a research made by comScore in 2016 (**Figure 1**), they have revealed that across the different age brackets of users in the UK and Canada, the average usage time of mobile devices is considerably higher than the average usage time of desktops.

A statistic developed by Broadbandsearch discovers that the total percentage of users accessing global websites through their mobile devices has increased exponentially within the last five years, ranging between the year 2013 to 2018. In 2013, the amount of combined web traffic from mobile devices was at 16.2% and the value has surged year by year, where by the combined web traffic was at a high value of 52.2% in 2018. Another research made by Statista (**Figure 2**) reveals that the number of mobile users will continue to increase within the next 5 years, where it estimated that the number of smart mobile device users will grow from 6.8 billion in 2019 to 7.33 billion in 2023.

Overall, as users spend more time with their mobile devices, these mobile devices would have accumulated and stored tremendous amounts of private data and information that it eventually becomes an attractive target for malicious groups or entities such as hackers. McAfee in their "Mobile Threat Report 2019" discovered that these cyber criminals will keep creating tactics to bypass mobile security in order to execute their cyber threat activities for the sake of one common goal, which is to maximise their income and profits.

There are various cyber threats that are affecting smart mobile devices and one of the cyber threats commonly found in mobile devices is malware. Malware had been infecting mobile devices for more than a decade and the increasing number of mobile devices infected by it is certainly very concerning. **Figure 3** shows that malware cases has increased by approximately 310% since 2016, thus reinforcing the undeniable fact that these malware authors have continued to adapt and create

Figure 1.
Average usage time of Mobile devices.

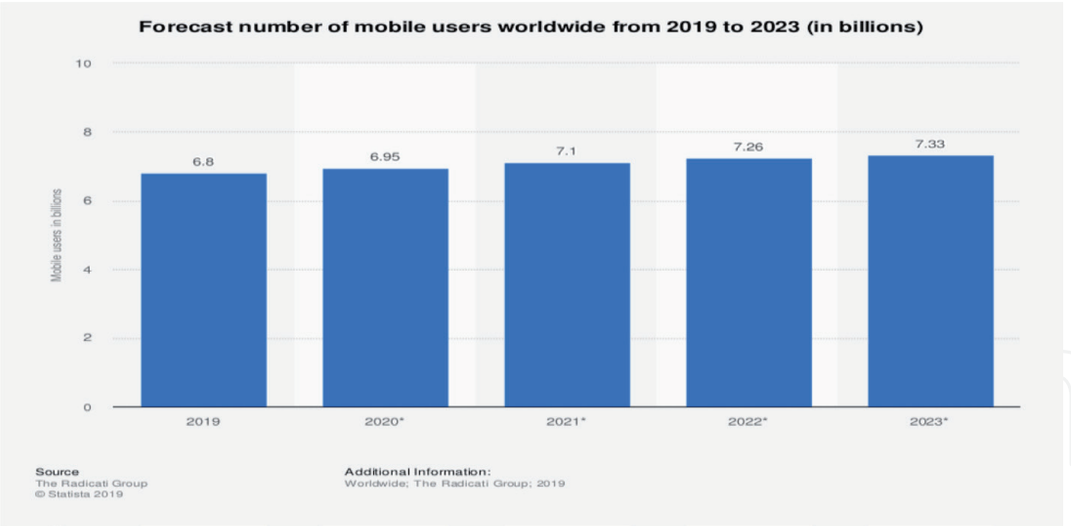

Figure 2.
Number of Mobile users.

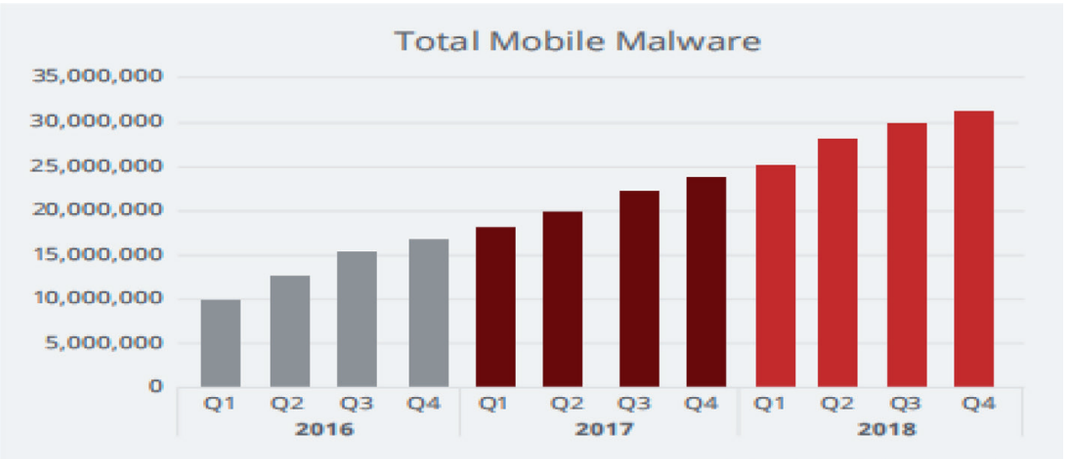

Figure 3.
Mobile malware.

new tactics against any challenges it encounters [2]. Malware, in the face of cyber security and countermeasures, instead has become more serious, dangerous and harder to detect, and it shows no signs of decline. Hence, all of this shows how important it is for users all over the world to protect and keep their smart mobile devices secure and safe from becoming a victim or prey to cyber criminals through implementation of cyber security in mobile devices.

Significance of the study.

Various researchers have highlighted the importance of protecting sensitive data from cyber threats by implementing cyber security measures within smart mobile devices. Awareness of the risk of mobile threats invading and stealing personal information from their mobile devices and the methods of mitigating this risk through mobile security methods.

Aim and objectives of the study.

The aim of this study is to measure the level of smart mobile device security and privacy awareness. The specific research objectives are shown as follows:

1. To reveal the different types of smart mobile devices usage.

2. To explore the attitudes of users towards smart mobile device security

3. To discover the category, costs and impact of cyber threat incident on smart mobile devices

4. To propose a new framework approach to securing SMD

5. To ensure users have strong protection over their data and the type of cyber security required to combat cyber threats on SMD comparing with security standard.

Structure of the study.

This first section has outlined the background, significance of the study, the aims and objectives of the study as well as the limitations of the study. The rest of the paper will be structured in the following way. The second section will present the literature review related to cyber threats and cyber security. The third section will discuss on the methods utilised in collection of data. The fourth section will be the discussion on the survey findings and how it relates to SMD security. Finally, the last section will be on the recommendation of a new framework as well as conclusion.

2. Literature review

The topic of cyber threat and cyber security on mobile devices had been greatly debated by various researchers around the world. Thus, this section will be reviewing numerous literatures on cyber threats and cyber security in the context of mobile devices as follows:

- Definition of a mobile device
- Cyber threats in mobile devices
- Cyber security in mobile devices
- Related works

Definition of a mobile device.

Mobile device can only be defined when the two aspects such as the software and hardware aspect are explained together [3–5]. A mobile device will usually have a small form that has a non-removable data storage and are equipped with an operating system that is particularly different from the operating system of laptops or desktops. A mobile device should be equipped with at least one wireless network interface such as cellular network or Wi-Fi for the purpose of connectivity and communication. Also, a mobile device should be able to obtain and install applications through various ways such as app stores, websites or other third party sources. There are also other common features of a mobile device but are optional such as the ability to connect to multiple wireless or area network interface and the ability to connect to real-time location services through the use of Global Positioning System (GPS). Other features of a mobile device also includes the microphone which allows voice to be recorded, a built-in camera that allows mobile device to record or capture pictures as well as a removable data storage.

Cyber threats in mobile devices.

Mobile threats can be classified into four different categories of mobile threats which are (1) application-based threat, (2) physical threat, (3) network-based threat

and (4) system-based threat. The first category is application-based threats. Outdated or unpatched third-party applications in mobile devices poses risks as hackers may exploit the vulnerabilities within those applications. Users that are still using an old mobile device that has a lack of software updates, an untimely patch update or a cease in support for older operating systems are at risk of being compromised by hackers through the holes within the software or the OS itself [4, 6, 7]. Additionally, there are various application-based threats which consist of (a) Malware, (b) Spyware, (c) Privacy threats and (d) Vulnerable applications.

a. Malware is referred as malicious software that is operated by hackers to obtain access to a mobile device and perform illegal criminal activities. It requires the hacker to install malware into the mobile device through many devious ways that are very difficult to track or trace. Malware could be used to alter or execute actions without the owner's permission, such as sending prompt or subitaneous text messages to contacts, charging phone bills or acquiring successful control over the mobile device.

b. Spyware is known as a program used by hackers which utilises private or confidential data without consent for illicit motives, whereby it usually targets sensitive information such as owner's list of contacts, phone call records, text messages, real-time location, gallery images, browser history and email addresses.

c. Privacy threat could occur when hackers alters or erase the mobile device's data using a software applications that are not somewhat program codes. The sensitive data within the mobile device are visible to the attacker and can easily be exploited for different purposes that are ill-natured.

d. Vulnerable application refers to applications that have holes that could be exploited by hackers to sneak into the mobile device and gaining full control over the mobile device. Once control over the mobile device is established, hackers can easily acquire personal or sensitive information, execute unfavourable activities against user's will such as rendering certain services useless and force download unknown applications without authorization.

The second category is physical threat. The authors refer physical threat as a security incident which involved a mobile device being stolen or lost in the process. Mobile devices have a greater chance of being lost or stolen than laptops due to the features of mobile devices such as its small size, lightweight and easy to carry, thus making it the perfect target of attackers. An attacker that had successfully obtained physical access to a mobile device will proceed with other malicious activities that are conducted from the attacker's computer. The mobile device will display an image of a malicious system that is trying to install a harmful software or attempting for data extraction. Further added that mobile devices could be misused by attackers in several ways such as creating a fake identity by using the personal information contained inside the mobile device or by selling sensitive or confidential data to the black-market for profit motives [7, 8].

The third category is network-based threats. Most of the mobile devices used by consumers are usually connected to wireless network interface such as Wi-Fi or Bluetooth, the use of these network interfaces carries certain risks. It makes mobile devices vulnerable towards malicious activities such as wireless eavesdropping that is performed using off-the -shelf software such as Aircrack-ng Suite or Wifite. Attackers could exploit the network to plant malwares on mobile devices

unnoticeably whenever a mobile device is connected to a wireless or cellular network. Once the malware has been installed, it will give attackers free access to the mobile device, allowing them to modify or extract any confidential or sensitive information within the mobile device. Also, attackers can use the method of Wi-Fi sniffing to conduct criminal activities by reading, monitoring or altering any unencrypted data that is travelling in the same network [9–11]. Mobile device manufacturers introduce unintentional flaws or vulnerabilities into their own devices such as the incident with Samsung's Android SwiftKey keyboard which was discovered to be susceptible to eavesdropping attempts. Another similar incident occurred with Apple devices, specifically the iPhone's Operating System (iOS) where the "No iOS Zone" flaw causes any iOS devices within range to automatically connect to a malicious fabricated network and constantly crashes those devices. In addition Web-based threats are known as threats that involve user's interaction with online services through the access of the Internet, which could be divided into smaller categories which are (a) Phishing scams, (b) Drive-By downloads and (c) Browser exploit [5, 8, 12, 13].

a. Phishing scams happens when users are being delivered through their email, text messages or social media links that appears to originate from a legitimate company or organisations when in reality it is a scam. The main purpose is to trick users, individuals or organisation, into disclosing sensitive or confidential information such as debit/credit card number or passwords.

b. Drive-by-downloads occurs when a hacker obtains illegal access to a mobile device as a result of a user opening up a web page or clicking on a link found on a website. It will then trigger an automatic download of malicious applications that wasn't consented by the user.

c. Browser exploit is described as a devastating code that allows hackers to exploit the unsecured data within the mobile operating system. It could also be described as malicious software that aims to alter a mobile browser's settings without any consent that is usually triggered when a user had visited unsafe websites.

Another research classifies cyber threats into two different aspects which are the technical aspect and the management aspect of mobile security. The technical aspect of mobile device cyber threat are quite similar to what was described by previous researchers, where it consisted of device security threats, network security threats, services security threats and content security threats. However, there was one factor that wasn't touched on in the two previous research but was present within this research work, and it was concerning on the management aspect of cyber threat in mobile devices [1, 14, 15].

The management aspect of mobile device cyber threat studies the threats that are associated with the security policy of mobile devices, which can be broken down into three categories namely (a) application distribution environment security threat, (b) law institutional security threat and (c) domestic and foreign enterprise environment security threat.

Cyber security in mobile devices.

However, the study revealed measurement of users that may possibly undertake in order to protect their personal data stored inside their mobile device [16–18]. One of it is by using password or PIN lock features to ensure that only the user can access the device and prevent outsiders from accessing it. Also, users should only connect their mobile device to wireless networks that are protected by a password and avoid connecting the device to public networks as public networks raises the chances of

the user being compromised. Users that have their devices with Bluetooth enabled should set it to non-discoverable to other users so that attackers will not be able to sneak in and steal the user's sensitive data and the user's contact number should never be revealed easily to other people as it might be used to execute ill-intent activities.

Basic steps that users can exercise to protect their mobile devices from cyber threats such as (1) Regular or prompt update of operating system, (2) Device rooting or jailbreaking prevention, (3) Mobile applications management and (4) Mobile antivirus.

1. Regular or prompt update of operating system - when mobile devices run on outdated operating system (OS) such as Android or iOS, these devices are much more vulnerable to cyber attacks, such as the entry of malicious applications into the mobile device. This situation could have been prevented if the latest operating system had been updated on time and without delay.

2. Device rooting or jailbreaking prevention - When users decided to root or jailbreak the operating system on their mobile device for certain personal reasons, users should remind themselves the gravity and consequences of it because at the moment they do so, the responsibility of the privacy and security of their mobile device have transferred from the developers to the users themselves. Users should also be informed that cyber threats such as spyware are more likely target devices that are rooted or jailbroken.

3. Mobile applications management - Users should install mobile applications from trusted and secure source such as Apple store or Google store and avoid installing from untrusted sites from the internet. By downloading applications from trusted sources, users do not need to worry about security as the applications are scanned for any vulnerabilities before installed and the installed applications will automatically be updated to fix any vulnerabilities in the future.

4. Mobile antivirus - Installing a mobile antivirus may seem ineffective for Apple devices as Apple ensures that it will not be allowing any applications from gaining any permission it needs to execute any damage. It may seem redundant to install a mobile antivirus in Android devices as Android restricts any app installation from sources other than Google store but for users that tend to install applications from outside sources, an antivirus will protect the device to some extent from unknown threats originating from the installed applications.

Moreover, a set of security solution was proposed as function as it can be implemented by organisations and enterprises to manage mobile device security [19–22]. The first solution is by creating a general policy that includes the restrictions on the use of mobile devices within the organisation such as restrictions on user access and application access tools and hardware such as cameras, removable storages such as USB flash drive and hard disk drive (HDD) as well as to local OS services, for instance inbuilt email, web browser, contact and calendars. The policy also includes guidelines on the management of wireless network management such as Wi-Fi or Bluetooth and additionally limits personnel's access to organisation's services based on the mobile device's brand, model, software client version and OS status (ensures device is not rooted or jailbroken). Any suspicious actions will be monitored, detected and reported back to the management and once it has been found that the actions has violated the general policy, further actions and reprimandation will automatically take place accordingly.

The second solution concerns on the data storage and communication within the organisation. The management should strongly encrypt organisation's confidential data that are contained within the built-in storage as well as the removable media storage and any device that will be reissued to other personnel must first be wiped to clean the data previously stored in it. Additionally, if any of the organisation's device is assumed to be lost or stolen by unknown instigators that by any chance cannot be trusted, the management should initiate remote wipe on the device to prevent confidential information from being harvested by malicious attackers [16, 23–25]. Another way to prevent the mobile device from being accessed illegally is by implementing a configuration that has wipe feature within its devices that will automatically factory-resets all the data within after it detected several failed authentication attempts. The organisation should also aim at having a secure data communication between organisation and mobile devices by encrypting it using Virtual Private Network (VPN) or other encryption tools that suits their needs.

The third solution is based on the device and user authentication. A user authentication step should be implemented before any personnel could access the organisation's data and resources, which could be in the form of password or other various authentication such as token-based or domain authentication. The organisation should also include certain parameters for password characters, password length and the maximum number of retries allowed before the device is locked out or wiped. In cases where a user has requested a password reset or was locked out of the mobile device, the administrator should be able to restore the user's access to it remotely. Any device that is suspected to be accessed in an unsecured location should be remotely locked under the supervision of the administrator and any device that is in an inactive state for a certain period of time should be locked automatically by the device itself.

The final solution involves restrictions on various aspects of mobile applications. The management should restrict the list of app stores that can be accessed by personnel to download mobile applications or instead, the management could issue applications from a chosen application store. In addition, the installation of certain applications should also be restricted through the process of whitelisting and blacklisting. There should also be a restriction on what device location are permissible for the application to access such as storage access or camera access. The digital signatures found in applications should be verified to ensure that the applications installed are from a safe and trusted source and that the code wasn't altered in any way.

3. Methodology

The evaluation method which has been utilised by countless researchers in obtaining research data known as the questionnaire method was implemented in this study. A random sampling method has also been chosen and implemented as a method of collecting the research data in this study. The nature of questionnaires asked will be focused on the topic of cyber threats, cyber security and its relationship with SMD. Through the employment of the random sampling method, a set of questionnaires have been distributed within the duration of approximately three months to the targeted group of respondents. Other platforms as well as social media had also been utilised to distribute the online survey such as WhatsApp and Instagram. The target respondents of this study are focusing particularly on the youths which include the generation-Z strictly. This particular group of respondents have been chosen as they represent the majority of mobile device users that are

technologically literate. A variety of respondents with different gender, background and educational level had taken part in the study. A total of 109 respondents have participated in the online questionnaire where almost all of the respondents are within the age range of 20–29 years old which matches the targeted group of respondent previously mentioned before.

4. Findings and analysis

The data analysis will be made according to each of the section that has been created within the survey questionnaire as follows:

- Demographics
- General section
- Password security
- Application security
- Email and Account security
- Personal security
- Knowledge and Attitude towards mobile security

Demographics.

In this section, the questions asked the respondents about their gender, their age group, their current status as well as their present educational level.

Referring to **Figure 4**, out of 114 respondents that participated in the survey, 67.5% of them are female respondents and consequently 32.5% of them are male respondents, thus highlighting that a majority of the respondents are female. When looking at the age range of the respondents who have answered the survey questions, a large number of them are within the age range of 20–29 years old which contributes to a high 83.3% of total respondents. The rest of the respondents originated from two other age groups where 15.8% of the respondents are aged below 18 years old while the remaining percentage are within the age group of 30–39 years old.

Figure 4.
Respondents demographic.

It has been observed in **Figure 5**, that amongst the respondents, 49.1% of them are students from Universiti Teknologi Brunei, 13.2% of them are students from Universiti Brunei Darussalam, 5.3% of them are from Politeknik Brunei and 11.4% of the respondents came from various other public or a private higher institutions such as Institute of Brunei Technical Education (IBTE), Laksamana College (LCB), Cosmopolitan College of Commerce & Technology and Micronet International College. Additionally, the survey also received responses from non-university students where it comprises of 7.9% from high school students, 7.9% from the working population as well as 5.3% from the unemployed population.

General Section.

In this section, the questions that were asked were focused on finding out the type of mobile device the youths are generally using, their general purpose of using a mobile device as well as the frequency of internet connectivity amongst the youths.

Figure 6 shows the questions that were asked within the general section of the survey questionnaire. When respondents were asked about the type of smart mobile device they are currently using, there are 86 respondents that uses Android devices which contributes to 75.4% of the chart, 24 respondents that uses Apple devices which contributes to 21.1% of the chart and a small number of respondents which is 4 respondents uses both Android and Apple devices thus contributing to 3.5% of the chart. An assumption was made in this survey whereby every respondents that answers the survey has at least one mobile device, which is the reason why the question directly asks its respondents the type of mobile device used. It can be seen

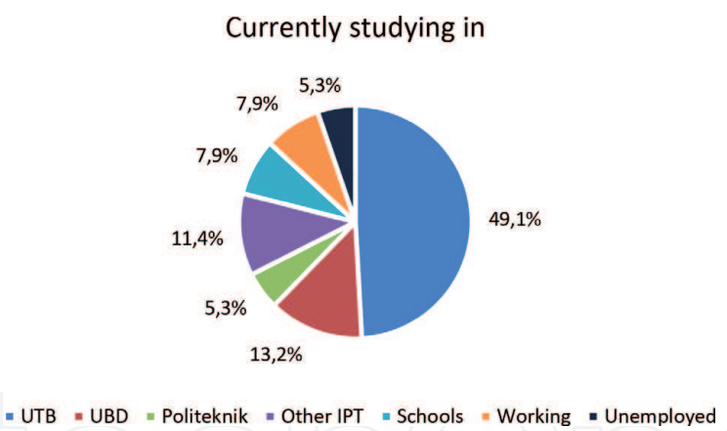

Figure 5.
Education background.

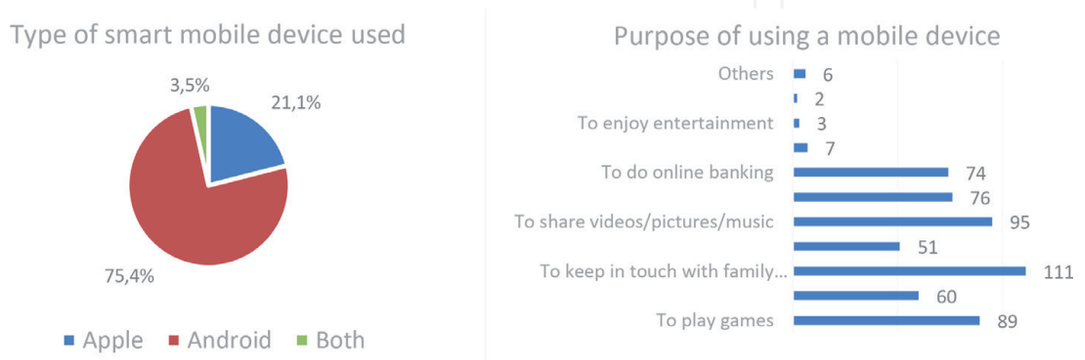

Figure 6.
Smart Mobile device usability.

that majority of the respondents favours the android devices compared to the apple devices which is proven by the results shown on the charts.

Also, when the respondents were asked about their general purpose of using a mobile phone, the respondents have chosen various purposes as the survey questionnaire allowed them to choose more than one purpose. The chart shows that 111 out of 114 respondents which agreed that one of the main purpose of using a mobile device is to keep in touch with family and friends. The chart also showed that 95 respondents uses a mobile device to share videos, picture or music, 89 respondents uses their mobile device to play games, 76 respondents uses their mobile device to make online transactions, 74 respondents uses their mobile device to perform online banking, 60 respondents utilises their mobile device to make professional and business contacts and 51 respondents uses their mobile device to create new friends.

There were also some minority purposes chosen by the respondents where 7 respondents believes their purpose of using a mobile device is to go on social media platforms, 3 respondents uses their mobile device to watch entertainment, 2 respondents uses their mobile devices to take pictures and lastly, one respondent each believes that their purpose of using a mobile device is to either surf the internet, read news, listen to radio, download video, create digital notebooks or doing some phone modification. This means that most of the respondents feel that it is safe to use their mobile device to do important activities such as maintaining communication as well as making online/bank transactions. It also acts as an indicator that the respondents felt it is secure enough to send and share videos, music or pictures amongst themselves and their friends through their mobile devices.

Figure 7 shows that when the respondents are asked about how frequent they are connected to the internet, 100% of the respondents agreed that they are constantly connected to the internet and when asked about how they are connected to the internet in which they are given three choices, 95.4% of the respondents are connected through the Wi-Fi medium, 93.6% of the respondents are connected through their mobile data (cellular connection) and 25.7% of the respondents are connected through the use of hotspot. Another assumption was made while doing the survey which believes that almost all respondents are constantly connected to the internet and this assumption was proven through the survey results whereby 100% of the respondents stated that they are frequently connected to the internet. It is inevitable for the users of mobile device to be constantly connected to the internet because within this technological era, the only way to maintain communication and receive information is through the use of internet.

Password Security Section.

In this section, the questions asked were focused on discovering respondent's behaviour and habit in regard to the security of their mobile device and the network they are using to surf the internet.

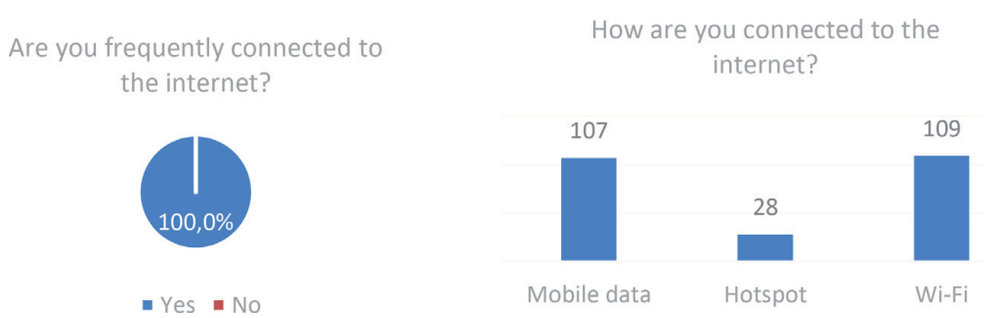

Figure 7.
Internet connectivity types.

In **Figure 8**, when the respondents were asked about how frequent their network password are changed, 43.0% of the chart which accounts to 49 respondents rarely changes their network password, 26.3% of the chart which accounts for 30 respondents changes their password sometimes, 23.7% of the chart which accounts for 27 respondents never changed their password, 4.4% of the chart which accounts for 5 respondents frequently changes their password and finally, only 2.6% of the chart which accounts for 3 respondents always changes their password.

It is important to change the network password regularly as it is one of the simple measures to avoid people from silently stealing the user's network data unconsciously. Few of the dangers of not changing the network password regularly is that the users might be exposed to network attacks such as sniffing or eavesdropping and there might also be illicit entities or hackers that had previously obtained the password to enter the network, hacked into the user's network and using the network to perform unlawful actions.

In **Figure 9**, when the respondents were asked about what type of security measure they have implemented to their mobile device, the responses received were divided into few categories. About 40.4% of the respondents uses fingerprint protection only, 24.6% of the respondents uses password protection only, 11.4% of the respondents employs solely pattern protection, 2.6% of the respondents uses face protection measure and 5.3% does not employ any kind of protection measure. There were also respondents that utilises multiple protection measures for their mobile device where 12.3% of the respondents uses a combination of two protection measures and 3.5% of the respondents uses a combination of three protection measures.

It can be seen that many users tend choose fingerprint lock compared to other security measures such as password or pattern. It is considered as the best option because fingerprint is a unique identifier of each individual person and since it is

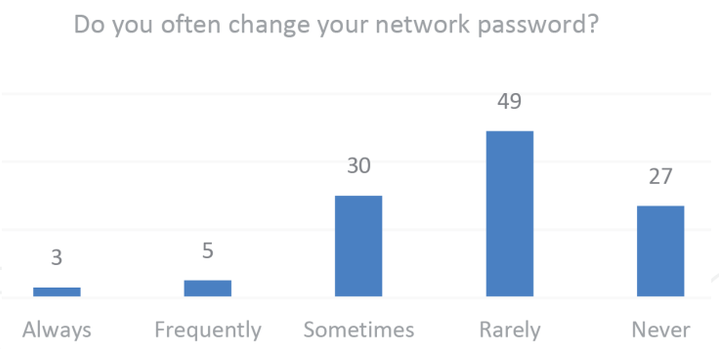

Figure 8.
Changing the passport.

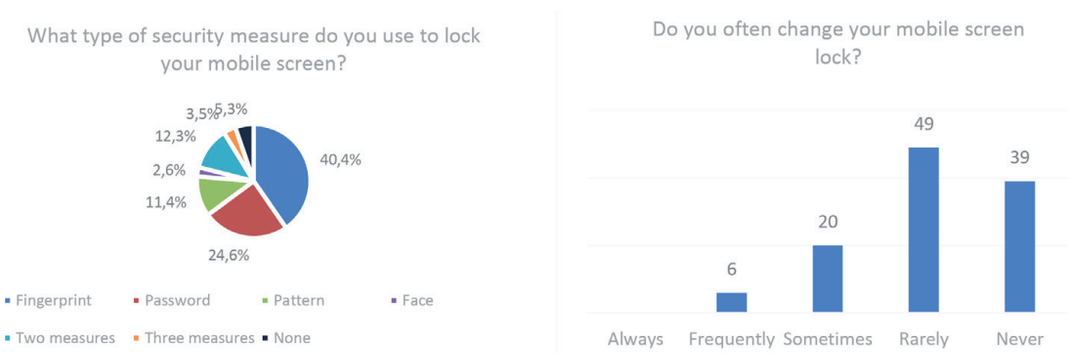

Figure 9.
Security measuring.

hard to obtain someone else's fingerprint, it makes it difficult for attackers to gain access to the mobile device. Password and pattern are also good measures of security lock for mobile devices, but it has a disadvantage. As all smart mobile devices have touch screen input, any act of accessing the mobile device by using the pattern or password lock will inevitably leave smudges or residues of the screen which could be used by attacker to retrace the pattern and access the device. But then again it will take the attacker some time to figure out the pattern correctly, hence it is still better for a mobile device to be protected by a security measure rather than having none at all in order to reduce the risk of being breached.

The final question asked within this sub-section was aimed at discovering how frequent does the respondents change their mobile screen lock or protection measure and it was seen that 43.0% of the respondents which contributes to 49 respondents rarely changes their mobile screen lock, 34.2% of the respondents which is equivalent to 39 respondents never changed their mobile screen lock, 17.5% of the respondents which contributes to 20 respondents alter their mobile screen lock sometimes and 5.3% of the respondents which is equivalent to 6 respondents frequently changes their mobile screen lock.

It can also be see that many respondents have never change their mobile screen lock or rarely do so. The act of changing the mobile screen lock regularly is particularly important to users that implement password and pattern lock measures. It will reduce the user's risk of being breached physically or virtually and if the worst case comes whereby an attacker that aims to breach the device had figured out some of the correct password or pattern, the process of regularly changing the lock screen will ensure that these attackers will fail in their attempt.

Application security section.

In this section, the respondents were asked on questions that were inter-related in nature that aims at revealing respondent's behaviour as well as awareness towards the security of applications.

In **Figure 10**, when the respondents were asked about whether the respondents have installed any mobile applications from unknown sources, 71.9% of the respondents agreed that they have installed applications from unknown sources while the remaining 28.1% of the respondents have never installed applications to their mobile device from unknown sources. When users downloads applications from unknown sources, it means that users are downloading third party applications from third party app stores rather than the official stores such as Google or Apple store. Third party applications are known for being risky because these applications has been created by other creators or programmers and not made by the manufacturer of the mobile device or the operating system of the mobile device. Basically these applications cannot be guaranteed safe and secure for use or free from malware by the mobile device's manufacturer as they came from unknown sources.

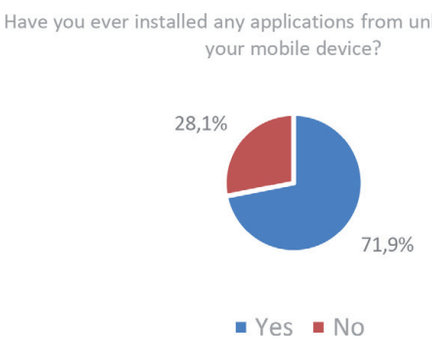

Figure 10.
Apps installation from unknown sources.

Figure 11 shows two charts which reflect the in-depth questions that were aimed towards the security aspect of applications, where one of the questions asked whether they have read the End User-Licence Agreement (EULA) and privacy policy before installing any applications. The chart shows that 56.1% of the respondents have never read it, 36.8% of the respondents have read the policy sometimes and the remaining 7.0% of the respondents always reads the policy prior to installing any applications to their mobile device. When users are being prompted to install any application, there will usually be a window which request the users to deny or agree to the agreement stated in the application's privacy and policy which includes the EULA policy. It is very important for users to read these policies because some these policies will state the purpose and the time period for using the user's personal data and information as well as how users are supposed to use their manufacturer's applications without breaking any of the policies.

The respondents were also asked on whether they have read the application's phone access permissions before installing any application and it was revealed that 46.5% of the respondents always reads it before installing any applications, 36.0% of the respondents reads it sometimes while 17.5% of the respondents never reads it. Prior to installing any application to a mobile device, the application will request the user's permission to access certain folders or areas within the mobile device such as the camera, storage, location and more. Before accepting such permissions, users must first read the "phone access permission" carefully so that can evaluate for themselves whether it is safe to do so instead of just accepting any permissions because there might be instances where some applications requested certain permission that it does not necessarily needs. The act of just accepting any permissions that prompt up could lead in the user handing over their information willingly and unknowingly to shady application developers or fraudulent data miner, which could further result in the exposure and breach of the user's personal information.

Email and Account Security.

In this section, the questions asked were aimed at measuring and assessing respondent's tendency as well as awareness towards the security aspect of email and accounts.

In **Figure 12**, when the respondents were asked a question on whether they would initially check the authenticity of the sender before opening the attachment received. The second chart shows that 67 respondents which would always check the authenticity of the sender before opening the attachment, 41 respondents would sometimes check for the authenticity while the remaining 6 respondents had never checked the authenticity of the sender. This is a good indicator that shows users are taking precautionary measures to protect themselves from harmful attacks that are being orchestrated through the medium of emails and even text messages. These

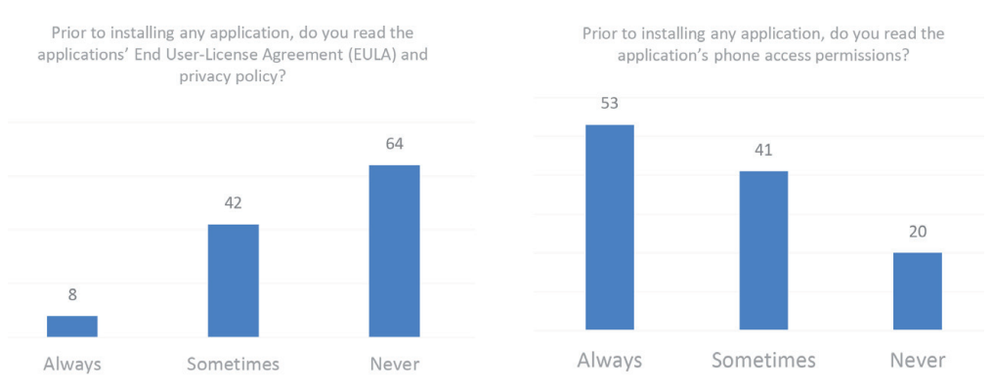

Figure 11.
Security aspects of apps.

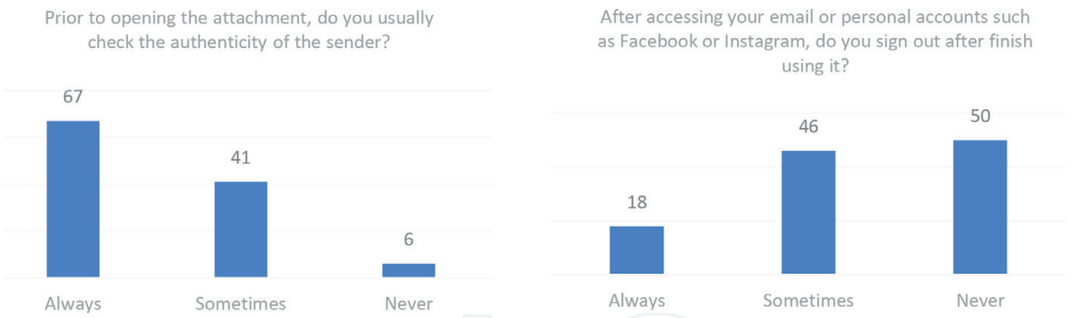

Figure 12.
Sender authenticity.

attackers could be sending emails or attachments that may seem to be from a legit sender such as official corporations initially but it is a scam that aims to trick the users to open, download or click the sent attachment or link. When users successfully downloaded it, the virus will start to spread to other emails or contact list thus as a result endangering other users as well. Hence, this behaviour of checking the sender serves a good measure to protect user's mobile device and the sensitive information contained in it from being harmed.

Additionally, when respondents were asked whether the respondents sign out from their email or personal accounts after using them, the graph showed that only 18 out of 114 respondents always logs out from their accounts after use wile 46 respondents does log out from their accounts sometimes and 50 respondents had never signed out from their accounts after using them. Most users that accessed their personal accounts through their mobile device tend to tend to stay logged in rather than logging out after using them. This might pose risk and dangers to user's personal data and information because if someone unknown such as an intruder gained access to a user's mobile device such as in the case of mobile device theft, these intruders could easily access the user's personal accounts as they are already logged in and it makes it possible for the intruder to steal the user's identity this way. Hence, the behaviour of logging out from personal accounts after using them is a best practice to ensure that the user's sensitive and personal data are constantly protected from any possibilities of malicious actions.

Personal security.

In this section, the questions that were asked to respondents were focused on the security aspect of respondent's personal data in their mobile device and their action in securing it. The result shows that 66.7% of the respondents stores their confidential or sensitive data within their mobile device while 33.3% of the respondents does not store any within their mobile device. Many users considers their mobile as an item that is very near and personal to their owners and it is also regarded very crucial as it usually kept the user's sensitive or confidential information which is proven from the results stated above. Due to the mobility of mobile devices, users tend to keep their confidential or sensitive information within their mobile devices since it allows users to access is much faster compared to other means. It is necessarily not wrong for users to keep their precious data within their mobile devices, but it is recommended for users to set up the most optimum level of security measures to their mobile devices in case it is under a threat of being compromised or breached by malicious entities. Then, when the respondents were asked next on whether they have installed any security software such as anti-virus within their mobile device, only 39.4% of the respondents installs a security software within their mobile device while the remaining 60.6% of the respondents do not equip or install any security software to protect their mobile device.

From the results, it is observed that many users believes that installing security software or applications such as anti-virus is not crucial or important for their mobile device. Thus, when these respondents were asked on their main reason for not installing any security software, various answers have been received where one of responses mention that their mobile device already had a built-in antivirus, hence the absence of need to install another anti-virus. There are few similar responses that were made by different respondents where some of it mentions that some respondents did not know the existence of an anti-virus for a mobile device and some had problems choosing an anti-virus that is trustworthy to be installed. Some of the respondents also stated that it is not necessary to install an anti-virus because they believed that they have not installed any malicious programmes or applications to their mobile device. A few of the respondents are hesitant to install a security software due to the need to pay for it while some are blatantly has no desire to install one at all as they deem anti-virus as unnecessary.

Various kind of behaviours in these responses reflects that many users are having a lack of awareness and knowledge on the importance and benefits of having an anti-virus within their mobile device which is worrying in general. For instance, users are hesitant to install an anti-virus software because they assumed that the built-in anti-virus is sufficient and it makes users think their mobile device is safe enough. But it still does not justify the reason for not installing any security software because there is no operating system that is completely secure and invulnerable from cyber risk and danger. Malicious programs, applications, viruses or malwares could still infiltrate mobile devices through every possible way which is why it is recommended for users to set layers of protection for their mobile device instead of being negligent and over-reliant on the built-in protection within their mobile device.

Then, a question was also asked to the respondents that have installed anti-virus on their mobile device on whether they regularly update their mobile security software. The responses that were received was surprising because out of 44 respondents, 18 respondents relied heavily on the auto-update feature of their mobile device to update their anti-virus, 16 respondents regularly updates their anti-virus and the remaining 10 respondents rarely updates their anti-virus. This indicates that there are over reliance amongst users towards the automatic update function in their mobile device's operating system or the anti-virus itself. Users that rarely updates their anti-virus or only relying on automatic update are usually the type of users that assume that it is "good enough" to have an anti-virus that prevents harmful activities being done to their mobile device.

Knowledge and attitude towards mobile security.

Within this last section of the survey questionnaire, the questions asked are aimed at measuring the respondent's level of knowledge towards mobile security as well as their attitude on the subject of security within mobile devices.

In **Figure 13**, when the respondents were asked on whether they have experience any privacy or security breach on their respective mobile devices, 97 respondents which contributes to 85.1% of the chart had never experienced anything similar before while 17 respondents which is equivalent to 14.9% of the chart have experienced a privacy or security breach on their mobile device beforehand. It can be assumed that these 17 respondents or users might have become victim to privacy or security incidents due user's lack of security measures implementation to their data and mobile device. Thus, due to a prior experience in a privacy or security breach, these users might have increased their knowledge on this matter and started tightening their security measures in their effort to prevent the incident from happening again. On the other hand, it also shows that most of the respondents have never experienced such incidents which might be due to sufficient implementation

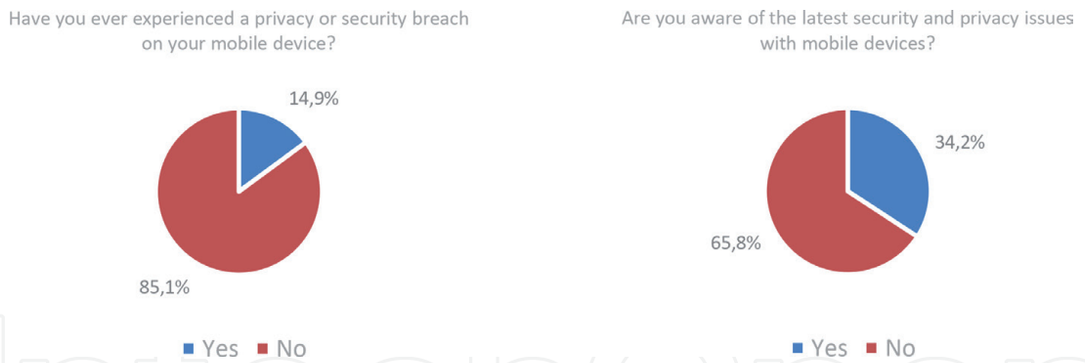

Figure 13.
Smart Mobile devices security breaches.

of some security measures to protect their mobile device and their personal data. But it is gravely reminded for users not become negligent and starts lowering down their security efforts because attacker will always look for those small opportunities to perform malicious activities.

Then, when the respondents were asked on whether they are aware of the latest security as well as privacy issues that is occurring to mobile devices, 65.8% of the respondents are apparently not aware of any mobile security issues while 34.2% of the respondents are aware of the security issues that are trending nowadays and happening to mobile devices. This means that most of the mobile device users are not educating themselves with the latest security incidents and happenings associated with mobile devices. It is a fact that many cyber crime related cases such as privacy and security issues are not being publicised and the society rarely hears anything about these issues but it does not mean that users should not take any initiative in educating themselves especially within this era of digitalization. It is important to be updated with such matters because the information gained by reading, researching and knowing how the security issues happen could turn out to be useful to users. Users which had beforehand known of such incidents could equip themselves with the useful information and when users are encountering a similar incident, users knows the know-how to handle such matters and not be tricked by the scheme created by attackers.

Additionally, the respondents were asked on whether they would be willing to use an application that have previously suffered a privacy or security issue. The chart in **Figure 14**, shows that 46.5% of the respondents might be willing to use such applications, 49.1% of the respondents were not willing to use such applications and the remaining 4.4% of the respondents are willing to use applications that have previously suffered a privacy or security issue. When the respondents were further asked as to why they are not willing to use them, various respondents provided similar answers. Some respondents believed that an application that has been breached or hacked is not secure enough for users to use, some have lost their trust to use a breached app and many respondents believed such application is not secure at all and prioritise over their desire to protect their data and privacy.

A similar in-depth question was also asked to respondents as to why they might give it another chance to use applications that previously had security or privacy issues, there are a number of responses received from various respondents that were similar in nature. Many respondents stated their desire to use the app once the issue had been fixed, resolved or patched while some respondents believed they will do so depending on several factors which are the availability of the app, the necessity of the app, the rating of the app and the severity of the security issue that occurred before. Several respondents also highlighted that they will only use the app if they know or were informed of the true cause of the issue, for instance a security breach that occurred might not have been caused by the developer itself but by the users of

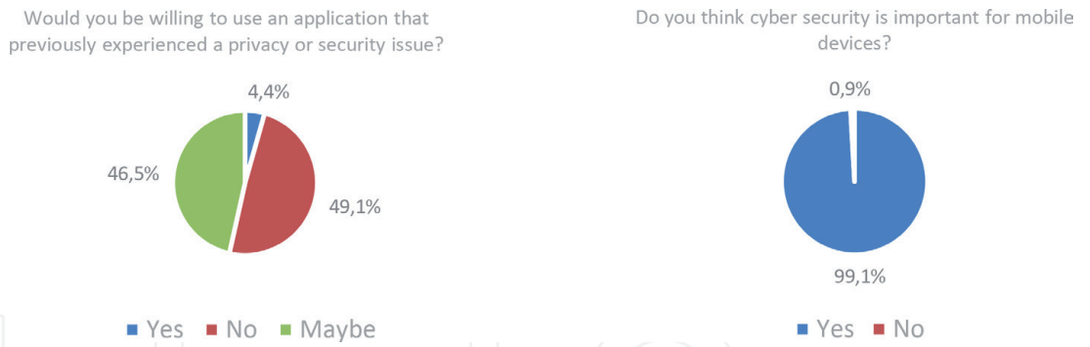

Figure 14.
Apps issues towards security.

the application itself. If it was in such instances, then these respondents are willing to use the application once more.

Lastly, when the respondents were asked on whether they think cyber security is important for mobile devices, 99.1% of the respondents agrees on the importance of cyber security for mobile devices while 0.9% of the respondents disagrees and believes that cyber security is unimportant for mobile devices. Almost all respondents believed that cyber security is important to mobile devices because the respondents believed that cyber security will protect their personal or sensitive data, their privacy as well as confidentiality that were available within their mobile device from being manipulated, misused or taken advantage of. The respondents also believed that the presence of cyber security is the most effective way to fight against cyber threat issues and reduce the number of cyber crime cases throughout the world.

5. Discussion

From the analysis of the survey results in the previous section, it can be seen that there are still mobile device users that aren't taking cyber security measures seriously and continued to stay negligent towards the dangers of cyber threats occurring to mobile devices. Number of reasons behind user's behaviour of not implementing any security measures in general such as:

- User's habit of making irrational thoughts or decisions such as clicking "I accept" without reading what they are actually agreeing to and not contemplating about the consequences of their behaviour

- User's extreme preference for convenience rather than taking the more difficult method namely security

- User's extreme priority on fulfilling user's desire rather than going for security such as downloading applications that they deem very important when there are alternatives that could be a much secure

- The financial costs of opting for security such as purchasing security software such as anti-virus is much greater than the security gains felt by the user.

- Users felt that the level of effort required to fully exercise security measures is too high such as remembering different passwords for different accounts and keeping anti-virus updated regularly.

- Users do not perceive any benefit and believes their behaviour will not affect security at all or users instead justify the cyber risk they perceived such as believing connecting themselves to an unsecure website for a short period of time is a safe action or by thinking there is no possibility of them being attacked or breached

- Users are lacking the knowledge and skills to handle any security issue such as ways and method of handling any fraudulent activities they encountered

- Users do not understand that any behaviour they have conducted will have an impact on the security risks as well as their level of vulnerability to these risks

- Users are simply forgotten to take on security measures due to various distractions encountered while surfing online

In order to increase the level of awareness amongst mobile device users, it is necessary to increase their awareness on how each of their actions and behaviour could affect the security of their mobile devices. In order to do so, a new framework which has been proposed which has been created by analysing and assessing a number of factors that influences user's cyber security behaviour.

Environmental influencers: Design factors.

It has been discovered that creating a good design or interface for a security software or application has an impact on user's willingness to use such applications. Interface design is deemed as a crucial property compared to user participation in regards to security systems in computer. The rationale behind this discovery is that a good design can effectively transmit the correct information in an orderly manner to users, thus allowing users to make an accurate and precise decision in regards to the system's state, structure as well as the security aspect of it. When this is applied to the context of mobile devices, having a good design such as good visualisations and smooth interface allows the security applications to effectively communicate its users with the necessary information useful for users to assess their current security status and risk as well as making informed decisions. Additionally, it can also promote constant interactivity with users which will then eventually result in enticing user's involvement and willingness to use such security applications.

Economic factors.

When users are determining themselves on how to behave, they will usually conduct a cost benefit analysis on the situation. One of the factors that could affect the analysis and consequently their behaviour is the presence of incentives, whether they are in the form of positive incentives such as rewards or any sort of benefits bestowed to the users or the incentives could also be negative in nature such as the cost or punishment for certain conduct or behaviour. When the economic factors of performing insecure actions are seen as acceptable to users, they would perform those risky actions such as visiting insecure websites and dismissing any security risk and credentials that could endanger both the user's mobile device as well as their sensitive information. The relationship between rewards and user's probability of behaving securely and it has been revealed that punishment, rewards as well as control assurance has an impact on user's conformity.

Personal influencers: Knowledge, skills and understanding.

It is very important for users to have the knowledge, understanding as well as the skills in order to defend themselves against fraudulent or unlwaful attacks. It is necessary for users to be equipped with the essential knowledge in order to perform and promote security measures as well as actions. Lack of user's knowledge in regards best security within the security aspect could result in a security failure. But

one of the challenges faced by users is that it is quite difficult for users to conform to best practices of protecting their mobile device because users would not know which specific type of attack or risk they will encounter, especially during these times where by the nature of cyber attacks are always changing as attackers could find many different method to perform fraudulent actions. Due to such uncertainties, users tend to rely on their individual heuristics ability or skills that enables users to make quick and efficient judgements as well as decisions within a short period of time. However, it is also noted that even though the use of heuristics is beneficial, it may lead users to create biases.

On the other hand, the availability and delivery of constant and beneficial information is required in order for users to exhibit security behaviours but it is also noted that such information might not be enough to inspire or motivate users to change their behaviours into a more security oriented in nature. Users still exhibit poor security behaviours even after attending cyber awareness training and campaigns and further added that it is not recommended to refer to user's knowledge level as a determiner of good cyber security behaviours.

Perceptions, attitudes and beliefs.

Attitude can be defined as a person's inclination to judge or assess something in a particular way. Attitude has been known to influence an individual's behaviour, whereby individuals and users each own a number of beliefs and attitudes unique to themselves that may affect their behaviour in various aspects which also include their security behaviours. But it is noted that uncomfortable tensions may occur as a result of the misalignment between attitude and behaviours and the only solution to solve it is by undergoing change to one's attitude or behaviour. Within the discussion on the matter of behaviours, it will always involve various different factors that interact together in complex ways and researchers have come up with various models to illustrate such relationships such as:

1. Rational choice based model - One of the main assumption within the rational choice model or also known as rational action model, is that it assumes that users has perfect information. What is meant by perfect information here is that users are assumed to acquire all information regarding every possible choices or alternatives and then users will act on it by behaving in a manner that will provide them with the best outcome out of all possible choices. But an individual's act of processing the obtained information does not necessarily lead to the generation of a rational behaviour and consequently, individuals does not necessarily perform a rational choice in order to achieve the optimum result. Hence, according to this model, it can be said that every mobile device users are already equipped with the cognitive ability and motivation required to make rational decisions when faced with security incidents such as the act of applying facts in assessing cyber incidents. However, it is also noted that there is a challenge in doing so primarily due to the uncertainties of outcome or end results when dealing with anything related to cyber security.

2. Theory and model of planned behaviour - The main motive behind the use of the planned behaviour model amongst researchers is to analyse and describe the behaviours exhibited by individuals that are equipped with the ability to exercise self-control. One of the assumption that has been created within this model is that it assumes that any behaviour is planned and any individuals that plans to act or behave in a certain way will actually commit to it and behave in the way they have initially planned. A fundamental element within the planned behaviour model is behavioural intent, where the intention to behave in a certain way is subject to the attitude towards the expected outcome

of the desired behaviour as well as the evaluation of cost and benefit produce by the behaviour. Thus, according to this model, it can be said that when users believes that by behaving securely and employing security measures to their mobile devices will produce positive outcome to themselves, the users will effectively perform the security behaviour that they had planned in their minds.

3. Protection motivation model - The protection motivation model was created with an intention to aid individuals in resolving and coping with their fear appeals and this model believes that the behaviour of individuals are influenced by two appraisals namely the threat appraisal and the coping appraisal. The threat appraisal refers to user's perception on the gravity of an incident and user's perception on the likelihood of an incident or vulnerability while the coping appraisal refers to user's efficacy of the suggested precautionary behaviour as well as user's perception of their own efficacy (self-efficacy).

4. Learning model - One of the assumptions made within the learning model is that it assumes that behaviour is a process that individuals need to learn and that the learning process is influenced by two different elements which are incentives in the form of punishment or rewards and the social environment surrounding the individual which includes role models.

5. Change models - Change models are known to be built by the assumption that changes in behaviour is a step-by-step process that involves many stages and it does not ever occur in a single step or occasion. Researchers have constructed various change models and some of the most frequently models that have been implemented includes Lewin's 3-stage model of change management and Kotter's 8-step theory of change management.

Social influencers: Social norms at home, workplace and lifestyle.

It is in human nature that every person are bound to be influenced by the people that surrounds them regularly which includes family members, friends, top managers, work colleagues or other various entities that could be labelled as a role model to the particular individual. In other words, the behaviour, norms or beliefs of another person could heavily influence user's behaviour towards SMD security. In the context of organisational workplace, one of the main predictors of employee's behaviour towards the implementation of security policies is how employees perceived the expectation set by the managers on complying with the security measures or policies. The main reason of employees ignoring the instruction of the organisation to employ security practices and measures such as encrypting their email messages is primarily due to employee's not seeing the practices being exercised by fellow peers and managers. Thus, within the context of mobile device security, it is highlighted that user's chances of exhibiting security behaviours are increased exponentially when the entities or role models surrounding the user is exhibiting similar security practices or behaviours. When users feel that they are doing an activity that is similar to their role models or the neighbouring people, it could result in a sort of connection or "aligned" interest that could significantly promote the users of SMD to conduct a set of security behaviour [4, 26].

Generation-Z perception towards SMD Information Security.

It is a widely known fact that generation Z are regarded as the generation of youths that does not remember any strand of moments or memories without the usage of smart mobile devices, and they are considered as the top targets of attackers due to their constant usage of mobile devices. This is where the youth's awareness on cyber threats as well as the best practice of security behaviour on SMD

comes into the bigger picture. The generation Z was observed to express concerns on the security of their mobile devices where within the research, it was discovered that about 40% of the Generation Z youths expressed their desire to be able to know the person they are communicating with when making online shopping or retail through authentication so that they are able to trust the person they are interacting with. It further added that generation Z are also concerned on various aspects of security such as the likelihood of their mobile device being hacked and the risk associated with cyber crimes which includes fraud and identity theft.

Even though it seemed that the Generation Z are actively concerned about security issues, there were also evidence from other research which states that the Gen-Z are overconfident in their ability to tackle security issues. In other hand, the Gen-Z assumed to themselves that they are very cyber secure but in reality, it was the vice versa. It was proven so from the survey conducted by the researcher where in one of the questions, the researcher discovered that the 96% of the Gen-Z youths believes that they are able to keep their personal or sensitive online data save but in another question, it was revealed that the 32% of the Gen-Z respondents have not put in little to no effort in creating their passwords. Within another question, it was also revealed that 78% of Gen-Z youths agreed that they had created and used the same passwords for various personal accounts. It is also revealed in recent studies that most of the Gen-Z youths are more open or encouraged to the idea of balancing between their desirability for a greater personalised experience and their concerns on security/privacy issues. However, generation Z are 25% more prone opt for a digital world compared to generation X and boomers, where in that digital world applications and websites have the ability to forecast and deliver what the user requires at any period of time. Here, the Gen-Z youths which accounts to 45% of total Gen-Z respondents were willing to give out their data in order to experience a more personalised environment at the cost of their privacy. The Gen-Z youths founds a website in which the website fails to predict the items they wanted, about 50% of the Gen-Z respondents will halt their activity on that website and stop visiting it.

In conclusion, it can be seen that despite the concerns for cyber security, some of the youths are behaving overconfidently towards their ability to protect themselves from cyber incidents while some behavioural patterns seen in youths presently are their willingness to trade their privacy just for some personalised environment or experience. One way to solve these behavioural problems is by creating or promoting security awareness on their behaviour. There could be different ways to solve them, thus this indicates that there is more work and research to be done on the topic of SMD information security and its relationship with the main users of mobile device, the Generation Z.

Effect of security awareness to customer trust.

Various researches had been established and conducted that was looking into the relationship between awareness of security and customer trust. There are possibility of risk associated with their transaction such as trust as well as privacy risk when a vendor or an organisation requested users to provide information that are considered irrelevant for the transaction such as asking questions on the user's age or gender. Trust amongst public towards organisations or corporations had been deteriorating for the past few years and one of the main rationale behind the drop of public trust is due to the advancement of cyber crime and cyber criminals, especially within this technologically advanced era.

Their study further revealed that there is a strong relationship between cyber security and user's assurance or trust towards an organisation. In the study, 53% of the respondents revealed that their perception of an organisation as a brand that can be trusted were based on the strict and meticulous security measures they had

to undergo during the sign in process, and also, 49% of the respondents revealed that their experience of never encountering any security issues acted as an indicator for choosing which organisation to trust. Furthermore, 47% of the users within the study revealed to have stayed with their chosen organisations in which they assume to be more secure that other organisations.

6. Conclusion

In summary, with the increase in SMD usage contributed by the Generation Z youths, it is expected that more cyber attacks or incidents such as malware will be aimed towards the mobile device users. The study is aimed at measuring the level of smart mobile device security and privacy awareness. Firstly, a survey questionnaire was conducted in order to measure the level of awareness of SMD security amongst Generation Z youths.

The major findings of the survey showed that on average 43% of the users rarely changed their network and mobile screen password. It is also found out that over 56.1% users have never read the EULA policy before installing any applications and about 43.8% users always stay logged in after using their personal accounts. Additionally, more than 50% of users have stored sensitive data within their mobile device but 61.4% users have not installed any security software or applications to their mobile device, thus making their sensitive data vulnerable to cyber attacks.

Secondly, a new framework have been proposed in order to increase the awareness level of mobile device users which is based on the security behaviours exhibited by SMD users. Within the framework, it is highlighted that in order to increase the level of SMD security and privacy awareness, users need increase their level of awareness on security behaviours by understanding the importance and rationale behind various cyber security behaviours.

Author details

Heru Susanto[1,2,3]

1 School of Business, Universiti Teknologi Brunei, Brunei

2 Research Centre for Informatics, the Indonesia Institute of Sciences, Indonesia

3 Information Management, Tunghai University, Taiwan

*Address all correspondence to: heru.susanto@utb.edu.bn; heru.susanto@lipi.go.id

References

[1] Choo, Kim-Kwang Raymond. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. Computers & Security. 30. 719-731. 10.1016/j.cose.2011.08.004.

[2] McAfee Mobile Threat Report. (2019). Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

[3] Park, D. H. Kim, M. S. Kim and N. Park, (2013). "A Study on Trend and Detection Technology for Cyber Threats in Mobile Environment," 2013 International Conference on IT Convergence and Security (ICITCS), Macao, 2013, pp. 1-4.

[4] Sheila, M. & Abdollah, Mohd & Sahib, Shahrin. (2015). Dimension of mobile security model: Mobile user security threats and awareness. International Journal of Mobile Learning and Organisation. 9. 10.1504/IJMLO.2015.069718

[5] Susanto, H., Almunawar, M. N., Leu, F. Y., & Chen, C. K. (2016). Android vs iOS or Others? SMD-OS Security Issues: Generation Y Perception. International Journal of Technology Diffusion (IJTD), *7*(2), 1-18.

[6] Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Government Office for Science.

[7] S. Vashisht, S. Gupta, D. Singh and A. Mudgal, "Emerging threats in mobile communication system," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 41-44.

[8] Thiruvaazhi, U. & Arthi, R.. (2019). Threats to mobile security and privacy. International Journal of Recent Technology and Engineering. 7. 407-412.

[9] Androulidakis, I., & Kandus, G. (2011). Mobile Phone Security Awareness and Practices of Students in Budapest.

[10] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). "Information Security Policy Complaince: An Empirical Study of Rationality-Based Beleifs and Information Security Awareness," MIS Quartely (34:3), pp. 523-548

[11] Puhakainen, P. (2006). A Design Theory for Information Security Awareness. Unpublished doctoral dissertation, University of Oulu, Oulu, Finland.

[12] Susanto, H., & Almunawar, M. N. (2018). *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard*. CRC Press.

[13] Susanto, H., & Almunawar, M. N. (2015). Managing Compliance with an Information Security Management Standard. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1452-1463). IGI Global.

[14] Susanto, H., Yie, L. F., Setiana, D., Asih, Y., Yoganingrum, A., Riyanto, S., & Saputra, F. A. (2020). Digital Ecosystem Security Issues for Organizations and Governments: Digital Ethics and Privacy. In *Web 2.0 and Cloud Technologies for Implementing Connected Government* (pp. 204-228). IGI Global.

[15] Thomson. M.E, and Von Solms, R. (1998) Information security awareness: educating your users effectively, Information Management & Computer Security, Vol. 6 (4), pp.167-173

[16] Leu, F. Y., Ko, C. Y., Lin, Y. C., Susanto, H., & Yu, H. C. (2017). Fall Detection and Motion Classification by Using Decision Tree on Mobile Phone. In *Smart Sensors Networks* (pp. 205-237).

[17] Souppaya, Murugiah, Scarfone, Karen. (2013). NIST Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise. 10.6028/NIST.SP.800-124r1.

[18] Susanto, H., & Almunawar, M. N. (2016). Security and Privacy Issues in Cloud-Based E-Government. In *Cloud Computing Technologies for Connected Government* (pp. 292-321). IGI Global.

[19] Leu, F. Y., Susanto, H., Tsai, K. L., & Ko, C. Y. (2020). A channel assignment scheme for MIMO on concentric-hexagon-based multi-channel wireless networks. International Journal of Ad Hoc and Ubiquitous Computing, *35*(4), 205-221

[20] Leu, F. Y., Chiang, P. J., Susanto, H., Hung, R. T., & Huang, H. L. (2020). Mobile Physiological Sensor Cloud System for Long-term Care. Internet of Things, 100209.

[21] O'Dea, S. (2020, February 28). Forecast number of mobile users worldwide 2019-2023. Retrieved from https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

[22] Susanto, H., Yie, L. F., Rosiyadi, D., Basuki, A. I., & Setiana, D. Data Security for Connected Governments and Organisations: Managing Automation and Artificial Intelligence. In *Web 2.0 and Cloud Technologies for Implementing Connected Government* (pp. 229-251). IGI Global.

[23] Susanto, H., Leu, F. Y., Caesarendra, W., Ibrahim, F., Haghi, P. K., Khusni, U., & Glowacz, A. (2020). Managing Cloud Intelligent Systems over Digital Ecosystems: Revealing Emerging App Technology in the Time of the COVID19 Pandemic. Applied System Innovation, *3*(3), 37.

[24] Susanto, H. (2018). Smart mobile device emerging Technologies: an enabler to Health Monitoring system. In *High-Performance Materials and Engineered Chemistry* (pp. 241-264). Apple Academic Press.

[25] Yie, L. F., Susanto, H., & Setiana, D. (2020). Collaborating Decision Support and Business Intelligence to Enable Government Digital Connectivity. In *Web 2.0 and Cloud Technologies for Implementing Connected Government* (pp. 95-112). IGI Global.

[26] Susanto, H., Ibrahim, F., Nazmudeen, S. H., Mohiddin, F., & Setiana, D. (2020). Human-Centered Design to Enhance the Usability, Human Factors, and User Experience Within Digital Destructive Ecosystems. In *Global Challenges and Strategic Disruptors in Asian Businesses and Economies* (pp. 76-94). IGI Global