International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey on Mobile and Wireless Security Awareness: User Perspectives

Nadhirah binti Nazri[1], Noor Azian binti Mohamad Ali [2], Jamaludin Ibrahim [3]

Department of Information System, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia

Abstract: ***The use of wireless and mobile devices especially smartphones has become the norm nowadays. The emerging and advancement of wireless and mobile devices has brought the issue of security breaches and attacks back into focus. Many users are not aware of the security issues related to wireless and mobile devices. This has resulted in devices becoming attractive targets for malicious attack. In this paper, we discuss and analyze the factors of attack on mobile and wireless platforms and give in-depth overview of the attack mechanism. It is hoped that users will become aware and alert about the security issues and subsequently take the necessary action and precaution to protect themselves.***

Keywords: Mobile devices, wireless technologies, behavior, awareness, attacks, threats

1. Introduction

Beginning with a humble wired environment where we see cables all around, the world is evolving rapidly that with new innovative technology. Now there are almost no more hanging cables but yet data can be transmitted better and faster: this is the era of wireless technology. Demand for mobile technology is growing tremendously at an enormous rate. Corporations are deploying mobile applications that provide substantial business benefits, and consumers are readily adapting mobile data applications which are downloadable at their fingertips just in seconds. More and more exciting new mobile devices and gadgets are constantly entering the market, supported by the wireless technology which provides data access almost anywhere and anytime.

One of the major and crucial concerns in implementing mobile and wireless solutions is security of data. It is already difficult to protect enterprise data in a wired environment, adding wireless transmission and mobile storage makes the task even more challenging [9]. Information has been valuable since the dawn of mankind. The area of Information Security (IS) is designed to protect the confidentiality, integrity, and availability from those with malicious intentions.

The mobile devices are starting to function similar to PCs, both in their capabilities and the way people use them. The various mobile platforms such as Android, iOS and Symbian are becoming more similar towards PC operating systems. As a result, the standard malicious attacks for PCs, such as worms and Trojans, as well as attack vectors, like the Internet access, are becoming applicable to the mobile platforms [6].

In a recently incident, an anonymous group spread a banking malware that targets internet banking user. The so-called "God" of Malware namely ZeuS Tracker or Trojan which is now active and could be a significant threat to users who perform online banking through mobile phones. ZeuS malware incorporated mobile elements and it functions to intercept SMS banking authentication codes.

In order to do the most damage, malware has to become more intelligent. It stays stealth in phones and gadgets without the user noticing it. With the improvement in technology, mobile processing power becomes more powerful, thus it is quite difficult for users to realize the presence of malware in our phones. Some might say, "Why bother about malware? As long my phone runs smoothly and gives me no harm then it should be alright." But in reality, once attacked the impact can be disastrous and beyond comprehension.

A recent survey [5] published in April 2011, which was done in Budapest focused on mobile phone security awareness. It was found that the majority of the respondents were concerned about security issues. However, there is no culture of security and no advanced technical knowledge of their mobile phones.

Another study presented an exploratory and descriptive examination of users' smartphone security awareness conducted in South Africa. This study shows that users are complacent in their smartphone security behaviors, displaying high levels of trust towards smartphone app repositories. Users rarely consider privacy and security when installing new applications and also do not adequately protect themselves by adopting smartphone protection mechanisms (controls) [1].

This leads to the same hypothesis which is human behavior factors greatly influencing the information security system. The role of the human is really significant in information security systems. Information security vulnerability could be caused by human, either intentionally or unintentionally [2]. Whatever the technology, it is still up to the human to use it to benefit or harm others.

2. Objective

The main purpose of this paper is to measure awareness among mobile and wireless users on information security. The world has faced various cases of security breaches and attacks recently. Unfortunately to our dismay, nobody really pay attention about it. Viega (2009) said in his book, The

Myths of Security, these days, the world rarely hear about the security issues. It is neither due to lack of security issues nor the threats has minimized, but the presses do not bother to report it because people do not care anymore. On the contrary, the less the press reports, the less people care, thus, creating a nice downward spiral into ignorance [12]. Viega (2009) said, there are plenty of other factors keeping people from caring about the security issues, which include [12]:

1. Malware likes to stay hidden
One of the core characteristic of malware is that it operates without being obvious. If the infection was obvious and the user paid to get the thing cleaned, they were not going to make as much money off a user. Therefore, instead of thousands of pop up ads appear on our screen, malware makes it easy and does not overwhelm us with them. As a result, we do not notice many infections, so our perception is that our security software is doing its job very well.

2. Security products are not top of mind
We may never see the security product for example the Antivirus software working and will not give it any credit as long as the product is working well. We fail to recognize the importance of such security software to help protect our information. In our eyes, whether it is there or not makes no difference.

3. The consequences have not been too bad
In the event where people got their bank accounts drained and their identities stolen, some still consider it as a small issue. It is just an Internet disaster which occurs once in a blue moon. For that period of time, some may be afraid of doing transactions online, but after some time, we will get back to doing e-commerce on the Net. Even if our credit card is stolen, we are somewhat consoled because credit card companies will absorb the risk. So there is nothing much to worry, is it?

4. The story is boring
Despite the number of attacks have been launched and the same issues may be recurrent and reported in newspaper headlines, we feel that the same incident occurs to someone else. We may then arrive to a point where it becomes just another one more attack. Eventually we may stop reading the headlines and so reporters do not feel the importance to report similar attacks and stories again.

5. The security industry is not too credible
Having antivirus software solutions, be it in your PCs or mobile devices, may sometime not work or slow down your devices to a walking crawl. So why trouble ourselves with such solution? Furthermore, we may think that the antivirus company is the one that produces virus and they are the one that create magical cure for the virus, so that they have something to detect. True enough is not it?

3. Methodology

A very useful evaluation method for surveying users' practices is the use of questionnaire. We chose random sampling as our methods of data collection. The target group of the survey was mobile and wireless users. Our survey was conducted using a set of questionnaire with a total of 116 respondents participated. The respondents were selected based on their awareness against the current security issues involving mobile and wireless. The online survey was distributed to the user via social network (e.g: Facebook) and online messenger (e.g: WhatsApp). The analysis started from collecting, organizing and interpreting the data using the Google sheet. The data responses of the surveys were automatically collected and real-time response info and charts were available directly from the forms.

4. Survey and Discussion

All the findings presented in this paper are based on aggregated data, totaling 116 randomly sampled users.

4.1 Mobile and Wireless User

In term of the use of mobile devices, we assume that almost all users owned at least one device. To strengthen this assumption, the survey included a question to know what type of mobile devices users prefer. The survey result shows that 100% of the respondents own a mobile device. As shown in Figure 1, of all the devices, smartphones are the most significant and favourite mobile device chosen. This proved our assumption all of the respondents have their own mobile devices.

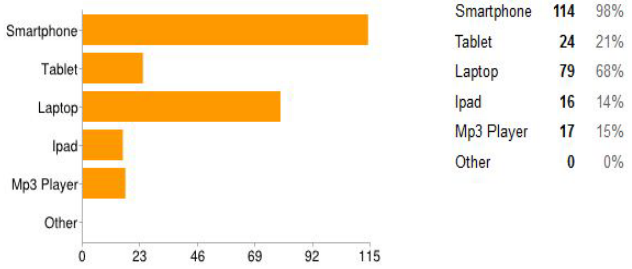

Figure 1: Type of mobile devices owned by the users

Among these users, we assume that half of the user has the experience connecting to the internet. To prove this hypothesis, they were asked whether they frequently connected to the Internet or not and how they are connected. The survey result in Table 1 shows that 99% of the users frequently connected to the Internet and majority of 82% users connected to the Internet via mobile data package.

Table 1: Type of Internet Connection

Type of Internet Connection	*Percentage*
Mobile Data	82%
Home Wi-Fi	64%
Public Wi-Fi	35%
Broadband	16%
Cable	3%
Other	2%
Dial-up	0%

4.2 Security Issue

In this section we will explain and analyze the users' practices regarding the information security of mobile and wireless technology. A set of questions were asked to study the common practice of password security, application security, email security, personal security, and security

product usage.

4.2.1 Password Security

In order to ascertain a concrete understanding of individuals' normal practice towards securing mobile devices, we came up with the question whether they implement any password in their mobile device screen. Survey reveals that 51% of the respondents use password on their mobile device screen. That leaves the remaining 49% of the users without a screen saver password which in turn put their phones vulnerable to threats and can be manipulated by "irresponsible" hands easily.

However, touch screens are the current common feature on mobile devices especially the smartphones and tablets. It is now common for mobile devices to have touch screen input and the password pattern is one graphical password where a user traverses an onscreen 3x3 grid of contacts points. Touch screens are touched, so oily residues, or smudges, remain on the screen as a side effect. By inspection of the smudges, an attacker can extract sensitive information about recent user input, specifically attacks against the password pattern as illustrated in figure 2 [11]. Then again, even if the attacker has the physical access to the mobile devices, he needs time to figure out and trace the smudge on the screen, in order to discover the password pattern. Therefore in a nut shell, having the password-protected screen on mobile devices is far better than not having one. The password screen lock alone is not sufficient to protect the data against sophisticated attackers though. However, it might be good enough in practice for most users and mitigate the risk at the very first level.

Figure 2: the smudging effects that enable an attacker to launch a smudge attack

Following that, we move on to user's perspective regarding security of the network. The respondents were asked whether they often change their network password or not. We assume that, half of the users do not bother to change their network password. This is further proven where a significant number of the respondents (89%) rarely change their network password. Without security measures and controls in place, users' data particularly in mobile devices might be subjected to an attack. The network and data are vulnerable to any type of network attack such as eavesdropping, man-in-the-middle attack, and sniffer attack if the users do not have a security plan in place like changing the network password on a regular basis [4]. According to several studies, Ciampa M. (2010) highlighted that passwords have become a prime attack target due to the following reasons which include; users do not use a unique password, users do not want to be forced to change their passwords, users either use the same password for different applications or write down the password, and users do not change password regularly [14]. These conclude that, it is due to the ignorance and unawareness behavior to implement and secure password that influence the attacker to target the users.

4.2.2 Application Security

Due to the increase of mobile applications in the market such as PlayStore and AppStore and being very easy to download, a question had been asked to understand the users' behavior when they downloaded and installed the mobile applications. They were asked whether or not they usually read the End-User License Agreement (EULA) before installing the applications. It is interesting to note that according to a research [13], almost a quarter of the tested applications are built with logging and storing sensitive data on the device that can be readable by other non-privileged applications on the device. They found that applications on mobile devices are just as prone to security vulnerabilities as their web counterparts.

The pie chart in Figure 3 shows that, 71% of the respondents do not read the End-User License Agreement before installing an application in their mobile devices. This is certainly a bad practice as their mobile devices are now vulnerable and exposed to threats. Users are unaware of the potential malicious action these applications might do. There was a case where a Trojan called TSPY_DROIDSNAKE can infect a phone via HTTP POST, immediately after the user accepts the application's end-user license agreement (EULA). This Trojan masquerading as a game Tap Snake can transmit the GPS location of the infected phone. A renowned threats analyst, Mark Balanza, advises users to first check out what kind of permission an application asks for before installing it. This is a mitigation action to reduce the risk of a Trojan like attack [8].

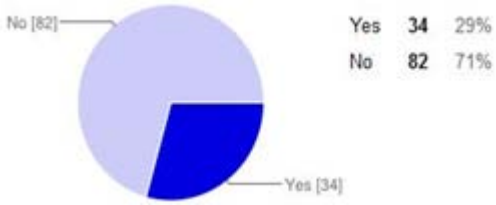

Figure 3: Number of user usually read End-User License Agreement (EULA) before installing an application.

4.2.3 Email security

Our survey then continue with a question asked on how careful and aware the users are when they open attachments or link via email, SMS, MMS, messengers and etc. The majority of them (78%) said that they always make sure the attachment is from the person they know, whereas the other 15% of the users just open it no matter who the sender is and another 7% just ignore the attachment. From the survey, noticed that 85% (78% + 7%) of the respondents have actually shown a good practice by taking appropriate pre-emptive measures as to avoid malicious attacks by means of the attachments in their emails. This good behavior will indirectly help to stop virus from spreading and widening its harmful strength to other email users.

Nevertheless, the attack on the email not only spread via anonymous email address but it can also distribute from someone that we know. Email distributed virus will infect and replicate themselves in an email message and sending themselves to all contacts in email address book. The unsuspecting recipients seeing that an email and attachment arrived from a "friend" typically open the attachment and get infected. In 2001, a malicious computer virus, SirCam, uses email to spread across the Internet rapidly. It searched through the emails, user files and email address books to find new email addresses to email itself to in order to replicate [7]. Table 2 shows the average rate of emails with infected attachments as reported by the security firm Sophos [14].

Table 2: Average rate of emails with infected attachments

Year	*Average number of infected attachments*
2005	1 in 44
2006	1 in 337
2007	1 in 909
2008	1 in 714

4.2.4 Personal Security

These days, almost all mobile device users tend to keep sensitive personal data into their mobile devices for example like photos, videos, important documents, discussion recordings and etc. To prove this hypothesis, we came up with a question "Do you keep sensitive personal data into your mobile devices?" The result of the survey shows that 73% of the respondents tend to keep their sensitive information in their mobile devices. When we look at the security aspect of it, basically it is neither wrong yet nor advisable to store such kind of information in mobile devices. Considering the threat that might occur when the mobile devices have been compromised by an attacker, adequate protection should be given to the mobile devices in advance if we still want to keep sensitive information in there. Additionally, it seems that we consider our mobile phone to be a very personal device and we save equally important and sensitive information there [5]. Again it is quite true for most of us but just to bear in mind that we are responsible to ensure as maximum defense as possible to the mobile devices and the sensitive information.

4.2.5 Security Product Usage

Due to the increasing cases of security threat and attack, users were given a few questions regarding security products. The main objective of the questions asked is to understand the common practices and behavior toward the security products.

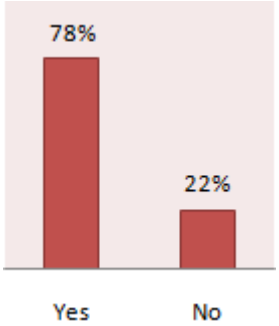

Figure 4: Is there any security product (e.g: anti-virus) currently installed, update and enable on your devices?

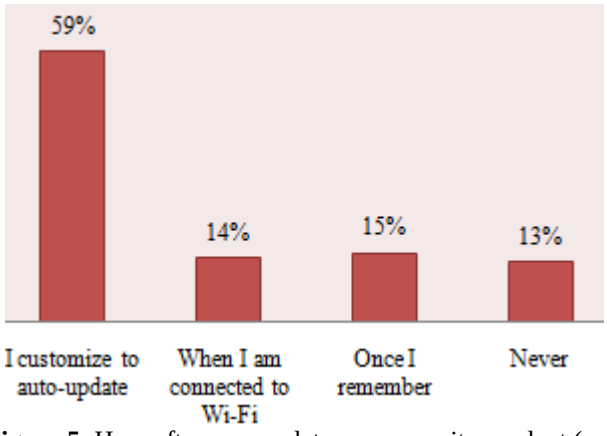

Figure 5: How often you update your security product (e.g: anti-virus)?

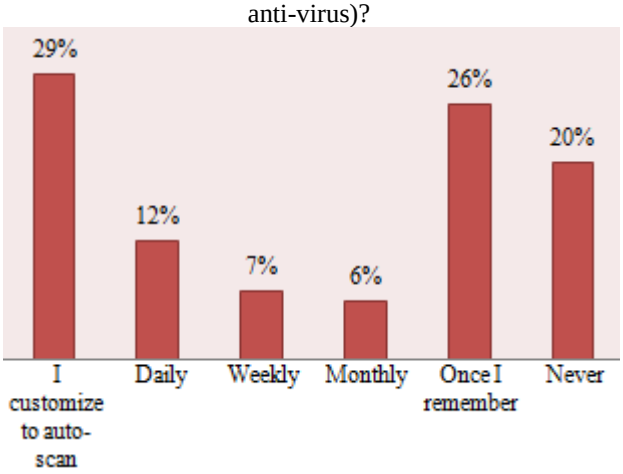

Figure 6: How often you scan your mobile devices?

From the study, we notice that majority of the users feel that privacy and mobile security are important to them. Out of the total respondents (Figure 4), 78% of them currently install, update and enable security product on their devices whereas only a small group of 22% users does not equip their mobile devices with any security product. This shows that the users do care about the privacy and security issues of their devices.

However, according to John Viega (2009), nearly all users think that security products are not important and not the main concern, hence the ignorance leads them to merely put the software to run own its schedule automatically without having to think about it. Users fail to recognize the importance of such security software to help protect their information. For several people as long as the product is working well, proactively stopping bad stuff from executing on their devices it is good enough [12]. This is confirmed when the majority, 59% of the respondents only rely on auto-update customization when updating the security product (Figure 5) and 29% users have confidence in using auto-scan customization to scan their mobile devices (Figure 6). In addition, those users who update the security product and scan their mobile devices "only when they come to remember" clearly describe their unawareness towards information security.

4.3 Human Behaviors and Knowledge

In this section we will discuss and review some of the survey results relating to human behaviors and knowledge in the security perspective. A few questions were asked to

measure level of concern and awareness of information security knowledge. The first question asked is whether the users are aware of current privacy and security issues with mobile and wireless devices. It is true to say that these days the world rarely hears about the security issues and threats although in reality the threats are exponentially increasing tremendously with the evolution in technology. This is neither due to the threat have really minimize nor the issues are very common that people feel uninterested and so the press feel discourage to report on it. This has in turn reflected to our survey where 42% of the respondents are unaware of the current security breach and attack on mobile and wireless device. While 29% of them are not sure of the attack, we feel quite relieved that the other 28% is attentive to the issue.

Moreover, the other reason that may contribute to ignorance of the security issues is due to inadequate amount of information and knowledge regarding information security. This is very well proven when the second question is asked to the users whether they have ever learnt about information security. As expected, the result of the survey shows that 56% of the respondents acknowledged that they have never learnt stuff on information security (Figure 6). This worrying phenomenon may lead to unprepared situation where users are unable to handle and mitigate security issue when it happens, hence are exposing their wireless and mobile devices to threats and malicious attacks.

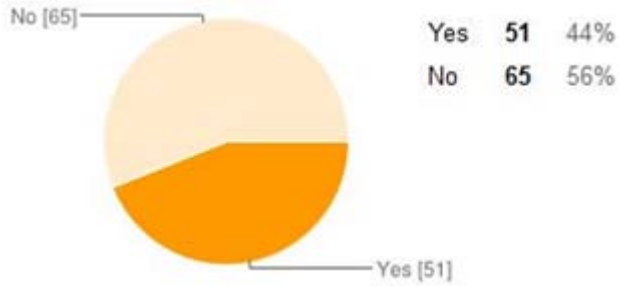

Figure 6: Knowledge on Information Security.

Notwithstanding the above, it is hard to detect whether a mobile device has been compromised. Even a well verse person in information security says the same. Here the third question is asked whether the users know how to tell if their mobile device is hacked or infected. Through the survey, it reveals that 71% of the respondents do not know and do not realized if their mobile devices are infected or hacked by attackers. It is a common scenario due to the reason that the virus or worms will stay stealth and hidden inside the devices that make the existence 'unseen'. This is proven when Viega (2009) said that one of the factors keeping people from caring about security issues was "malware likes to stay hidden" [12]. As a result, users do not notice that their devices have been compromised.

Table 3: Users' consent of security breach or attack.

Make report or not?	*Percentage*
Yes	34%
No	13%
I'm not sure	19%
I do not know to whom I should report	34%

Closing our survey, we present here the issue of whether the users would report a security breach or attack on the Internet when it occurs. The result (Table 3) of the survey illustrates two groups of respondents having the same weight age of 34%. The first group exclaims that they will report a security breach whereas the other group expresses that they do not know to whom they should report to. This is in fact not a good sign for the second group. It denotes that they have no exposure concerning security-related body or organization where they can lodge a report or sit down and share issues on security with the authorized body prior to appropriate action and measures are taken. Conversely, 13% of the respondents do not care at all to report a breach in security over the Internet. This is perhaps due to ignorance and a thought of not worth worrying about it as long the attack or breach does not fall on their shoulders or they feel that the impacts have not been too bad.

For some reason, users assume that hackers do not target them because their devices have no value for the hackers to attack. 44% of the respondents think that their devices are not worth to be hacked. A common misconception many people have is that they are not a target for cybercrime. They think that their devices do not have any value. As a result, they do not take the necessary actions to protect their information. In reality, people may not realize it, but their devices and their information have tremendous value to cyber criminals around the world. Every day, their devices are being attacked without their consent [15]. Due to this behavior, unaware users are the greatest weaknesses themselves and unconsciously become the primary target.

5. Proposed Solution

There is an increase in information security incident globally, mainly because of the increase in electronic data, mobile devices, increase of organized cybercrime groups, difficulty of tracing the attackers and lack of adequate information security knowledge among users [3].

Various cases of security breaches and attacks of malware have been reported over the last year. High level cases of cyber attacks have been documented in history, which include security threats conducted by malicious hacking groups like the LulzSec that attacked Sony Pictures where they took data that includes names, passwords, emails addresses, home addresses and date of birth for thousands of people [3]. Meanwhile in China, about 85 percent of all computers were infected with a computer virus during the year 2003 [7].

Recent studies have shown that the most common factor contributing to these breaches is the human behavior towards security. The lack of user awareness and knowledge on Information Security are the main factor. Some of the measures suggested to change the user behavior include:

- Training and education: Training used for raising awareness of the users especially among employees. From the studies above has shown that more than half of the user did not learn about Information Security. This training aims at facilitating a more in-depth level of users/employees information security understanding
- Awareness-raising campaign program: Supply information on topical issues and examples of breaches and attacks to users through pamphlet, advertisement like

advertising through TV commercial, Internet and newspaper. These media contain all the information about information security required by users. The awareness campaign aims to raise the collective knowledge of information security and its controls.

- Web site home page: Provides an introduction to information security and the motivation to users towards securing information security and mobile devices. The users need to be motivated as to why information security is important as important as their bank information [10].

6. Conclusion

In summary, with the increasing volume of mobile devices over the last decade, the rise of mobile malware seems inevitable. Where there is a popular platform, malware will breed there too. There are various factors affecting information security; regardless the information is transmitted through wired or wireless devices. One of the main factor is human itself such as user awareness and carelessness. The lack of user awareness and knowledge on security not only affects one user but also all users in the network. Users and awareness factors are considered the most important means of enhancing and improving information security. On the other hand, lack of isolation in mobile system platform could severely compromise the mobile device and malicious application would easily gain access to critical systems and private data.

References

[1] Ophoff, J., Robinson, M., "Exploring End-user Smartphone Security Awareness within a South African Context," Journal of Information Security for South Africa (ISSA), pp. 1-7, 2014.
[2] Malahat Pouransafara., Nurazean Maroop., Zuraini Ismail., Maral Cheperli, "Review of Information Security Vulnerability: Human Perspective," Journal of the Second International Conference on Informatics Engineering & Information Science (ICIEIS2013), pp. 119-126, 2013.
[3] Basamh, S. S., Qudaih, H. A., Ibrahim, J., "An overview on cyber security awareness in Muslim Countries," Journal of International Journal of Information and Communication Technology Research, 4 (1), pp. 21-24, 2014.
[4] "Common Types of Network Attacks." [Online]. Available: http://technet.microsoft.com/en-us/library/cc959354.aspx. [Accessed: December 18, 2014].
[5] Iosif Androulidakis., Gorazd Kandus, "Mobile Phone Security Awareness and Practices of Students in Budapest," Journal of the Sixth International Conference on Digital Telecommunications, pp. 18-24, 2011.
[6] Delac, G., Silic, M., Krolo, J., "Emerging Security Threats For Mobile Platforms," Journal of MIPRO, 2011 Proceedings of the 34th International Convention, 2011.
[7] Erbschloe, M., Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code, Amsterdam: Elsevier Butterworth Heinemann, 2005.
[8] "Malicious Android App Spies on User?s Location | Malware Blog | Trend Micro," August 17, 2010. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-android-app-spies-on-users-location/. [Accessed: November 2, 2014].
[9] Mallick, M., "Mobile and Wireless Design Essentials," Indianapolis, IN: Wiley, 2003.
[10] Gundu, T., & Flowerday, S. V., "Ignorance to Awareness: Towards an Information Security Awareness Process," South African Institute OF Electrical Enginers, 104(2), pp. 69-79, 2013.
[11] Adam J. Aviv., Katherine Gibson., Evan Mossop., Matt Blaze., Jonathan M. Smith, "Smudge Attacks on Smartphone Touch Screens," Journal of WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies, pp. 1-7, 2010.
[12] Viega, J., The Myths of Security: What The Computer Security Industry Doesn't Want You To Know, Beijing: O'Reilly, 2009.
[13] Hewlett-Packard Development Company, "HP whitepaper: Know the Big Three," 2012, November 26.
[14] Ciampa, M. D., Security Awareness: Applying Practical Security in Your World (3rd Ed.). Boston, MA: Course Technology/Cengage Learning, 2010.
[15] The SANS Institute, "Yes, You Actually Are A Target," April, 2014. [Online] Available: www.securingthehuman.org/ouch. [Accessed: Jan, 5, 2015]

Author Profile

Nadhirah binti Nazri, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia.

Noor Azian Mohamad Ali, Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communications Technology, International Islamic University Malaysia.

Jamaludin Ibrahim, Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communications Technology, International Islamic University Malaysia.