SECURITY AND PRIVACY OF SINGLE-SIGN-ON (SSO) IN MOBILE ENVIRONMENT: STUDENTS' EXPERIENCES AND PERCEPTIONS (LEADS RESEARCH GRANT: S/O 12397)

NORLIZA BINTI KATUK
HATIM BIN MOHAMAD TAHIR

UNIVERSITI UTARA MALAYSIA
2014

DISCLAIMER

We are responsible of the accuracy of all opinion, technical comment, factual report, data, figure, illustration, and photographs in this report. We bear full responsibility for the checking whether material submitted is subjected to copyright or ownership right. UUM does not accept any liability for the accuracy of such comment, report, and other technical and factual information and the copyright or ownership right claims.

CHIEF RESEARCHER:

_____

NORLIZA KATUK

MEMBER:

_____

HATIM MOHAMAD TAHIR

DATE: 1 JUNE 2014

ACKNOWLEDGEMENT

The authors wish to express their gratitude to Universiti Utara Malaysia (UUM) for the financial support under the LEADS grant. Appreciation also goes to Mr. Mohamad Subri bin Halim, a graduate research student who performed data collection for this research.

The authors also acknowledge the support given by Mr. Amran bin Ahmad and Madam Sharmila binti Mat Yusof in recruiting participants for this research, as well as the students of UUM who had participated in this study.

Last but not least, thank you to those you had given their constructive comments and suggestion throughout the process of completing this research.

ABSTRACT

The number of password-protected Internet-based applications is increasing significantly compared to a decade ago. Many Internet applications require users to subscribe to their services and authenticate themselves through the use of login credentials. The number of such applications is increasing exponentially. Consequently, it causes an increase in the number of login credentials that users have to manage for both Internet and mobile environments. Due to the limitation in human memory, users usually forget their credentials (i.e., user names/IDs and passwords) and they tend to write down the passwords or replicate single password for many different applications. This practice could expose users to variety of security threats and attacks. A recent technological development on user authentication has introduced single-sign-on (SSO) that intends to help users with their credentials management.

This research aims to investigate password management and SSO for accessing Internet applications especially through the use of mobile devices. The research was carried out in two phases: (i) a focus group study and (ii) survey. The researchers interviewed 11 students from School of Computing (SOC), Universiti Utara Malaysia (UUM). The results of the study found that the students did not practice proper password management. Further, it suggested that SSO may not be the immediate solution to improve the students' password management.

A behavioral study was conducted on 250 students from Universiti Utara Malaysia to understand how they managed their login credentials while accessing the Internet via their mobile devices, and their perceptions and awareness towards SSO. The results suggested that students practiced poor login credential management, however, the students are concerned about the security and privacy of their credentials.

Security and privacy in mobile environment are important and need to be addressed through the use of technology and policy. The findings of this research imply system developers and policy makers on the aspect of users' security and privacy. The findings are also useful for the purpose of training and educating students on the importance of security and privacy in mobile environment.

ABSTRAK

Bilangan aplikasi Internet yang menggunakan kata laluan adalah semakin meningkat jika dibandingkan dengan sepuluh tahun yang lalu. Kebanyakan aplikasi Internet menghendaki pengguna melanggan perkhidmatan yang disediakan dan membuat pengesahan identiti menggunakan kredensi log masuk. Bilangan aplikasi seumpama ini telah meningkat secara mendadak. Ini telah menyebabkan pengguna terpaksa menguruskan satu jumlah kredensi log masuk yang sangat banyak untuk mencapai aplikasi Internet dan mudah alih. Oleh kerana ruang ingatan manusia sangat terhad, ramai pengguna lebih cenderung untuk mencatat kata laluan atau menggunakan kata laluan yang sama untuk mencapai banyak aplikasi. Amalan ini boleh menyebabkan pengguna terdedah kepada pelbagai ancaman dan serangan keselamatan. Salah satu pembangunan teknologi terkini yang dapat membantu pengguna menguruskan kredensi log masuk adalah menggunakan perakam-masuk-tunggal (Single-Sign-On, SSO).

Penyelidikan ini mengkaji tentang pengurusan kata laluan dan penggunaan SSO untuk mencapai aplikasi Internet khususnya melalui peranti mudah alih. Penyelidikan ini telah dijalankan dalam dua fasa iaitu melalui (i) kajian kumpulan fokus dan (ii) tinjauan. Penyelidik telah menemuramah 11 pelajar dari Pusat Pengajian Pengkomputeran (SOC), Universiti Utara Malaysia (UUM). Hasil kajian ini mendapati bahawa pelajar tidak mempraktikkan kaedah pengurusan kata laluan yang betul. Selain itu, ia juga mendapati bahawa SSO bukan penyelesaian segera yang dapat menyelesaikan masalah pengurusan kata laluan.

Satu kajian gelagat telah dijalankan ke atas 250 pelajar dari UUM untuk memahami bagaimana mereka menguruskan kredensi log masuk untuk mencapai aplikasi Internet melalui peranti mudah alih. Ia juga mengkaji tentang persepsi dan kesedaran pelajar dalam pengurusan kredensi log masuk. Hasil kajian ini mendapati bahawa pelajar mempraktikkan pengurusan kredensi log masuk yang lemah, walau bagaimana pun, pelajar mengambil berat tentang keselamatan dan privasi kredensi mereka.

Keselamatan dan privasi di dalam persekitaran mudah alih adalah sangat penting dan perlu dikendalikan melalui penggunaan teknologi dan polisi. Dapatan kajian ini melibatkan pembangun system dan pembuat dasar khususnya dari segi keselamatan dan privasi pengguna. Dapatan kajian ini juga adalah berguna untuk tujuan latihan dan pendidikan pelajar mengenai kepentingan keselamatan dan privasi di dalam persekitaran mudah alih.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	NAME
IT	Information technology
SOC	School of Computing
SSO	Single-Sign-On
UUM	Universiti Utara Malaysia

CHAPTER 1: INTRODUCTION

Managing login credentials for multiple Internet applications is very difficult for many of us. Different user names/IDs and passwords for different applications may not be easy to maintain. For convenience, users often create a same login ID and password for many applications. However, this could expose users to security threats that may penetrate their data particularly in critical applications such as email and Internet banking.

With the high demand of Internet applications that require login credentials, Single-Sign-On (SSO) has been introduced to improve this issue. Clercq (2002) defined SSO as a way to allow users to access multiple secure resources by authenticating themselves to an authentication authority once for all. Authentication authorities are trusted entities that manage and organize users' credentials as well as access to the resources.

Many leading Internet entities, such as Google, Yahoo, Twitter and Facebook provide SSO services to public users to access external applications. Not only that, SSO has gone beyond web applications, and now accessible through mobile devices such as smart phones and PDAs. There is also an increasing demand from mobile application providers to integrate the SSO into their applications so that they can easily be accessed by users.

In the context of security and privacy, this could increase threats to users due to the single login credentials. The more applications are authenticated using a single login credential, the higher security and privacy risks are faced by users. A recent study by Wang et al. (2012) found that the SSO services by some prominent web entities, such as Google ID, Facebook, Paypal, Freelancer, JanRain, Sears and FarmVille were vulnerable. Users' login credentials of these entities were discoverable through browser traffic analysis that revealed the flaws in the SSO protocol. The results of this study suggested an increase in security and privacy risks of SSO in both Internet and mobile environment, which has been the main concern of our research.

1.1 PROBLEM STATEMENT

The number of Internet applications with password-protection is increasing. In 2007, it was reported that average users maintained 25 password-protected accounts to access various Internet applications (Florencio & Herley, 2007). However, a recent study in 2012 reported that the average number of password-protected applications a user had was 105.7 (Bang, Lee, Bae, & Ahn, 2012). It was a substantial increase. With an increasing number of password-protected applications, users have to manage their login credentials effectively. A recent development in Internet authentication that is SSO can possibly help users in managing their login credential. It has been used in authenticating users within web-based applications which can also be accessed through mobile devices such as computer tablets and smartphones.

As the number of mobile applications with SSO has increased and many users rely on these applications extensively, how young adults at university deal with this

issue is the main concern of this research. This research chose students because they have been found as heavy users of mobile devices and social networks (Shambare, Rugimbana, & Zhowa, 2012). Hence, students certainly use SSO over mobile environment somehow. This research is interested to identify the security and privacy issues of SSO that students had experienced, and what losses that they had in corresponding to the events. Apart from this, we aim to investigate the security precautions that students may have taken to deal with the issues. We also aim to find out students' anticipations about the SSO security and privacy.

1.2 RESEARCH OBJECTIVES

The objectives of this research are:

(i) to identify how users manage their login credentials and understand the role of SSO among Internet users.

(ii) to identify users' behaviors on their Internet and mobile device usage.

(iii) to analyze how users' perceived the security and privacy of their data on the Internet and mobile devices.

1.3 SIGNIFICANCE OF THE RESEARCH

Security and privacy in mobile environment are a crucial aspect that needs to be addressed through enhanced technology and policy. The outcomes of this research would be beneficial for policy makers to develop a proper security and privacy policy with regards to SSO. The results could be also useful for the purpose of training and educating students on the importance of security and privacy in mobile environment.

1.4 RESEARCH METHODOLOGY

This research employed two methods:

(i) **Focus group study**

Participants who enrolled in Network Project course at School of Computing (SOC), UUM were invited to participate in this focus group discussion. The research participants were divided into few small groups and they were interviewed using a set of guided questions about their experiences and perceptions related to SSO in mobile environment. The data were analysed qualitatively and were used to design a structured questionnaire about the security and privacy of SSO. This method is intended to achieve the first research objectives. Please refer to Chapter 3 for the detail implementation and the results.

(ii) **Survey:**

UUM's students were invited to participate in a survey. We recruited 250 participations that were students who enrolled in Information Technology (IT) Fundamental course. This was a service course for non-IT students. The data we analysed using statistical software. This method is intended to achieve the second and the third research objectives. Please refer to Chapter 4 for the detail implementation and the results.

1.5 SCOPE AND LIMITATIONS OF THE RESEARCH

The research is limited to the specified scope as below:

(i) The respondents of this study were selected from the students of UUM. Students from other higher learning institutions could have different culture and believe that may produce different results if the similar study is replicated.

(ii) The respondents selected for this study represent a group of young adult that is below 25 years old. Similar study replicated on mature students (i.e., post graduate students) may produce different results.

The results of the study should be used with consideration of the following limitations:

(i) It is important to note that the focus group interview and the survey were conducted using English as the communication language. As the majority of the participants were non-native English speakers, there is a possibility that the respondents understood and interpreted the questions differently which may influence the results.

(ii) Some participants may feel uncomfortable discussing and revealing their behaviors. They may change the answers to look good on themselves which can also influence the results.

1.6 ORGANIZATION OF THE REPORT

This report is organizes as follows: Chapter 2 presents the fundamental concepts of login credential management and SSO. It also reviews selected literature in the same field of study. Chapter 3 demonstrates the method, results and discussions of a focus group study that aimed to identify how users manage their credentials and their

awareness towards SSO. Chapter 4 explains the method, results and discussions of a survey that aimed to identify users' behavior pertaining their Internet and mobile device usage. It also aimed to analyze how users perceived security and privacy of SSO. Chapter 5 wraps up the two studies and highlights the contributions of the research, as well as possible future works.

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

This chapter introduces the readers to the fundamental concept for the research. It first explains the role of login credentials to access Internet applications. It also portrays the issues that were experienced by many Internet users in managing login credential.

In this section, the readers will find an explanation on SSO, which of the alternative to overcome the login credential management issues. Lastly, the past related studies were analyzed to see how this area of the research grows and to demonstrate why this research is needed.

2.2 USERS' LOGIN CREDENTIALS

It has been mentioned earlier that many Internet applications are password-protected. In other words, users have to provide their login credentials in order to get access to the intended applications. The most common login credential method for Internet applications is a combination of a username and password (Bang, et al., 2012).

The main purpose of login credentials is to authenticate users (Preibusch & Bonneau, 2010). Authentication will enable authorised users to access resources from the applications particularly static information and data from databases and perform transactions such as those in online banking and online shopping applications.

Although many researchers suggested that the use of password is no longer a secure authentication method (Ciampa, Revels, & Enamait, 2011; Gaw & Felten, 2006),

there is no other alternative so far. Hence, the use of login credentials as an authentication method is still feasible and it gives a substantial level of security when proper practices are implemented including the use of strong password and enforcement of security policy. Summers and Bosworth (2004) highlighted some of the good practices including the use of alphanumeric words consisting of six to ten characters, and avoiding dictionary words as well as words that are related to ourselves. They also highlighted security policy concerning passwords management such as frequent changes of user passwords, restrict users from reuse the old passwords, just to name a few.

However, users often practice poor password management. Tam et al. (2010) reported in their study that users know what a good password is and the consequences of practicing poor password management. However, they tend to practice weak password management because they did not see the immediate negative implications on themselves. Many researchers also agreed that users' behaviours can expose applications in the Internet to various security threats and attacks (Ciampa, 2011; Kumar, 2011; Tam, et al., 2010). Therefore, an approach that can help users to improve their password management is highly needed.

One of the possible approaches is SSO. SSO can be used to solve problems related to multiple number of login credentials for accessing different applications (Radha & Reddy, 2012). The next subsection explains the SSO concepts in further details.

Authentication of users' identity in mobile and internet applications plays two important roles. Firstly, it acts as a security method to authenticate access from

authorized users, and secondly, it is a way to recognize users' preferences and characteristics that act as a method to provide them with personalize contents. Both reasons have made applications providers implement user authentication. Consequently, the number of Internet and mobile applications requiring registration has dramatically increased.

This imposes a new challenge to users, as they need to keep a lot of login credentials to get access to the applications. It is critical when users are unable to manage their login credential effectively that demanded for a new alternative approach of its management. Having multiple login credentials is not only a bothersome aspect of the Internet and mobile environment; it is also one of the most serious security issues that has been continuously debated. When a user has a number of login credentials, how he or she manages them is always been an issue. The user tends to write them on paper, or keep them stored in the mobile devices. Another potential behavior is reusing or repeating the same login credential on many different applications. Any of this behavior is actually exposing users to various security attacks.

It is important to realize that a strong security protection does not guarantee that a particular system is secure. This is definitely true when the users' practices and behaviors do not bother with it. Mistakes due to users' malpractices and behaviors are the easiest point of attack in computer systems. Hence, it can be said that, security is only working when both technical and users' behavioral perspectives are there at the same time (Bang, et al., 2012; Ng, Kankanhalli, & Xu, 2009).

Good login credential management practices are important to ensure that systems and applications are secure. The practices include regular change of the password, use non-dictionary word for the password and combining password with special characters.

Another alternative that may help users to manage their password is through the use of SSO. The detail concept of SSO is explained in the next section.

2.3 SINGLE-SIGN-ON (SSO)

Mobile computing is increasingly popular among young generation of Internet users. Furthermore, mobile phone users who are connected to the Internet are much higher than desktop users with the most popular application is the social networks (Mascolo, 2010). Apart from social networks, users can also accessed emails and performed online banking and commercial transactions through mobile devices. Many applications are available through mobile devices which cause data exchange between users can be a source of security attacks and threats.

Internet and mobile application providers protect their data and systems from security attacks by implementing user authentication. Authorized users can access the specified resources or perform transactions by providing login credentials to the systems. The combination of user ID and password is the most common user authentication method for mobile and Internet applications.

As explained earlier in the preceding section, Internet users experienced problems with password management especially when many applications require them to create login credentials. Users were unable to remember all user names and

passwords, which lead them to practice poor login credential management such as replicating single password for many applications, writing down the passwords on paper or storing them in mobile devices.

This issue was the main reason why Single-Sign-On (SSO) technique was introduced. Hardy (1996) analogised SSO as a "master key" that allows a user to get access to all the systems that he or she is allowed to. Clercq (2002)defined SSO as a way to allow users to access multiple secure resources by authenticating themselves to an authentication authority once for all. Authentication authorities are the trusted entities that manage and organise users' credentials as well as access to the resources. Radha and Reddy (2012) further classified SSO into three dimensions: (i) the type of networks that the SSO is applied (i.e., Intranet, Extranet, or Internet), (ii) the architecture of SSO implementation (i.e. simple, or complex), and (iii) the types of credentials (i.e., single or multiple) and the protocols used for the implementation. Other names similar to SSO that practitioners and researchers always used are single sign-in (SSI), authentication and authorization infrastructures (AAIs), privilege management infrastructures (PMIs) and identity management tools (Oppliger, 2004).

In general, there are three entities involved in SSO; users, application providers, and authentication providers. The basic concept of SSO is that users can use a single login credential of their own to access multiple number of Internet applications by supplying their identity to authentication providers. This is usually done by subscribing to their service. The application providers will use the service of the authentication provider to authenticate users' identity. The application providers do not keep users

identity and their personal information. They rather use the services offered by the authentication providers. The following Figure 2.1 simplifies the communication flow between the entities utilising SSO. Many leading Internet entities, such as Google, Yahoo, Twitter, Paypal, MySpace and Facebook provide SSO services to public users to access external applications.

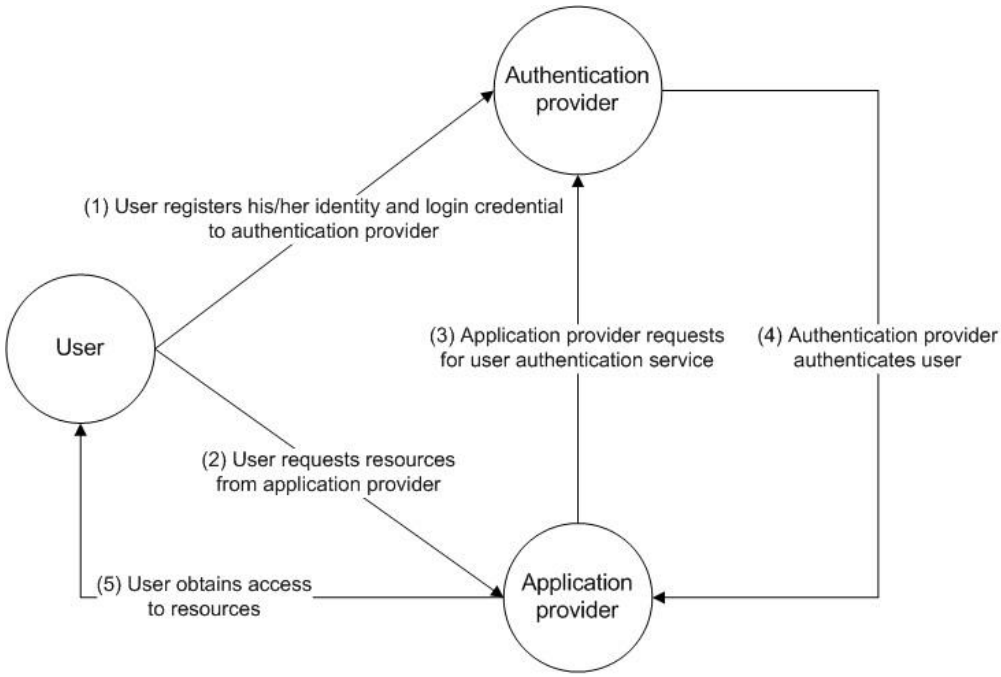


Figure 2.1: Communication between SSO entities

Although SSO has been used since distributed systems were started two decades ago, it was limited to users within an enterprise computing environment. However, it is gradually popular when the web 2.0 was introduced. Within the social network environment, many leading providers such as Facebook, Yahoo!, Linkedln, MySpace and Google provide the authentication services for both users and application providers. The social networking providers offer developers with software development kit (SDK)

that enables them to integrate the SSO service into their applications. This would be of great advantage for the application providers as they do not have to create user profiles for their applications. Further, they also have higher chances to attract new users of the social networking providers to use their applications or services. In general, the SSO has eased the user identity management for both application providers and users.

Within the Internet environment, SSO standards such as SAML Oasis (SAML, 2013) and OpenID (OpenID, 2013) have been proposed and developed by community groups. OpenID is the standard that has been used by major social networking providers. It aimed to provide users and application providers with secure cyber identity management. Any web entities can be an OpenID provider for free. It guarantees the security and privacy of users' passwords that they will not be revealed to the application providers in any way. Some of the benefits of using OpenID for users are: (i) accelerate login process of favourite websites, (ii) efficient maintenance of login credential, (iii) gain greater control over personal cyber identity, and (iv) minimise security risks (OpenID, 2013). The benefits for application providers are: (i) increase users' subscription as they do not have to register and fill in registration form, (ii) share rich users' profile data, (iii) less maintenance of users' profile data, and (iv) link the applications to the social websites.

As we discussed earlier, SSO gives users and application providers with a simple solution for cyber identity management, particularly users' login credentials and their profiles. Further, many social networking websites have provided this infrastructure which can be an advantage for application providers to attract more users. Users can

simply login using their existing social network login credentials; hence, the registration process is no longer required. Apart from this, the standards that govern the implementation of SSO guaranteed the security of users' passwords which makes SSO an efficient approach towards identity and login credential management.

2.4 RELATED STUDIES

Many past studies in the area of computer security were more focusing on users' behaviors in the Internet environment. Users' behavioral studies within a mobile environment are still new, and not much attention has been given to this particular domain. The following paragraphs discuss studies that particularly related on Internet users' login credential management.

Bang et al. (2012) studied Korean Internet users' behaviors specifically on their login credential management. Their study revealed that user's behaviors make their login credentials vulnerable and susceptible to attacks. This is particularly true when users replicate the same login credential for many unsecure online systems. This practice also jeopardizes other secure online systems, as the replicated login credentials can be used by cyber criminals as a tool to penetrate them. The results of Bang's study proposed two important points to organization and government agencies, (i) the needs for formulation of a security policy that prevents users from replicating their login credentials, and (ii) the needs for new authentication methods other than remembering login credentials.

Tam et al. (2010) conducted a study to understand whether users are aware of the good password management practices and how do they behave towards it. They

conducted an experimental study on 140 Internet users. The results of their study revealed that users were aware of the characteristics of good and weak passwords. However, they tend to practice bad password management because they did not see and anticipated the immediate consequences of those practices. They rather see that other people would get the consequences of bad login credential management than themselves. The result also suggested that users tend to go for convenience-security trade-off.

Kumar (2011) conducted a survey in India investigating the usability of alphanumeric passwords. In his study, he found that alphanumeric passwords are difficult to remember causing users to write them down on papers. The study suggested that usability can be a security tradeoff. Although alphanumeric passwords can be considered as robust against attack, however, many users are unable to remember them. Consequently, they wrote the password on papers.

The three studies discussed above show users practiced weak login credential management by replicating the same passwords in different applications, use weak password, and write down the passwords on papers. These are common users' behaviors when they access the Internet through a wired network. In the context of mobile computing, we wonder how users behave. Hence, the following sections explain our research approach to understand how users manage their login credential and how they behave in a mobile computing environment. Two studies were carried using different methods that are focus group discussion and survey.

CHAPTER 3: THE FOCUS GROUP DISCUSSION

3.1 METHOD

This study aimed to identify how users manage their login credentials and understand the role of SSO among Internet users. As students have been found to be the heavy users of mobile and Internet technology (Shambare, et al., 2012), their participation in study can give useful information and findings to understand their password management behaviours.

Data for this research were collected through focus group interviews. It is a suitable way for studying human behaviour especially in the area of human-computer interaction. Data obtained from the study were qualitatively analysed and presented in a descriptive analysis form.

3.2 PARTICIPANTS

The respondents were recruited among undergraduate students of Universiti Utara Malaysia who took the final year project paper of Information Technology (IT) degree program. Students who enrolled in this course were encouraged to actively participate in the school research projects as a way to expose them to research. Eleven students (ten males and one female) participated in the study. The students comprised five Malaysians, five Yemenis, and one Russian aged between twenty and twenty three. This study was carried out during the first week of September 2012.

3.3 MATERIALS

A set of open-ended questions for the interview was constructed based on our literature analysis of current and past studies concerning password security and SSO. The questions were divided into three parts as below (Refer Appendix A for the questions):

Part I: Demographic information

Part II: Password security practices

Part III: Knowledge on SSO

3.4 PROCEDURES

The focus group interviews were conducted in 3 sessions. Each session comprised either 3 or 4 students with a same facilitator for all the sessions. The focus group interviews were conducted between forty minutes to one hour.

It was conducted in a room where the participants and the facilitator sat in a circle facing to each other. The facilitator posed the same questions to each of the participants. The students took their turn to answer the questions and they were allowed to discuss the topic within the group. The students were also provided with light refreshment.

The focus group interviews were voice-recorded with consent from the participants. The interviews were transcribed and the analysis of the data is presented in the next section. Refer to Appendix B for the transcript.

3.5 RESULTS

Based on the interview, we were able to collect valuable data as described below:

3.5.1 Access to Applications with Authentication

We firstly investigated the number of Internet applications with login credentials (i.e., a user name and a password each) for authentication that the students subscribed. In average, the students subscribed to five Internet applications. It ranges between two to ten applications including emails (Gmail, Yahoo, Hotmail, university email, etc.), social network sites (i.e., Facebook and Twitter), video-on-demand, online shopping, file sharing, and voice-over-IP applications.

3.5.2 Password Practices

We were interested to know how the students managed their usernames and passwords. Hence, the facilitator asked the students on their techniques to remember them. As expected, five of them reuse the same user names and passwords to access different applications. A student wrote his usernames and passwords on a piece of paper, and save them in his mobile phone respectively. In order to remember the password easily, a student used his best friend's phone number, his parents' names, his pet's name, his date of birth and his citizen identification number respectively. One student used his favourite movie titles for passwords[1].

[1] The respondents were asked about the categories of the password but not the exact passwords.

The facilitator further asked them whether the approaches they used for remembering their passwords were working well. All of the students reported that they had no problem so far.

3.5.3 Techniques to Improve Password Management

The students were asked to suggest ways to improve password management particularly for users with many login credentials. A student suggested the use of biometric technology for authentication. Another student suggested the use of a SSO mechanism.

Further, the facilitator asked the students concerning the feasibility of SSO. Ten students thought that SSO is feasible to be implemented. Although SSO is feasible, one student suggested that it is not suitable for banking and financial systems.

In terms of managing the SSO, the students suggested that the government should play a role in initiating an independent and trusted body to manage SSO for the citizen. Such body could be Malaysian Communications and Multimedia Commission (MCMC) for example.

3.5.4 Students' Awareness of Single-Sign-On (SSO)

The facilitator asked the students whether they know the existence of SSO technologies that manage users' credentials in the Internet. Four of the students knew about it. The students who knew about SSO were further asked to explain the basic concept of it. All of them were able to explain the concept correctly. The students who

knew about SSO anticipated that it is secure. However, those who did not know about SSO thought that the technology does not provide users with high level of security and privacy. The students also anticipated some security weaknesses especially cyber-crime involving identity theft and breach of privacy.

3.5.5 The Role of Single-Sign-On (SSO)

In order to understand the students' views regarding the role of SSO, the facilitators first informed them the needs to have good password management. Then, they were asked on the methods or strategies to secure users login credentials for Internet applications. The majority of them suggested that Internet application providers should strengthen their security protections. Only one student recommended that Internet users should manage their login credentials properly by protecting and securing them from other people. He also indicated that the use of different usernames and passwords for different Internet applications is sufficient.

3.6 DISCUSSIONS

The previous section discussed the results of focus group interviews regarding password management and SSO. Generally, we found that the students had many Internet applications that require them to provide login credentials to access the applications. The students had used the minimum of two and up to ten Internet applications at one particular time. This shows that many applications are now being online and users are required to authenticate themselves to get an access to these applications. Although authentication through login credentials can provide security protections, this has obviously created another issue to users. The growing number of

Internet applications with authentication causes users to manage a number of login credentials at one particular time.

Managing a number of passwords is difficult. Users that have security precautions in their mind might create strong alphanumeric passwords. However, if the number of login credentials is large and it keeps increasing; users are more likely to face problems to recall and match passwords with their correct applications especially for those that are used seasonally. Users will not be able to recall the passwords and this require them to reset or contact the administrator to get the new passwords. This issue is common due to the reason that human memory is limited in their capability in remembering and recalling things (Kumar, 2011). Hence, remembering a number of alphanumeric passwords is a great challenge especially when the passwords have no relationships with other things or events in their memory.

Users often experience this issue and they tend to practice techniques that will ease them to recall those login credentials quickly. Among those practices are repeating the same login credentials in many applications, writing them on paper, save them on mobile phones, and use easy-to-remember passwords. These are among the practices that we discovered in this study.

We also found that the students were comfortable with their practices because of two reasons. First, the practices helped them to manage their login credentials easily with low chances of forgetting them. Second, they did not experience any security issues as immediate consequences of their practices. These two reasons have made the students think that their password management practices were adequate.

Further, the students thought that their practices have no security implications. In reality, this could be a source that leads to security attacks to the Internet applications. Many Internet applications are securely protected through the use of encrypted passwords. However, there are also some other Internet application providers that have not implemented such security protections. When users replicated passwords in both secure and unsecure applications, this will open a door to hackers. Hackers can observe and analyse users' passwords, capture the unencrypted passwords and use them to access the secure applications. This kind of security attack does not affect the users directly; however it does have impact on the Internet application providers and their resources.

From the interviews, we also found that students have limited knowledge on SSO and its current implementation. Some of them suggested that the government should play a role in initiating centralised digital authentication systems. This could be beneficial for local Internet applications. However, it is important to note that many users use Internet applications hosted in other countries around the world. Hence, the government role is limited in this scenario.

It is interesting that the students have mix views in terms of SSO security. A quarter of the students knew about its existence and they were certain with SSO security. In contrast, the students with no prior knowledge on SSO indicated that SSO does not provide strong security and privacy protections. They also anticipated that SSO implementation could lead to cyber-crimes.

Another interesting finding is on the students' thought that Internet application providers should implement strong security protections for their applications. Through

this thought, we can see that users highly rely on Internet application providers to provide security protections. On the other hand, they do not realise the importance of their role in ensuring the security of the applications. This could be an important signal from users to Internet application providers and security experts. It can be translated that the owner of the systems should be aware of all consequences as the effects of the users' behaviours including password replication.

The main issue that should be taken into consideration is on users' behaviours and attitudes. Although Internet application providers implement all possible security protections, they are still exposed to security attacks due to their users' behaviours. In this case, the use of SSO is not a direct solution to this problem. This is true when users still replicate their passwords for applications with SSO and without SSO. The fundamental issue remains there and unresolved. In a nutshell, SSO is a good solution to reduce the number of login credentials that users have, however, it does not improve users' password practices especially the behaviours on passwords replication.

From the discussion in the preceding paragraphs, we highlighted some actions that need to be taken to ensure that computing recourses pertaining Internet applications are properly protected against security threats and attacks. The actions include:

(i) the need for users' security education especially on proper password management practices,

(ii) the need for a security policy that enforces secure password behaviours among users,

(iii) the need for SSO implementation, and

(iv) the implementation of alternative authentication methods other than login credentials.

It is suggested that the above strategies are implemented as a group of actions rather than individually.

3.7 CONCLUSION

Weak password management among users could be a security threat for Internet applications. Although Internet applications implemented strong security protections, their users' password practices can be a source of security attacks especially users who practice password replications. Passwords that are used for fully-secured applications can be easily captured by hackers. They can simply analyse or steal passwords from the same user in unsecure applications.

The SSO implementation is a good solution to reduce the number of login credentials that users have at one time. However, it is unable to improve users' password management practices especially password replication. The only way to this is through education and awareness programs. This study would like to emphasise that the core issues to this is users' behaviours. Organisations and governments should take part and play their roles to educate users.

The findings of this research also indicates the need to study for alternative authentication methods that are more friendly to users than the existing multiple login credentials. This could be an opportunity for researchers to explore a new method for Internet authentication.

CHAPTER 4: THE SURVEY

4.1 METHOD

A survey was conducted to obtain information from respondents on their login credential management. The survey attempted to answer the following research questions (refer to Appendix C for the detail questions):

Question 1: How the students used the Internet?

Question 2: How the students managed their login credential?

Question 3: How the students perceived the security and privacy of their data on the Internet?

The above three research questions were the main concern of this study. The following sections explain the participants, materials, procedure, results and implication of the study.

4.2 PARTICIPANTS

A number of 250 students of Universiti Utara Malaysia from various programs (e.g., Business, Accounting, Economic, Linguistic, Finance, Social works, etc.) participated in this study during October to November 2012. The researchers asked permission from selected instructors who taught IT Fundamental course to recruit students from their classes. Students received no compensation for their participation.

The university students were selected as the sample for this study because the current younger generation grows within mobile computing technology and the Internet.

Past research had also proven that university students are particularly the heavy users of mobile devices (Shambare, et al., 2012), hence making them appropriate to be the targeted group for this study.

4.3 MATERIALS

A close-ended questionnaire was designed according to common questions that had been asked in other past studies pertaining login credential practices. It was divided into 4 parts as follow:

(i) Part I- Demographic information (6 questions)

(ii) Part II- Mobile devices and Internet behavior (4 questions)

(iii) Part III- Login credential management (5 questions)

(iv) Part IV- Perception on security and privacy (7 questions)

It is important to note that this is an exploratory study, hence the questions were mostly asked to investigate the respondents' behavioral information.

4.4 PROCEDURES

A self-report study was conducted as the main research method. The participants were asked to fill-in a self-report questionnaire to assess their login credential practices. They completed the given task in a large seminar hall within a researcher's supervision. They were asked to return the questionnaire to the researcher before they left.

4.5 RESULTS

This section explains the results of the study. A descriptive analysis was carried out on the data obtained for the study.

4.5.1 Demographic Information

Demographic information of the respondents is shown in Figure 4.1. In total, 78.4% female students participated in the study. In terms of the respondents' age, 99% of them were below 25 years with the mean age of 21.25.The majority of them were undergraduate students from different number of semesters and courses.

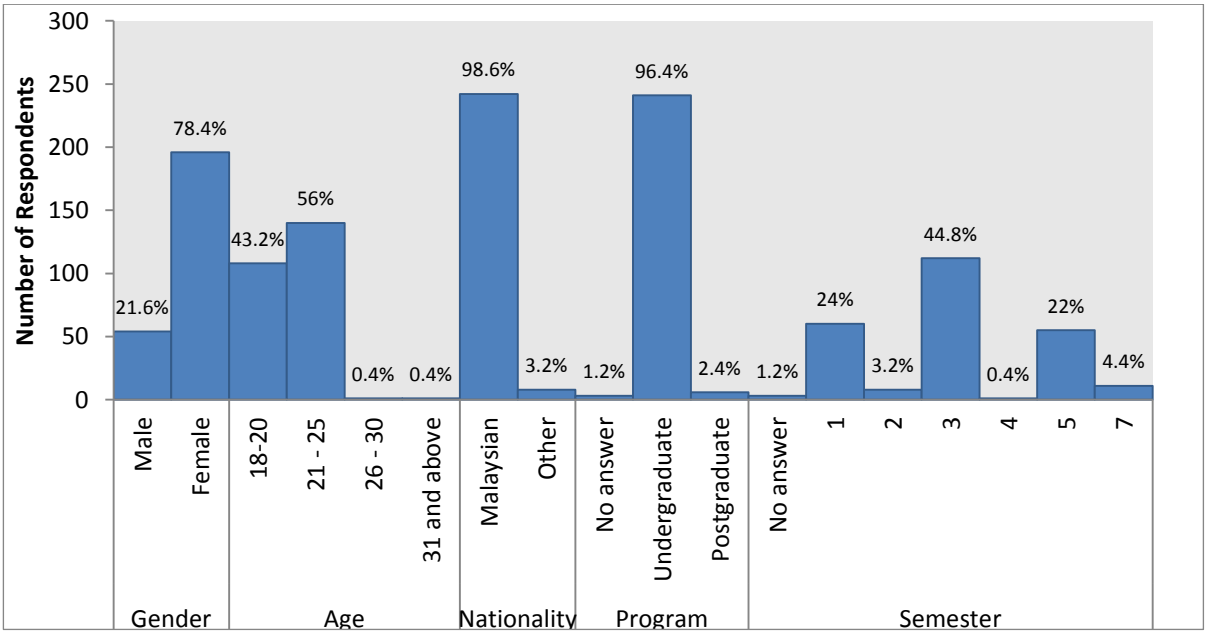
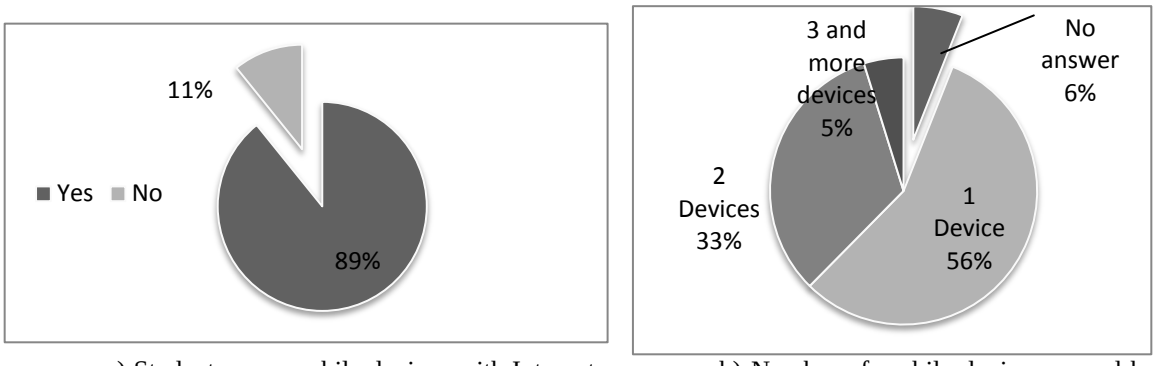


Figure 4.1: Demographic information

4.5.2 Mobile Device and Internet Usage Behaviors

In studying the behaviors of the students, we first asked them on their mobile devices ownership. The pie charts in Figure 4.2 (a) show that 89% of the students

(approximately 223 students) own mobile devices with Internet connectivity including smart phones, tablets, netbooks, and laptops. Out of this number, 56% had only one mobile device, 33% had two mobile devices, and 5% had 3 or more devices as shown in Figure 4.2(b). About 6% of them did not answer the question.



a) Students own mobile devices with Internet connectivity

b) Number of mobile devices owned by the students

Figure 4.2: Mobile devices ownership

We also investigated how long the respondents spent their time accessing the Internet. The bar chart in Figure 4.3 shows the information.41.6% of the respondents spent more than 4 hours a day connecting to the Internet, 21.2% and 20.4% used the Internet between 2 – 3 hours, and 3 – 4 hours a day respectively. Less than 6% had accessed the Internet less than an hour a day.

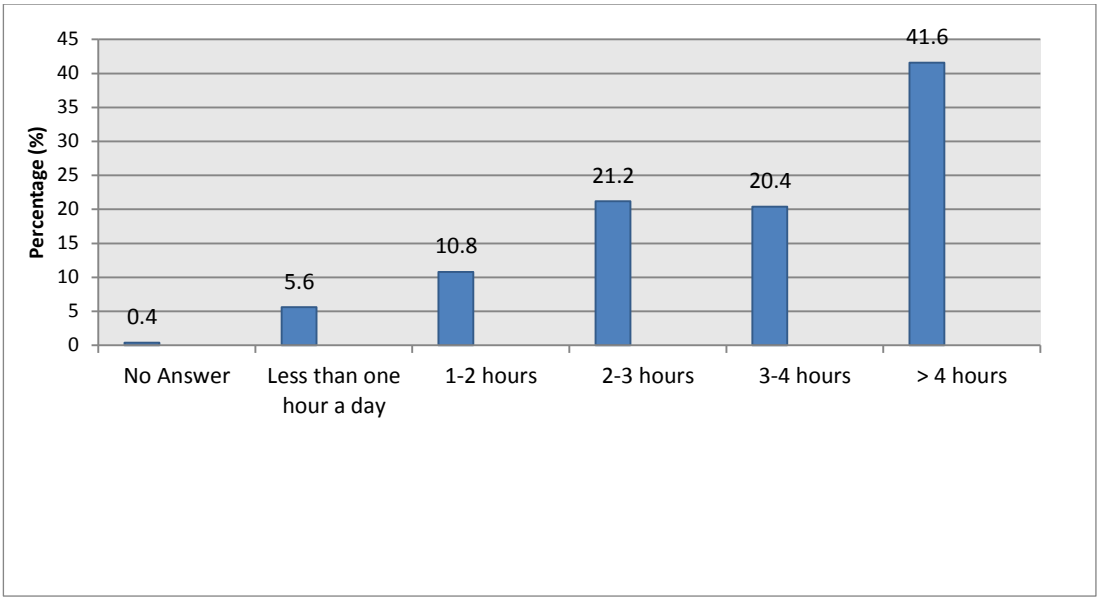


Figure 4.3: The duration of access to Internet daily

We also investigated the type of Internet resources that the respondents accessed. The respondents were asked to choose the top three Internet resources that they frequently access every day. Figure 4.4 below shows that the majority of the students used the Internet for social networking with 216 counts. The result also revealed that web browsing, music, news and file sharing also popular within the sample.

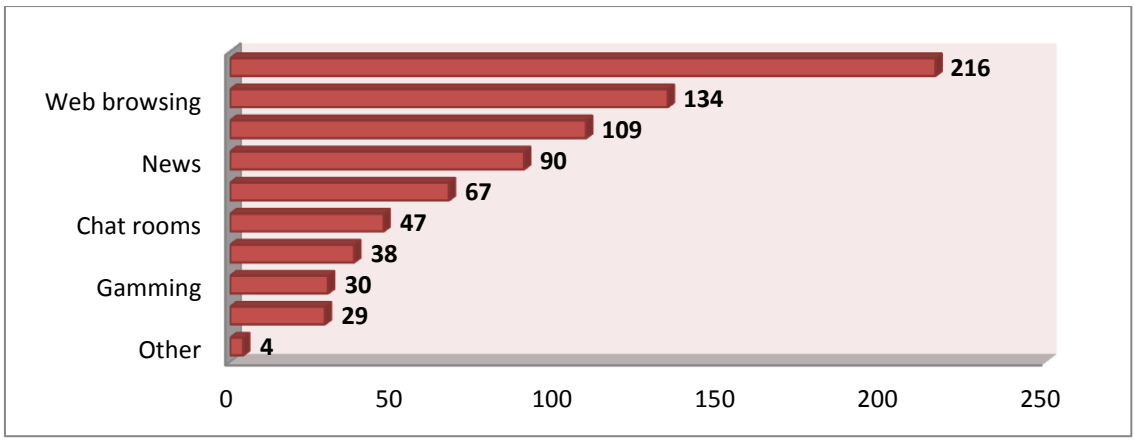
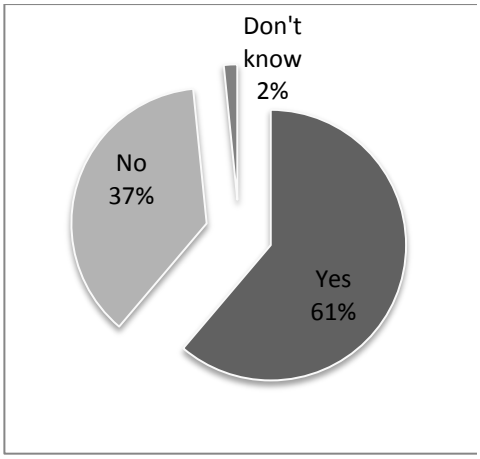


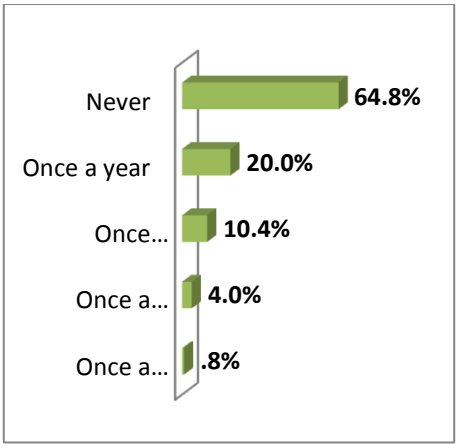
Figure 4.4: Types of Internet recourses that the students accessed

4.5.3 Login credential management

In order to understand the students' behaviors on login credential management, they were asked on how many login credential they have at the time this study was conducted. All respondents had at least an email account and a web login, and the maximum of eight accounts respectively with the password length was within 6 – 15 characters. Figure 4.5 shows how the students managed their login credentials.



a) Replicated the same password for multiple applications



b) How frequent the password was changed

Figure 4.5: Login credential management

From the figure, more than half of the respondents (61%) used the same usernames and passwords for accessing multiple applications. Only a small number of students (37%) used different passwords to access different applications. On the other hand, 64.8% of the respondents never changed their passwords. Nevertheless, some respondents changed their passwords once a year (20%), 10.4% of them changed their passwords every six months, and 4% every month. Only 0.8% changed their passwords every week. Although some respondents concerned about the password security, the study found that 25.2% of the respondents shared their passwords and mobile devices with other people (e.g., family, spouse, etc.).

4.5.4 Perception on security and privacy

The respondents were also asked on their perception about security and privacy. Figure 4.6 shows their responses. More than 70% of the respondents were concerned about privacy on the Internet. However, 9.2% of the respondents indicated that they were "less concerned" about their privacy while using the Internet.

This study also examined students experience whether they had been asked to provide personal information by the visited websites. Majority of the respondents (76.8%) had experienced it. Interestingly, 39.2% of the respondents chose to give fake information to the websites that requested for their personal information, and 14% chose to provide their real personal information. More than a half of the respondents (54%) were reluctant to provide their personal information.

In terms of supplying personal information for advertisement, the findings of this study suggested that 44.4% of the respondents were not willing to provide personal information for online advertising purposes. Further, half of the samples read the terms and conditions of web policies before they provided the personal data to particular websites, while the other half never read them.

From the findings, 60.8% of the respondents had never been contacted by strangers as a result of providing data for advertisement. While 24% experienced it, 13.6% did not remember such incidents. More than 70% of the respondents believed that many people can view their personal data if they place them on the Internet. However, in response to the question about security measure for personal data protection, only 54.4%

performed some security and privacy protection, while 17.2 % did not take any security measure. A portion of 26.8% did not know how to do it.

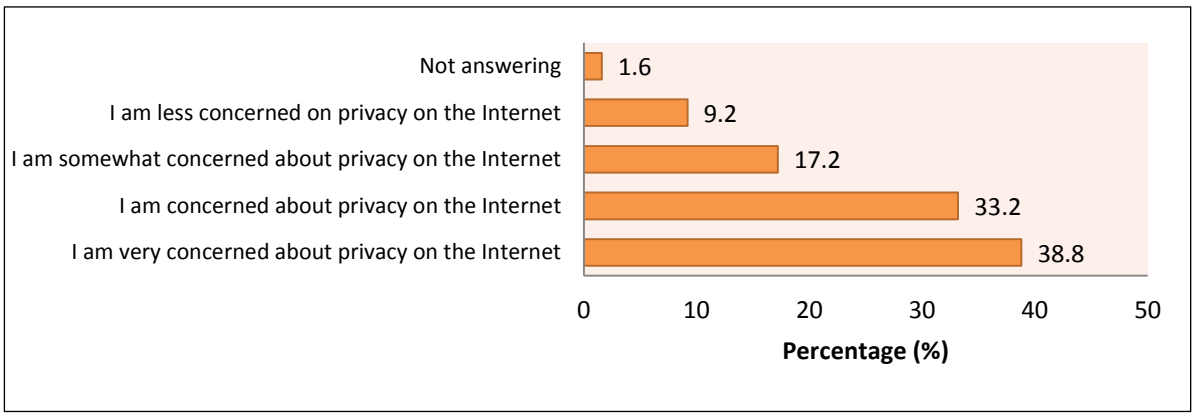


Figure 4.6: The students' perceptions on security and privacy

4.6 DISCUSSIONS

Mobile devices began a worldwide revolution when they provide users with the first time experiences connecting online away from computer and wired Internet connections. The development of smart phones and other gadgets took the power of mobile technology a step further and shifted students expectations for accessing digital content. With the increase of mobile technology such as smart phones and tablet PCs, it may also give rise to privacy and security threats. Nowadays, the traditional authentication method such as username and password are no longer sufficient to cope with the latest security threats. Therefore, strong authentication scheme becomes more relevant with the current Internet technology.

4.6.1 Internet usage behavior

This study revealed that the majority of the students owned at least one mobile device with Internet connectivity. It is also suggested that the students were heavy Internet users, where half of them spent more than four hours a day accessing the Internet from their mobile devices. The majority of the students accessed social network sites especially Facebook when they online. The Internet usage confirms that students show addictive and habitual behavior (Shambare, et al., 2012). Shambare et al.(2012) suggested that these two behaviors are associated with frequent used of mobile devices among students. Accessing the Internet has become the major focus of a person's life more than other activities and it is performed regularly and repetitively.

4.6.2 Login credential management

In terms of login credential management, a few interesting results have been found. This study suggested that two-thirds of the students never changed their password, and similarly, they replicated one single password in many Internet applications. This critically shows that the students did not practice proper login credential management. This finding confirms the results of a past study done by Bang et al. (2012) that found a similar behavior among students in terms of their login credential management. They explained that users tend to replicate their passwords due to limited memory capability that a human has. It is a common cognitive theory on human memory (Mayer, 2005). When more sites require users to create passwords, their mind requires more mental process of searching and retrieving the passwords.

Consequently, human mind is unable to remember each and every one, hence making users to simply reuse the existing passwords.

From this study, it is also discovered that a quarter of the respondents shared their passwords with other people including family members and friends. Although it is relatively a small percentage, this result shows that they were not fully aware of the threats that may rise from their actions. Password security is compromised if a cybercriminals learn a single word from it. They will be able to perform various security attacks such as impersonate the user, and access the resources to which this user entitled.

Another important finding of this study shows that the students created their password based on surrounding objects that can be easily broken through brute-force attacks.

The above evidence suggests that the students' practices did not comply with common security guidelines such as a password should be at least eight characters long, user should use different password for each login account, and change them regularly. Although the students were aware that they have to protect the privacy of their personal data, their behaviors and practices on the login credential management did not align with their perceptions. We are interested to study in the future, why do students' behave far away from what they thought in terms of the security aspects. We hypothesize that students' behaviors are influenced by their attitude and perceived norms.

4.6.3 Approach to increase login credential security

As mobile computing is increasingly popular among Internet users especially students, proactive actions should be taken to increase the security of its resources. Based on our findings, we suggest the following managerial and technological approaches to increase security and to promote good practices of login credential management within a mobile environment:

(i) Training - Students' practices and behaviors on their login credential management are insufficient and weak. Hence, proper training and awareness programs must be implemented to improve this condition.

(ii) IT Policy - The existing security policy should be modified in such a way that it promotes good security practices, such as regular password change and enforcement of long and secure passwords.

(iii) Single-sign-on (SSO) - SSO could be an alternative to avoid students from replicating their passwords in different applications. SSO technology and protocol such as OpenID and SAML (Armando et al., 2013; OpenID, 2013; Radha & Reddy, 2012) are available, and they can provide better login credential management to users.

(iv) Biometric authentication - The use of biometric authentication (Furnell, Clarke, & Karatzouni, 2008) such as finger print could be an alternative to login credential for a mobile computing environment as it could increase the efficiency of identity management.

The above approaches play two-fold roles. Training and IT Policy can be seen as managerial approaches that can educate students to change weak login credential management practices. On the other hand, SSO and biometric authentication are the technological approaches that can facilitate login credential management and as well as strengthen the security of mobile computing applications.

4.7 CONCLUSION

The survey managed to obtain the information from the respondents and the three research questions as stated at the beginning of this chapter were answered. Firstly, the results suggested that the students spent more than four hours a day accessing the Internet particularly Facebook. Secondly, the students did not practice good login credential management where they replicated the same password to access multiple applications. Finally, although the students were highly concerned about their privacy in the Internet, only half of them implemented security and privacy protections.

The findings of this study can be an input and useful for the higher institutional administrators and policy makers. As majority of the students accessing the Internet through campus networks, it is important to formulate Internet policy that can secure the institutions' network resources from threats and attacks either internally or externally.

CHAPTER 5: CONCLUSION

5.1 RESEARCH CONTRIBUTIONS

The results that the researchers explained in Chapter 3 and Chapter 4 respectively suggested some important findings with regards to Internet users, particularly young adults. The research demonstrates how users behaved towards the Internet and mobile device usage. They also present users' perceptions and awareness of SSO.

The outcome of the research contributes in the following ways:

(i) Contribution to application providers and system developers.

From the study, it is obvious that many users replicated their password for accessing many different applications. This behavior can have impact on the application providers either directly or indirectly. If a user replicates and uses a single password for accessing different applications, the mix up between secure and unsecure sites will have an impact on the application providers. By observing user's password in unsecure applications, a hacker can easily get access to other secure applications. Hence, system developers and application providers must identify and implement the best way to ensure that users will not replicate the passwords and mix up the use of secure and unsecure applications.

(ii) Contribution to policy makers at higher learning institutions.

The study also suggested that users were concerned about their security and privacy of their login credentials. However, users tend to practice poor credential management because managing a lot of credentials at one time can be very difficult. Hence, the internal applications accessed by students should use SSO so that, it will help to reduce the number of credential that users must manage. Other than that, the policy makers should also look into the way to educate and train users on proper credential management.

5.2 RECOMMENDATIONS AND FUTURE WORKS

User authentication is an important component of Internet-based applications. Whether the applications are accessed through mobile devices or personal computers, the security of the applications highly rely on the component. Hence, research pertaining user authentication will definitely improve security of Internet-based applications.

The currently growing area of research in relation to security is making security mechanisms more usable and user-friendly. Many past studies found that security is always the tradeoff to system's usability. In other words, when a system has high level of security, it has low level of usability. For example, a system that requires users to create a strong password (e.g., 8 characters long with combination of at least a symbol and a number) may likely to cause users to forget the password due to the limitation of human memory. Hence, research towards usable security is beneficial to improve users' experience with Internet-based applications.

The researchers are currently conducting an experimental study on the usability of web SSO. This is an extension to the research reported here. Unlike the completed research where the results were obtained based on participants perceptions, the ongoing study exposes the participants to real scenario of SSO that embedded in an e-learning system. The participants were asked to evaluate the usability of the web SSO in comparison to traditional authentication technique. The study is currently at reporting level. Another extension to this ongoing research is to investigate professional perception of the security and usability of SSO for accessing e-learning websites.

Another research that the researchers are currently engaged is on the security, usability and convenience of social network credentials for personal retailers who conduct businesses online. After completion of all of the research, the researchers intend to compare the usability of SSO in various domains of Internet-based applications.

REFERENCES

Armando, A., Carbone, R., Compagna, L., Cuéllar, J., Pellegrino, G., & Sorniotti, A. (2013). An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations. *Computers & Security, 33*(0), 41–58. doi: http://dx.doi.org/10.1016/j.cose.2012.08.007

Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *International Journal of Information Management, 32*(5), 409-418. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2012.01.001

Ciampa, M. (2011). Are password management applications viable? An analysis of user training and reactions. *Information Systems Education Journal, 9*(2), 4.

Ciampa, M., Revels, M., & Enamait, J. (2011). Online Versus Local Password Management Applications: An Analysis of User Training and Reactions. *Journal of Applied Security Research, 6*(4), 449-466.

Clercq, J. D. (2002). *Single Sign-On Architectures*. Paper presented at the Proceedings of the International Conference on Infrastructure Security.

Florencio, D., & Herley, C. (2007). *A large-scale study of web password habits.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

Furnell, S., Clarke, N., & Karatzouni, S. (2008). Beyond the pin: Enhancing user authentication for mobile devices. *Computer Fraud & Security, 2008*(8), 12-17.

Gaw, S., & Felten, E. W. (2006). *Password management strategies for online accounts.* Paper presented at the Proceedings of the second symposium on Usable privacy and security.

Hardy, G. (1996). The truth behind single sign-on. *Information Security Technical Report, 1*(2), 46-55. doi: http://dx.doi.org/10.1016/S1363-4127(97)89356-9

Kumar, N. (2011). Password in Practice: an Usability Survey. *Journal of Global Research in Computer Science, 2*(5), 107-112.

Mascolo, C. (2010). The power of mobile computing in a social era. *Internet Computing, IEEE, 14*(6), 76-79.

Mayer, R. E. (2005). Cognitive theory of multimedia learning. *The Cambridge handbook of multimedia learning*, 31-48.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi: http://dx.doi.org/10.1016/j.dss.2008.11.010

OpenID. (2013). The Benefits of OpenID, from http://openid.net/get-an-openid/individuals/

Oppliger, R. (2004). Microsoft .NET Passport and identity management. *Information Security Technical Report, 9*(1), 26-34. doi: http://dx.doi.org/10.1016/S1363-4127(04)00013-5

Preibusch, S., & Bonneau, J. (2010). The Password Game: negative externalities from weak password practices *Decision and Game Theory for Security* (pp. 192-207): Springer.

Radha, V., & Reddy, D. H. (2012). A Survey on Single Sign-On Techniques. *Procedia Technology*, *4*(0), 134-139. doi: http://dx.doi.org/10.1016/j.protcy.2012.05.019

SAML. (2013). Welcome to SAML Oasis.org, from http://saml.xml.org/

Shambare, R., Rugimbana, R., & Zhowa, T. (2012). Are mobile phones the 21st century addiction? *African Journal of Business Management 6*(2), 573-577.

Suriadi, S., Foo, E., & Jøsang, A. (2009). A user-centric federated single sign-on system. *Journal of Network and Computer Applications*, *32*(2), 388-401. doi: http://dx.doi.org/10.1016/j.jnca.2008.02.016

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233-244.

Wang, R., Chen, S., & Wang, X. (2012). Signing me onto your accounts through Facebook and Google: a traffic-guided security study of commercially deployed single-sign-on web services. *In Proceedings of the 33th IEEE Symposium on Security and Privacy*

APPENDIX A: FOCUS GROUP QUESTIONNAIRE

INTERVIEW QUESTION

Participant name (optional) :_____ **Group Number** :_____

PART 1 : PASSWORD MANAGEMENT		
1	How many user IDs and passwords do you have?	
	a. What types of applications do you need to use user IDs and passwords? (e.g. email, systems, etc.)	
2	How did you manage to remember all of your usernames and passwords if you have one?	
	a. How well it was?	
	b. What techniques to remember/keep many passwords?	
	c. What are the problems associated to keeping a number of IDs and passwords?	
3	Do you have any idea to improve the problems of having multiple user IDs and passwords to access multiple applications?	
	a. What would be your suggestions?	
	b. Do you think that the use of a single ID and password for accessing multiple applications is feasible?	
	c. Who should have the authority? What organization should manage user IDs and passwords?	

PART 2 : SINGLE-SIGN-ON		
1	Have you heard/used about single–sign-on (SSO)?	
	a. How do you think it work?	
	b. Do you think it is safe to access multiple applications through SSO?	
2	What kind of problems that user/you may come across when using the SSO in mobile environment?	
	a. Examples of problems? Breach of privacy (information is given to other persons), attack on ID and password by hackers in the central server, etc., server is not available, and access to other applications is suspended, etc.	
	b. How these problems can effects individual users like you? E.g., loss of access to important applications/ information, etc.	
3	What is your suggestion to improve SSO?	
	a. Do you have a better technique to improve the Id and password management?	

APPENDIX B: FOCUS GROUP TRANSCRIPT

INTERVIEW TRANCRIPTS

PART 1 : PASSWORD MANAGEMENT

Q1.
How many user IDs and passwords do you have?

Student A *: I have 2 user password*
Student B *: I also have 2*
Student C *: I have 3*
Student D *: I have 5*
Student E *: I have 3*
Student F *: I have 4 to 5 ids*
Student G *: I have 10 accounts*
Student H *: I have 7*
Student I *: I have 4 accounts*
Student J *: I have 3-4 accounts*
Student K *: I have 5*

Q1a.
What types of applications do you need to use user IDs and passwords? (e.g. email, systems, etc.)

Student A *: I have password for email, Facebook and file downloading which is 4shared.com*
Student B *: I share IDs and password for Facebook, Skype, Google and Yahoo*
Student C *: I use for gmail, yahoo and Facebook*
Student D *: I use for email, Facebook, Tonton, and online shoping*
Student E *: I use for Facebook and email*
Student F *: Used for email, Facebook, UUM portal*
Student G *: Facebook, Hotmail, Gmail, Yahoo, UUM portal and student email*
Student H *: Facebook, Twitter, Youtube, Learingzone,*
Student I *: Facebook, Hotmail,Gmail*
Student J *: For email, social network such as Facebook and Twitte, and for file sharing*
Student K *: I used for Fcaebook, email, and UUM portal*

Q2
How did you manage to remember all of your usernames and passwords if you have one?

Student A *: I used same username and password*
Student B *: I used first 10 digit of my IC*
Student C *: I used combination of number and character*
Student D *: I used same id and same password for all applications*
Student E *: I also used same ids and passwords*
Student F *: I used my best friend's handphone number*
Student G : I wrote down somewhere

Student H : Normally I used one username and password for two application
Student I : I used same id and same password for all
Student J : *No idea*
Student K : I used my father's and mother's name

Q2.a
How well it was?

Student A *: It is good so far*
Student B *: It is good*
Student C *: It is moderate*
Student D *: So far it is good*
Student E *: It I easy for me to remember*
Student F *: It good because it is combination of name and number*
Student G *: So far I don't face any issues*
Student H *:* I think it too simple
Student I *: No worry because I believe my password very strong*
Student J *: It is good because it is combination of numeric and character*
Student K *: So far I don't have any problem*

Q2.b
What techniques to remember/keep many passwords?

Student A *: Normally I use IC number*
Student B *: I used different IDs but same password*
Student C *: Normally I will use a name of my pet*
Student D *: Normally I use combination of numeric and character. It is about my self*
Student E *: I used my date of birth*
Student F *: I have no idea*
Student G *: Normally I will use my name and father's name*
Student H *: I use phone number to remember..sometime I use my house's phone number*
Student I *: I use phone number…easy for me to remember*
Student J *: I used name of movie*
Student K *: I save in my handphone*

Q2.c
What are the problems associated to keeping a number of IDs and passwords?

Student A *: I don't face any problem all this while*
Student B *: No problem*

Student C	*: I don't have any problem*
Student D	*: It is difficult to remember if I use different ids and passwords*
Student E	*: I don't have any problem at this moment*
Student F	*: Emmm…normally problem with the lost of username..it hard to recall*
Student G	*: I have no idea..i think no problem*
Student H	*: I don't have any problem because most of the password are same*
Student I	*: No problem so far*
Student J	*: I am sorry , I have no idea*
Student K	*: I don't have any problem*

Q3
Do you have any idea to improve the problems of having multiple user IDs and passwords to access multiple applications?

Student A	*: My suggestion is…maybe…emm..we can write down somewhere for example store in hand phone or diary*
Student B	*: In my opinion, use same IDs and psssword*
Student C	*: My suggestion is to used single sign-in*
Student D	*: I wrote down somewhere*
Student E	*: Err..emmm…no idea*
Student F	*: No idea*
Student G	*: No idea*
Student H	*: I have no idea..may be maintenance is important*
Student I	*: I have no idea*
Student J	*: May be we can consider to use biometric method*
Student K	*: I have no idea*

Q3.a
What would be your suggestions?

Student A	*: Same with the answer for question 3*
Student B	*: I would suggest to built own web application to link with other web application*
Student C	*: Same thing as I said just now*
Student D	*: Same thing*
Student E	*:It can be wrote down somewhere for example in diary or save I handphone*
Student F	*: I don't know*
Student G	*: Don't know*
Student H	*: May be you can write down somewhere..post to your email for example and it easy to retrieve*
Student I	*: Don't know..*
Student J	*: It is same question*
Student K	*: No idea*

Q3.b

Do you think that the use of a single ID and password for accessing multiple applications is feasible?

Student A	*: Not feasible*
Student B	*: Yes*
Student C	*: Yes, feasible*
Student D	*: Yes..it is feasible*
Student E	*: Yes*
Student F	*: Yes..it is feasible*
Student G	*: Yes feasible*
Student H	*: Yes feasible*
Student I	*: Yes..feasible*
Student J	*: It is feasible for some application..may be online banking is not suitable*
Student K	*: Yes feasible…I think feasible*

Q3.c

Who should have the authority? What organization should manage user IDs and passwords?

Student A	*: Your self should responsible*
Student B	*: Never*
Student C	*: Should be one trusted body to manage IDs and passwords*
Student D	*: No idea*
Student E	*: May be Suruhanjaya Komunikasi (SKMM)*
Student F	*: I think should engage with third party to organize the Ids and passwords*
Student G	*: No idea*
Student H	*: It depends on the usage*
Student I	*: it should be a government*
Student J	*: My suggestion is central information centre manage by government*
Student K	*: Develop your own system*

PART 2 : SINGLE-SIGN-ON

Q1

Have you heard/used about single–sign-on (SSO)?

Student A	*: I heard about SSO was 2 years ago*
Student B	*: Don't know*
Student C	*: Yes, like FB*
Student D	*: I never heard*
Student E	*: I never heard*
Student F	*: I just heard last week*

Student G *: I never heard*
Student H *: I never heard..this is first time I heard*
Student I *: I never heard*
Student J *: Yes*
Student K *: Never*

Q1.a
How do you think it work?

Student A *: It link with other server*
Student B *: I think it is secure*
Student C *: I guess with single sign in ID and password can navigate more application*
Student D *: No idea*
Student E : I don't know
Student F : just briefly
Student G : Of course I don't know because I never heard
Student H : No idea about that
Student I : Off course I don't know
Student J : My understanding is when we enter username and password, it will send a request to third party server for authentication
Student K : I don't know..i think it is a security system

Q1.b
Do you think it is safe to access multiple applications through SSO?

Student A *: It is not safe. Concern about third party*
Student B *: I have no idea*
Student C *: Yes..it safe*
Student D *: I think system performance will be slow*
Student E *: It is depends on application*
Student F : It is a new trend and I think it is safe
Student G : May be your device stole by someone
Student H : For me..it is 50-50
Student I : Quite safe may be
Student J : For some extend, I believe it is safe
Student K : May be safe

Q2
What kind of problems that user/you may come across when using the SSO in mobile environment?

Student A *: If using same PC. It have cache memory*
Student B *: For example if using smartphone and the phone is missing…so unauthorized person*

	may stole useful data
Student C	*: I don't have mobile device..so I don't know*
Student D	*: Don't know*
Student E	: I have no idea
Student F	: May be lost of device or someone borrow the device to their friend
Student G	: I am not aware about privacy all this while
Student H	: It is not safe when you leave your device anywhere
Student I	: May be same problem with my friends
Student J	: Someone can get access to your mobile device
Student K	: I think no problem

Q2.a

Examples of problems? Breach of privacy (information is given to other persons), attack on ID and password by hackers in the central server, etc., server is not available, and access to other applications is suspended, etc.

Student A	*: Errmm..i have no idea*
Student B	*: I have no idea*
Student C	*: No idea*
Student D	: No idea
Student E	: I never heard about this
Student F	: When you buy online..your identity will expose to the public
Student G	: Don't know
Student H	: *I don't know*
Student I	: Online banking … intrusion
Student J	: When you do online shopping, there will expose to system interception and personal information could be stolen
Student K	: For example..my email has been read by unauthorized person

Q2.b

How these problems can effects individual users like you? E.g., loss of access to important applications/ information, etc.

Student A	*: It will expose to cyber security*
Student B	*: For example …stolen of personal information could be misused*
Student C	*: Misused of personal information*
Student D	*: May be we don't have privacy*
Student E	*: No idea*
Student F	: It may be account intrusion
Student G	: Maybe it safe
Student H	: Will received private message…will disturb your life

Student I : Will disturb your life
Student J : Misuse of personal information
Student K : it too many..personal matter

Q3
What is your suggestion to improve SSO?

Student A *: It depends on organization…if campus student, university is the right authority*
Student B *: May be …can strengthen their security*
Student C *: Increase the security level*
Student D *: My suggestion is to use secret code*
Student E *: The web page should more secure, I meant to increase the security level*
Student F *: The third party should strengthen their system security to ensure the confidentiality*
Student G *: No idea*
Student H *: It depends on the organization how they measure the security issues*
Student I *: Make sure the service provider more secure*
Student J *: W must ensure nobody can access to a personal information*
Student K *: Must make sure all public Internet have good security*

Q3.a
Do you have a better technique to improve the Id and password management?

Student A *: Create own application with high authentication method*
Student B *: Can use same username and password for all application*
Student C *: For me, use same IDs but different passwords..it easy to remember*
Student D *: I don't know*
Student E *: My suggestion is every computer user must change their password every 6 months*
Student F *: Develop your own system is the better way*
Student G *: No idea*
Student H *:It I better to create your own SSO*
Student I *: Built your own program*
Student J *: Different password and different username is enough*
Student K *: No idea*

APPENDIX C: QUESTIONNAIRE FOR SURVEY

SECTION 1. DEMOGRAPHIC INFORMATION

Instruction: Please answer the following questions about yourself.

1. What is your gender?
   - ☐ Male
   - ☐ Female

2. What is your age?
   - ☐ 18 – 20
   - ☐ 21 – 25
   - ☐ 26 – 30
   - ☐ 31 and above

3. What is your race/ethnicity?
   - ☐ Malay
   - ☐ Chinese
   - ☐ Indian
   - ☐ Other (please specify): _____

4. What is your nationality?
   - ☐ Malaysian
   - ☐ Other (please specify) : _____

5. What is your program of study?
   - ☐ Undergraduate (please specify) : _____
   - ☐ Postgraduate (please specify) : _____

6. What is your current semester?
   - ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

SECTION 2. INTERNET MEDIUM AND BEHAVIOUR

Instruction: Please answer the following questions on your Internet usage

1. Do you have mobile or wireless device such as tablets (i.e. iPad, Samsung Galaxy Tab, etc.), smartphones, netbooks or any other mobile devices that use to browse Internet?
   - ☐ Yes
   - ☐ No

2. How many devices do you have?
   - ☐ 1 (please specify device product) : _____
   - ☐ 2 (please specify device products) : _____
   - ☐ > 3 (please specify device products) : _____

3. How often do you browse Internet?
   - ☐ Daily
   - ☐ Once a week
   - ☐ A couple of time a month or less
   - ☐ Other: _____

4. How long have you used the Internet?
   - ☐ Less than 6 months
   - ☐ 6 months to 1 year
   - ☐ 1 to 2 years
   - ☐ > 2 years

5. How many hours per day, on average, do you connect to the Internet?
   - ☐ Less than one hour a day
   - ☐ 1 – 2 hours
   - ☐ 2 – 3 hours
   - ☐ 3 – 4 hours
   - ☐ > 4 hours

6. What do you like to do with the most online?
   - ☐ Chat rooms
   - ☐ Social networking (Facebook, Twitter)
   - ☐ Music
   - ☐ News
   - ☐ Instant Messenger (YM, MSN etc)
   - ☐ Blogging
   - ☐ File sharing
   - ☐ Web browsing
   - ☐ Gaming
   - ☐ Other (please specify) : _____

7. Where do you access the Internet from?
   - ☐ Hostel room
   - ☐ Computer Labs
   - ☐ Library
   - ☐ Cafeteria
   - ☐ Other: _____

SECTION 3. SINGLE-SIGN-ON EXPERIENCE

Instruction: Please answer the following questions on your single-sign-on experience

1. Have you heard about "Single-sign-on" or SSO?
   - ☐ Yes
   - ☐ No
   - ☐ Don't know

2. Since you are using computer, how many login id and password do you have to remember? (Please indicate number, e.g. 1, 2, 3, etc.)
   a. Email account? : _____
   b. Web login? _____
   c. Network login? _____
   d. Other : _____

3. Do you have prior experience using a single copy of a username and password to access different multiple applications?
   - ☐ Yes
   - ☐ No
   - ☐ Don't know

4. How long is your password length (in characters)? _____

5. Have you used same id and password for login in different applications?
   - ☐ Yes
   - ☐ No
   - ☐ Don't know

6. Do you have your usernames and passwords written down on paper or book which hidden somewhere?
   - ☐ Yes
   - ☐ No
   - ☐ Don't know

7. How frequent do you change your password?
   - ☐ Once a month
   - ☐ Once a week
   - ☐ Never
   - ☐ Once every 6 months
   - ☐ Once a year

8. Have you shared your passwords and your mobile devices with your friends/family members?
   - ☐ Yes
   - ☐ No
   - ☐ Don't know

9. How often do you have to reset your password due to forgetting or time requires you to change?
   - ☐ Once a week
   - ☐ Once a month
   - ☐ Once every 6 months
   - ☐ Once a year
   - ☐ Never

10. Do you believe that single-sign-on can simplifies your authentication process (e.g. easy for systems to identify yourself)?
    - ☐ Yes
    - ☐ No
    - ☐ Not sure
    - ☐ Don't know

11. Do you believe that single-sign-on can increase the security of systems?
    - ☐ Yes
    - ☐ No
    - ☐ Not sure
    - ☐ Don't know

12. Do you know/aware about the existence of a public SSO provider such as OpenID, SAML etc?
    - ☐ Yes
    - ☐ No

13. If you encounter a website that supports third-party account for log in, will you use your existing account for example from Google, Yahoo, Hotmail or Facebook to login?
    - ☐ Yes, because _____
    - ☐ Depends on which website I am logging into, because _____ _____
    - ☐ Don't know, because _____

SECTION 4: SECURITY AND PRIVACY

Instruction: Please answer the following questions on the security and privacy issues

1. How concerned are you about privacy of information (such as name, address, credit card number) given over the Internet
   - ☐ I am **less** concerned about privacy on the Internet
   - ☐ I am **somewhat less** concerned about privacy on the Internet
   - ☐ I am **more** concerned about privacy on the Internet
   - ☐ I am **much more** concerned about privacy on the Internet

2. How important is your consent when Sites sell/share your personal information with others?
   - ☐ Very important
   - ☐ Somewhat important
   - ☐ Neutral
   - ☐ Somewhat unimportant
   - ☐ Unimportant

3. Have you been asked to provide personal information at web sites you visit?
   - ☐ Yes
   - ☐ No

4. Would you give your personal information to a particular website if you were asked to do so?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

5. Would you give incorrect (fake) information about yourself to a particular website if you were asked to give your personal information?
   - ☐ Yes
   - ☐ No
   - ☐ Not sure

6. Would you be more willing to provide personal information for online advertising purposes if the website compensated you for your information?

- ☐ Very willing
- ☐ Somewhat willing
- ☐ Not very willing
- ☐ Not willing at all

7. Do you ever read the terms of web policies when you are asked to provide your personal data into the web sites?
   - ☐ Yes, because _____
   - ☐ No, because _____

8. Have you been contacted by strangers because of the personal data you posted on the internet?
   - ☐ Yes
   - ☐ No
   - ☐ Forgotten

9. If you place your personal data on the internet, will you be concerned that many people can view it?
   - ☐ Yes, I am concerned that many people can view it
   - ☐ No, I am not concerned that many people can view it

10. Have you taken any internet security measures to protect your personal data?
    - ☐ Yes
    - ☐ No
    - ☐ I do not know how to set security