Jurnal
Teknologi

Full Paper

A CAUTION IN SOCIALIZATION: A PRELIMINARY IDENTIFICATION OF PERSONAL SECURITY JEOPARDIZING HABITS AMONG SOCIAL MEDIA USERS IN MALAYSIA

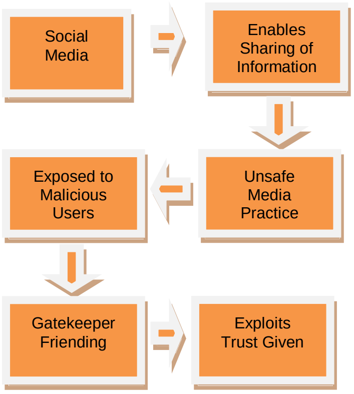
Md. Nabil Ahmad Zawawi

Centre of Information and Network Security, College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia

*Corresponding author
mdnabil@uniten.edu.my

Article history
Received
15 May 2015
Received in revised form
1 July 2015
Accepted
11 August 2015

Graphical abstract



Abstract

Social media is playing an important role to most people these days. People are using it to be connected among peers, updated with the latest information and also for e-commerce purposes. However, apart from its benefits there are others who would use the information obtained from social media in a malicious way such as harvesting personal information for black mailing, information manipulation and tele-marketing. This threat coupled with unsafe social media practice could expose the social media users to being manipulate into sharing sensitive and revealing information about them. In this paper, a preliminary investigation to identify distinct characterizations of unsafe social media habits is presented. For this study, we focused on one particular social engineering attack known as gatekeeper friending. In this attack, a would--be attacker or manipulator of information could exploit information shared over a social network and how an unsafe social media habits could expose its users to such attacks and exploitation. By identifying this habits we hope that a more secure and cautious code of conduct could be established to prevent unwanted disclosure of private information for malicious intention.

Keywords: Social media ethics, information security, personal information, privacy issues

1.0 INTRODUCTION

The use of social media is a norm these days. Taking Malaysia into account, in 2014, we have [2] 64 percent of population already connected in the social media and we have about 15,600,000 Facebook users in the whole country from 19,200,408 overall Internet users. Twitter [3] on the other and has 3,500,000 users with 760,000 of them are active users. These social networking platforms users comprises of teens, young adult, media and also political figure which utilizes the strong reach factor towards its target audience. However with the rise of this trend of social networking, there seems to be an increased of online security threats as a result of [4] cyber stalking and social engineering from social media sites. Most victims are usually unaware of risking their personal information while sharing online. The illusion of having a close circle of friends resulted in a reckless sharing of routine, location and other information that usually is not disclosed to strangers. A social experiment as demonstrated in [7] shows that in a social media network, most people are not really worried when sharing private information compared to when sharing the information in real life to complete strangers. What most people accept in the real world setting as unsafe and risky are treated differently when it was done online. These lack awareness or abandonment of personal safety are one of the concern discussed by Putchala *et al.* [4] and Jaakkola *et al.* [5]. Information carelessly shared over the social media could be used for profiling individuals and even the organization they are working for. Aside from monetary loss there are also other personal security risk such as disclosure of private information, home information, children location and whereabouts and daily movement routine. Organization's trade secret and practice are also at risk of being disclosed. This paper examines the current practices of social media user in Malaysia which could contribute to personal security breach and monetary losses related to the risks involved. The demographic for the study involved participants from age group ranges from 18-40 years of age with the purpose of understanding if their basic social media practices are related to those that is endangering to their own personal safety.

2.0 GATEKEEPER FRIENDING

One of the most common security threats but always dismissed by most users of social media is an approach known as [6] gatekeeper friending. In other term, gatekeeper friending is also known as social engineering [7]. The attack exploits one of the most basic human traits; trust. The approach consists of non technical steps whereby the assailant attempts to gain access to information specifically targeted to the victim. Most of the time, victims are identified to be employees or individual possessing information crucial to the attacker's causes. These cause ranges from monetary, personal secrets or possession and also organizational assets which the victim works for. The attack consists of the following steps:

1. Identifying the victim.
2. Penetrating the victim's circle through the disguise of sharing the same interest, organization, alma matter and goals.
3. Befriending the victim.
4. Establishing connection and trust.
5. Gathering personal information through what the victim openly shares to individuals he/she considered friends.
6. Exploiting the information for criminal intention.

In order to mask their malicious intention, the attacker's account is comprised of a fabricated personality made up of well planned list of followers or friends. The attackers will always try to mask their intention by masquerading as some with a friendly personality and uses fake collection of user images which will be thought of belonging to that friendly persona. Once the trust is established, the attacker can then manipulate his or her target to disclose information.

3.0 THREAT OF TRUST

Social media enables its user to have more access to information. However, this is a two way scenario. While its user could gain access to information, malicious users are exploiting the access to misuse it. Among possible outcome includes (but not limited to) possible leak of corporate or organizational information, information mining and other type of information breach.

What is more worrying about this type of threat is that it does not require any technical skills to do it. Any individual with the basic knowledge of setting up a social media account is able to do it. According to a study by security week [9], when connected to an active social media account, each employee, customers, executives and individuals connected to the target organization are the endpoints for a gatekeeper friending threat. Social network provide the illusion of safety among individuals which whom there are virtually friends with. Once the trust is successfully fabricated, the attacks (either stealthily or direct), could commence.

The victim could be encouraged by the attacker to voluntarily share personal information through the form of innocent games, exchange of personal information and daily routines.

These types of seemingly innocent and routine information could be used to exploit the users vulnerability. Children's information, home address, school address, birthdays and parents information are among the things most people are mistakenly sharing without understanding the security impact of that information.

4.0 MALAYSIAN SOCIAL MEDIA PRACTICE

This section explains the core of the paper which is to investigate the social media practice among Malaysians. The objective of the investigation is to identify unsafe social media practice which could potentially be exploited by gatekeeper friending. As previously discussed, these types of attack are targeting unsuspecting users by exploiting the connection of trust the attacker managed to establish. These exploitation could stem from the very beginning when a connection is attempted followed by the assailant harvesting information regarding the target's information and daily routines. Therefore, it is important to identify types of online behavior which can lead to opening the gate to access in the first place. Other than that, we investigate the motivation on the sharing behavior from our respondents to find out what causes individuals to willingly share that much amount information on their channel.

4.1 Our Survey Setup

Our survey demographic ranges from the age of 15 years old to 35 years and above. This group signifies the generation X and Y which are distinct in their experience of the Internet and social networking. We distributed survey questionnaire to be filled by our respondent indicating that the survey is to study their general behaviour in social media without stressing on the safety issues at hand. The objective at this point is just to find out, what people do with their social media account, how do they get connected and why they share information on their channel. The survey asked each of our respondent starting from their gender followed by their age group. The questionnaire then proceeds on finding out their social friends' criteria and characteristics. The scope of investigation then delves further into types of information shared with their supposedly online friends and the reasons for sharing that information. The question of the survey was constructed based on the premise presented [6], [7] and [9].

4.2 Collected Data Interpretation

For this section we compiled the responses we obtained from the study and observe some of the traits of an unsafe social media practices adopted by our respondents. The part which interest us the most for this survey is how our respondents react in situations where they have a friend or link request from a total stranger. We aim to find out factors which motivate users to accept a friend request from a total stranger. Table 1 listed the questions and the response related to this factor. As the table illustrate, sharing a mutual friend with the stranger simplifies the decision process, followed by an initial personal messaging attempt prior to the request and of course the physical traits portrayed in the stranger's profile picture.

Table 1 Factors of Accepting a link request

Entry	Factors for accepting a link or friend request	Percentage
1	Mutual friends in the same circle	53.1%
2	The interested party messaged them of the interest	27.6%
3	The physical look of the interested party	11.2%
4	No special reason but just to have more friends in their profile	8.2%

Our next investigation was to find out the type of information normally shared on our respondents' channel. Almost all of them (71.4%) revealed that they constantly share their routine activity on their channel followed by information on charity drive (20.4%) and politics (7.2%). The summary for the information are compiled in Table 2 below.

Table 2 Information Shared on their profile

Entry	Information Shared on their profile	Percentage
1	Routine Activity	71.4%
2	Charity Drive	20.4%
3.	Politics	7.2%
4.	Other	1%

After that, we dig further on finding out the reason why they actively share those information on their channel as depicted in Table 3. First and foremost we have discovered they agree that it was driven from the fact that they felt it draws out good conversation topics from their peers (38.8%), followed by the commonality of the things shared by their friends (30.6%) and the attention they managed to draw from the material they shared on their channel (19.4%). This commonality and social acceptance factor seems to be the reason why most users depicted by our respondents seemed readily available or committed to share whatever information they have inside their virtual social circle. If the entry was well received, there are tendencies to repeat the information sharing to get future acceptance.

Table 3 Sharing Motivation

Entry	Motivation on sharing information	Percentage
1	Draws out good conversation topics	38.8%
2	Common things shared by mutual friends	30.6%
3.	Prefer the attention obtained	19.4%
4.	Other	11%

When we probe further our investigation based on their age group starting from those from age 15-24 years of age, we attempt to find out other type of information that was also shared on their page. 89% of our respondents in this group openly disclosed their school or college information on their social channel. Other than that we have also found out that from the overall school or college related information shared on their channel, 46.4% of them admitted in sharing most of their daily activities in school apart from exams related event (25.8%) and also something notable such as their daily commute to school and college (20.3%) as shown in Table 4. These types of information could be exploited by individuals with criminal intention which actively studying their victims routine activity to see where and when the individuals will be at one particular time for a particular day.

Example of such cases are presented in studies [3], [5] and are not mere assumptions on how these criminals are doing there criminal activity by exploiting information easily obtained over the social media.

Table 4 Activities Shared

Entry	School / College Related Activities Shared	Percentage
1	Daily school activities	46.4%
2	Examination information	25.8%
3.	Daily commute to school / college information	20.3%
4.	Other	7.5%

Aside from that, for group of respondents ranging from age 25-34 our investigation found that 51.2% of them have their work information displayed on their social channel. Work information are information which states their occupation, work organization and even their job position.

For the group, we discover that most of them publicly shared office related event (56%), followed by their commute to work (33%) and anything that happen during their time at work.

It is also interesting to note that for both of this group, the responses indicate that they also share their family activities on their channel which consists of vacationing activity (73%), family outings (65.3%) and also weddings or special occasions such as birthdays or anniversary (86%).

5.0 SUMMARY OF FINDINGS AND CONCLUSION

Our preliminary findings indicate that in most cases, Malaysian social media users could be exploited and manipulated if they are still careless and not cautious on the individuals they add and the information they publicly share on their social network. It must be made clear that sharing information with regard to daily activities at work, college and schools should be done with caution since these information could endanger the individuals in terms of making it easy for criminals to use the information the read daily routine, personal and also private family information.

As of this point of the study, we have collected enough data to begin the next phase of simulating a scenario whereby an attacker could try and manipulate a social media account owner to willingly share other information through private messages and personal one to one chatting conversation.

6.0 UPCOMING WORK

The next step in our study of Malaysian social media habits is to have a controlled experiment whereby we will attempt to simulate a *gatekeeper friending* scenario on a group of targeted respondents and perhaps find out whether what was claimed in [4] and [6] could actually happen if the rules of engagement are closely followed. What we hope to gain from the experiment is attempt to prove whether users can be manipulated to share certain important information which could jeopardize their privacy.

Acknowledgement

We are grateful for all the respondents of this preliminary study ranging from teens, young adult and to working adults in Malaysia.
We also wish to thank Universiti Tenaga Nasional for providing the initial fund and support to perform this study.

References

[1] Suruhanjaya Komunikasi dan Multimedia. 2013. MCMC Annual Report 2013.

[2] Kemp, S. 2014. 2014. Asia Pacific Digital Overview. Retrieved January 15, 2014, from Wearesocial.net.

[3] Junior, D. 2015. Malaysia Social Media Statistic 2014. Retrieved March 2, 2015 from http://blog.malaysia-asia.my/2015/03/malaysia-social-media-statistics-2014.html.

[4] Putchala, S. K., Bhat, K. and Anitha, R. 2014. Information Security Challenges in Social Media Interactions. *British Telecommunications Engineering*. 17: 291-295.

[5] Jaakkola, H., Linna P., Henno. J. and Makela, J. 2011. (Social) Networking is Coming–Are We Ready? *MIPRO 2011, May 23-27, Opatija, Croatia.*

[6] Foster, J. 2015. A Match Made in Heaven: Fraud and Social Media. Security Week.

[7] D'onfro, J. 2015. Strangers on the Social Media. Business Insider. Retrieved November 19, 2013 from http://www.businessinsider.com/jack-vale-social-media-experiment-2013-11?IR=T&.

[8] Prince, B. 2009. Using Facebook to Social Engineer Your Way Around Security. E-Week Editor's Pick. Retrieved June 17, 2015 from http://www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook-277803

[9] Foster, J. 2015. A CISO's Nightmare: Digital Social Engineering. Security Week.