A Review on Social Media Issues and Security Awareness among the users

Nor Azlina Abd Rahman
Faculty of Computing, Engineering & Technology
Asia Pacific University of Technology & Innovation
57000 Kuala Lumpur, Malaysia
nor_azlina@apu.edu.my

Fauziah Permatasari
Faculty of Computing, Engineering & Technology
Asia Pacific University of Technology & Innovation
57000 Kuala Lumpur, Malaysia
fauziah.p@mail.com

Yuni Hafsari
Faculty of Computing, Engineering & Technology
Asia Pacific University of Technology & Innovation
57000 Kuala Lumpur, Malaysia
yunihafsari158@gmail.com

Abstract - This paper is reviewing on several issues faced by the users of social media especially users of Facebook and Twitter which are the most popular social media networks based on statistic provided by Statista. Some of the issues that being discussed are information theft and image misused due to no privacy setting set by the users to their social media accounts. The use of social media aggregator will lead to the hackers to easily access to all the Social Medias that are link together. Lack of security awareness among the social media users will exposed them to many cyber-crime activities. Several countermeasures are being discussed such as to improve the privacy setting of the social media, controlling the social media authorisation and increase the security awareness among the social media users. Other actions that can be taken to protect the social media accounts are by disable the connection between the infected accounts with other accounts by changing the registered email information on the unaffected accounts. Changing passwords could help to slowdown the hacker's activities and the last option that can be considered is by reporting and issues the social network's customer service

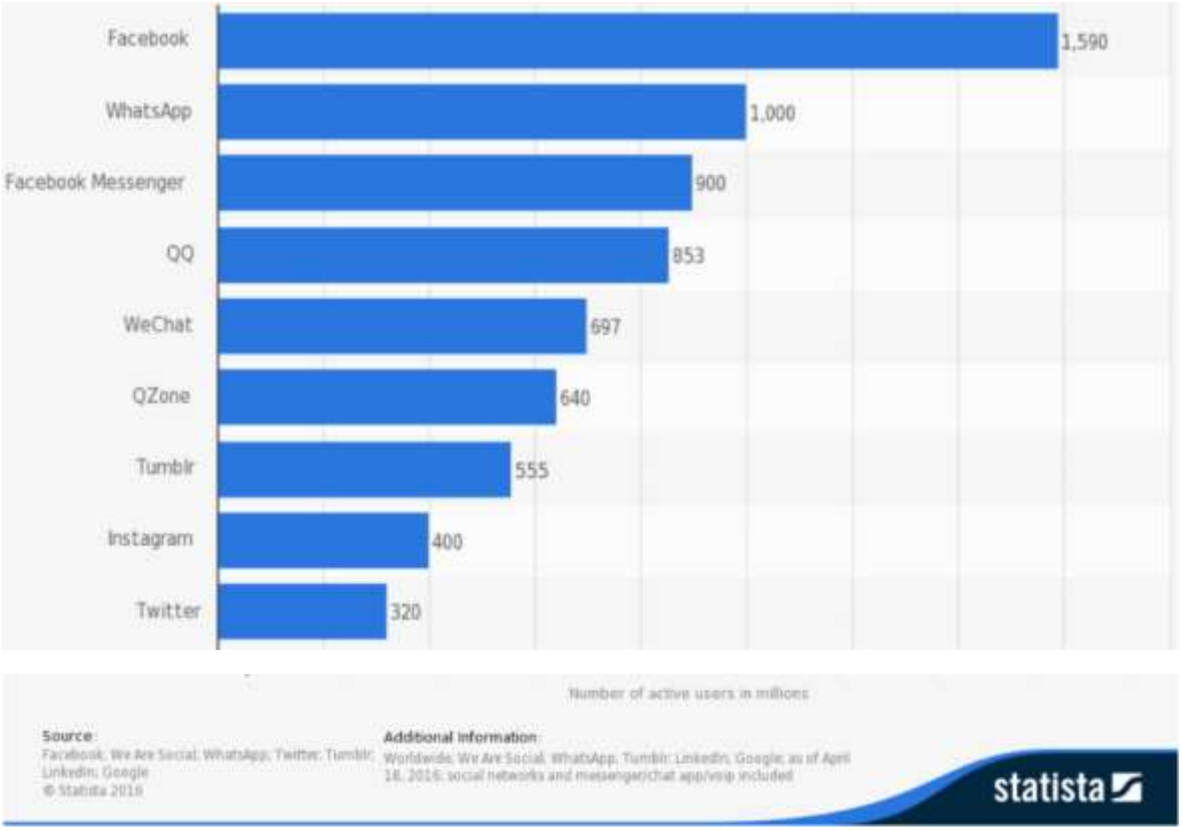
Index Terms – cyber security; social media; facebook; twitter; wikipedia; phishing

1. Introduction

Social media and its user has a relationship that is affected with cyber security and its environment. As the social media use explodes, this relation also becomes more intense as cyber criminals expand their hunting area and start to have their eyes on the social media accounts. Social media users are becoming one of their targets as most of the social media users are lack of knowledge and awareness in security and privacy that can be implemented to individuals account.

Social media nowadays have played a crucial part of people's daily life. Based on Fig. 1 showed that in 2016 Facebook had over 1,590 million active users while the Facebook-owned WhatsApp and Instagram had 1,000 million and 400 million respectively [1]. This clearly proved that social media has become more popular nowadays and this further proves that Social Media users have reached a significant number to be influential, and makes them even more vulnerable as hacking victims.

In this paper, Facebook and Twitter users are the main focus of discussion, considering that these two social networks are wide-spreading rapidly, as proven by the GlobalWebIndex Wave 11 that reported Facebook and Twitter have the highest penetration rates with 93 percent of Internet users owning a Facebook account, and 72 percent of them are a Twitter account holder [2].



Source:
Facebook; We Are Social; WhatsApp; Twitter; Tumblr; LinkedIn; Google
© Statista 2016

Additional Information:
Worldwide; We Are Social; WhatsApp; Tumblr; LinkedIn; Google; as of April 18, 2016; social networks and messenger/chat app/voip included

Fig. 1: Survey result of leading social media users as of April 2016 [1].

In relation with the rise of Internet popularity around the world, it especially has become even more popular amongst teenagers [3]. Based on Fig. 2, Social media users' number have significantly risen for the past few years both for adult and teen users. In 2008, 73% of American teens had been using social networking websites, an increase of 20% compared to the survey on 2006 [4].

Most of these teenager social media users are students whom the global environment changes had significantly affected them both academically and socially. These teenagers and young adults are clueless regarding their privacy settings. Since teenagers and young adults are more concerned on relishing the opportunity to link themselves to others and create authentic relationships, they want to express their identity and take the risk of exposing themselves to being discovered and come into contact with hackers [5] [19].

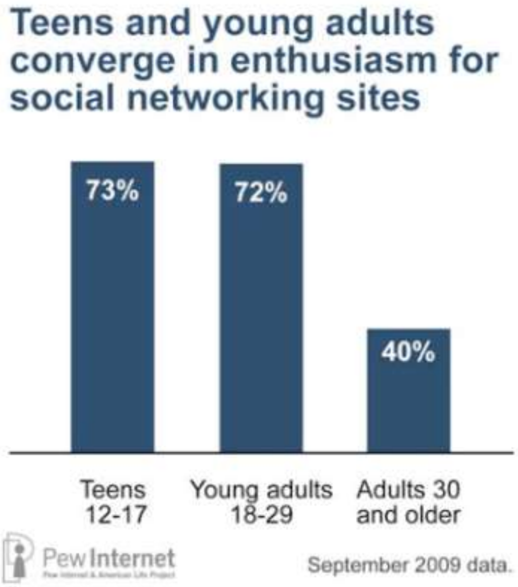


Fig. 2: Graph of American teenagers, young adults, and adults' use of social media [4].

2. Issues faced by social media users

In terms of personal security, users have done several activities that put them face to face with the risk of being a cyber-crime victim. Some of these social media users are digging their own grave in the case that they are exposing themselves toward the cyber-crimes and privacy leakage risks. The activities that they did on social media may seem trivial when actually it is significant in helping them to be one of a hacker's victims [6]. There are several issues that faced by the social media users which are:

2.1 Lack of social media privacy setting

Most of the users of social media are not really aware the importance of their social media privacy setting. Teenagers and young adults, are the most prone of being nonchalant regarding their social media privacy setting. According to Livingstone's research result (2008), teenagers' main use of social media is taking risky opportunities in youthful content creation by expressing themselves and intimacy. One example of a cyber-crime that is resulted by this lack of privacy setting is identity thievery. A related case as reported by The Telegraph [7], a 27-year-old woman in London, UK, had her Facebook profile pictures and identities stolen and they were being used as a fraud in an online dating social media. This gave her many social disadvantages as it would stain her professional reputation along with her relationship.

2.2 The use of social media aggregator

In relation to the first point, as the number of social media users grows, then so does the percentage of social media users who actively use different social network sites. This leads to the second activity on which users are easing hackers to discover them. Since the users are maintaining multiple social networks for their personal uses, they often link each of the social network account authorization to each other, or use the same password for different account [8].

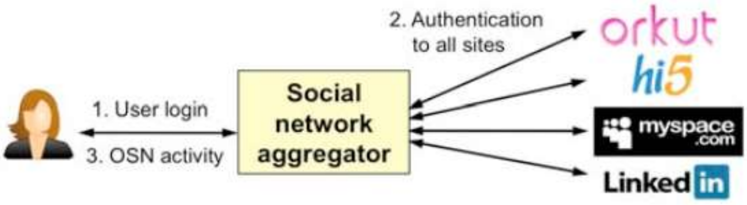


Fig. 3: Example of how a user links their social media accounts altogether [9].

As for the hackers, this can be said as heaven-sent target. They can easily gain access to multiple account just by gaining access to one of the person's many accounts. This is called as social network aggregator. Fig. 3 showed how the social network aggregator works when a platform is used to pull content from multiple social media into a single location and dispersing it to different profiles more conveniently. Although it is eases users on monitoring their social media accounts, it is relatively unsafe [9]. Considering hackers will be able to discover all of their other accounts once one of them has been compromised, putting other accounts on huge risk.

One example of this is the latest case with Facebook's founder, Mark Zuckerberg. A group of hackers has successfully gained access to his Twitter and Pinterest account using his LinkedIn credentials which had been leaked in a prior huge data loss of LinkedIn user information [10]. Even a person who is as sophisticated as Mark Zuckerberg in information technology and cyber industry, is a victim of such hacking activity. It opened many people's eyes on how vulnerable their social media accounts are.

2.3 Insufficient information about cyber crime

Insufficient information about cyber security can also be an issue to these teenagers and young adults. Due to the unawareness of the importance of the security implementation, makes them unaware of incidents of accounts being compromised which are happening around them.

Social engineering attacks may not sound as sophisticated as other methods of hacking, but in fact, it has some of the most successful attempts carried on targets. A report by Symantec (2016) showed that some of the attacks and tactics executed by these cybercriminals have deliberately proven how vulnerable the Internet users are online.

Social media especially took the number one spot of scamming target, as criminals seek to gain people's trust by having them in their social circles therefore these hackers would be able to spread scams, fake links, and phishing. An example of this case is Mocking birds, which is where thousands of fake Twitter accounts are made to gain branch boosting, get followers, and having retweets from legitimate Twitter users. This creates even more possibility of phishing cases to happen. While according to BofA Merrill Lynch Global Research, cybercrime already costs the global economy up to US$575 billion annually [11].

On December 21, 2016, U.S. Netflix's Twitter account was hacked by OurMine, a hacker group which has been known for hacking into several high-profile social media accounts and popular websites [12]. Some of its victims include Twitter and Vine co-founder Google chief executive Sundar Pichai, Wikipedia co-founder Jimmy Wales, Forbes, Buzzfeed, and Techcrunch. These people are in no way amateurs in information technology and its cyber security. However, in the latest case on which Netflix was compromised, OurMine shared that it gained the access of some Netflix accounts by hacking into its Director of Social Media who apparently had not changed its LinkedIn password post the recent user information leakage [13] [20].

These little things that some people may find as insignificant, can lead them to a chain reaction and result in a big loss. Netflix gains people's frowns and questions on its take on security and safety of its users' privacy. Because social media is a persona that people and organizations want the industry and the society to view them as. Social media has become a part of people's daily life; it now holds more worth than how it used to be just ten years ago, a fact that definitely is noticed by irresponsible parties such as hackers.

3. Countermeasures

In this section, countermeasures are discussed to avoid and prevent exploitations on personal social media accounts. Besides that, the recovery plan for attacked accounts will also be suggested in order to prevent further damage. Several countermeasures that can be considered are as the following:

3.1 Improve privacy setting

There are numerous security implementations that social media users can do to prevent cases mentioned above. For the first point on which social media users are not paying attention toward their privacy settings, countermeasures can be done both on their social network sites and their internet browsers.

Nowadays social networking sites have sufficient privacy settings which its users can adjust and customize based on their level of comfort. Users can set some of their identity information on private to be viewed only by selected users. As an example, is Facebook that upgraded its privacy profile privacy setting [14] to enhance the security.

Facebook allowed people to manage their privacy settings in different granularities, making it easier for the users to choose to whom they are sharing their profile content with. Even so, users are advised to keep their awareness on everyone because hackers can also be someone they are close with. Therefore, another tip that need to consider to ensure the security of the social media users are by avoiding sharing everything of their daily life to the internet [15].

Meanwhile for their browser, users can set its privacy setting to prevent the use of cookies and block pop-ups. In several browsers, they also have a location setting which the user can turn off too. This will lessen the risk of users to be exposed to much more contact with irresponsible parties.

3.2 Control social media authorisations

The users of social media should not use any social network aggregator or not to connect their social media accounts altogether. It may seem difficult to some social media users who already had their social network accounts linked to each other. Nevertheless, they can still set a different password for each of their social media account to decrease the risk.

The passwords used for each social media should be strong, meaning that it should consist more than six characters with upper case letters and numbers mixed in it. Make sure that the password is not of a common word or saying. This can prevent hackers to crack a users' account. Hackers are able to crunch and automatically run a tool which can generate a dictionary of commonly used phrases for passwords to crack a social media account.

3.3 Increase awareness of latest cyber security issues

Social media users have to kick their bad habits and start to safeguard against social engineering and even the cybercrime in general. They have to be more aware of the cybersecurity events and news. Also, they have to implement the good cybersecurity basics starting by themselves.

For the Twitter users, they have to be more cautious in choosing the people they want to follow or they want to approve of. They have to be sceptical for each of their new followers, to prevent of getting spammed by bots. And they also have to pay more attention on the 'verified' badge when they want to follow certain accounts.

4. Recovery Plan

It is very important to have a recovery plan as it will cover the steps to take after the social media has been hacked to prevent any more loss from happening. Specifically, for an individual whose professional work revolves around their social media use, which as stated before, their social media accounts are a persona to them, they need to consider on cooperating with an expert of the field. How to do the damage control and recover from such a state [16].

The crisis shall be divided into several levels depending on the damage impact. Every impact will require different response action, based on the situation. Some crisis communication exercises and scenarios can also be planned within the recovery plan, in order to help the crisis handlers to be ready whenever a crisis happens [17].

One example of things to consider listed in personal social media protection is by taking an immediate action to change other social media accounts' passwords. This relates to the social network aggregation in which when a hacker has gained access to one of a user's accounts, he might have access to other accounts as well. Changing other accounts' passwords will help minimizing the risk.

Then, if it is possible, disable the connection between the infected social accounts with other ones. This can be done by changing the registered email information on the unaffected accounts, and users are also encouraged to report the case to the social network's customer service.

5. Conclusions

Modern technologies help us a lot in communication nowadays. Based on research and statistic that has been discussed above, social media become one of the popular communication media among teenagers and young adults. Lack of security awareness among the users lead to many security issues such as information theft, image misused and others. Hence the users have to pay more attention on how they access and manage their accounts [18]. This is quite often when the little things which are insignificant to them, may lead into a much bigger reaction which can put them in risk. They also have to be in touch with the latest news and findings about information and cyber security issues. By being update regarding those, the social media users can adapt themselves to the situation and be more knowledgeable on cyber security and protect themselves. Social media is part of people's image in the society nowadays and a compromise in these accounts can cause damages toward the victims.

Acknowledgments

The authors wish to express gratitude to the management of Asia Pacific University for their support.

References

[1] Statista, (2017). The most popular social networks worldwide [#ChartoftheDay] - Smart Insights Digital Marketing Advice. [online] Smart Insights. Available at: http://www.smartinsights.com/digital-marketing-strategy/popular-social-networks-worldwide-chartoftheday/ [Accessed 8 Jan. 2017].

[2] Global Digital Statistics, (2014). GWI Social Summary. GWI Quarter Report. [online] Global Web Index. Available at: http://insight.globalwebindex.net/hs-fs/hub/304927/file-2377691590-pdf/Reports/GWI_Social_Summary_Q4_2014.pdf?submissionGuid=d75c46ce-922c-4efc-8ac3-08dbe9ba4904 [Accessed 1 Feb. 2017].

[3] Bennett, S., Bishop, A., Dalgarno, B., Waycott, J. and Kennedy, G. (2012). Implementing Web 2.0 technology in higher education: A collective case study. 1st ed.

[4] Lenhart, A., Purcell, K., Smith, A. and Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. In: ERIC, 1st ed. Pew Internet & American Life Project.

[5] Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media & Society, 10(3), pp.393-411.

[6] Marwick, A. and Boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), pp.1051-1067.

[7] Gammell, K. (2017). My Facebook profile was stolen to get dates on Tinder - and there's nothing I can do. [online] Telegraph.co.uk. Available at: http://www.telegraph.co.uk/women/womens-life/11588667/Facebook-identity-theft-My-profile-was-stolen-to-get-dates-on-Tinder.html [Accessed 8 Jan. 2017].

[8] Lewis, K., Kaufman, J. and Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of Computer-Mediated Communication, 14(1), pp.79-100.

[9] Benevenuto, F., Rodrigues, T., Cha, M. and Almeida, V. (2012). Characterizing user navigation and interactions in online social networks. Information Sciences, 195, pp.1-24.

[10] Hern, A. (2017). Mark Zuckerberg hacked on Twitter and Pinterest. [online] the Guardian. Available at: https://www.theguardian.com/technology/2016/jun/06/mark-zuckerberg-hacked-on-twitter-and-pinterest [Accessed 8 Jan. 2017].

[11] Symantec, (2016). 2016 Internet Security Threat Report. Internet Security Threat Report. [online] Symantec Corporation. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [Accessed 1 Feb. 2017].

[12] BBC News. (2017). Netflix US Twitter account hacked - BBC News. [online] Available at: http://www.bbc.com/news/technology-38390343 [Accessed 8 Jan. 2017].

[13] Schroeder, S. (2017). Hacker group OurMine has compromised another high-profile social media account. [online] Mashable. Available at: http://mashable.com/2016/12/21/netflix-twitter-hacked/#7BnKhHU70mqE [Accessed 8 Jan. 2017].

[14] Liu, Y., Gummadi, K., Krishnamurthy, B. and Mislove, A. (2011). Analyzing facebook privacy settings. Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference - IMC '11.

[15] Harkins, M. (2013). Managing risk and information security. 1st ed. [New York]: Apress.

[16] Pensa, R. and Di Blasi, G. (2017). A centrality-based measure of user privacy in online social networks. 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), (2016-08), pp.1438-1439.

[17] Ryan, D. and Jones, C. (2012). Understanding digital marketing. 1st ed. Philadelphia, PA: Kogan Page.

[18] Chu, S. (2011). Viral Advertising in Social Media. Journal of Interactive Advertising, 12(1), pp.30-43.

[19] Charlesworth, A. (2015). An introduction to social media marketing. 1st ed. London [England]: Routledge, p.209.

[20] Cross, M. (2013). Social Media Security: Leveraging Social Networking While Mitigating Risk. 1st ed. Newnes.