International Journal of Engineering & Technology, 7 (4.15) (2018) 109-112

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cyber Harassment Trends Analysis: a Malaysia Case Study

Sharifah Roziah Mohd Kassim*, Wira Zanoramy A. Zakaria*, Faiszatulnasro Maksom, Kilausuria Abdullah

MyCERT, Cybersecurity Malaysia, Selangor, Malaysia
**Corresponding author E-mail: roziah@cybersecurity.my, wira@cybersecurity.my*

Abstract

Each year, Malaysia Computer Emergency and Response Team (MyCERT) handles more than a hundred incidents of individuals and organizations being harassed online. A common platform for the harassment activities to take place is via social networks. This case study will illustrate and uncover several prevalent threats that targets social networking users in Malaysia. This includes discussion on online fake profiles, executing cyber extortion and cyber harassment based on the incidents received by MyCERT from year 2014 until June of 2017. Perpetrator's modus operandi and statistics analysis is highlighted in this paper. Countermeasures to cyber harassment is proposed as a preventive measure to limit the risks and impacts of potential cyber harassment threats.

Keywords: *Cyber Extortion; Cyber Harassment; Fake Profile; Phishing; Social Network.*

1. Introduction

In today's fast-growing information communication and technology, more than a billion people worldwide use social networking sites for various worthy activities. Web 2.0 is the technology platform for the social networking medium which can provide a more social, collaborative, and interactive platform compared to Web 1.0. This is such as to share knowledge, views, experiences, search for knowledge and to expand personal networking. They allow users to interact with other users, share knowledge, views, experiences, search for knowledge and to expand personal networking regardless of place and time. This interaction exposes lots of information to any users who wish to view them.

Apart being a platform for users to interact with friends for good purposes, social networking sites have become an avenue for various malicious activities such as being used in spamming activities, conduct scams, circulate harassing messages and hatred messages. Some of the features in social networking sites, such as "Like" or "Follow" has been manipulated by botnets to illegitimately promote products and services via social networking sites [1]. Facebook and LinkedIn are some examples of social networking sites and they had been rated as seven of the top 20 most visited Web sites around the globe. For the new so called Net Generation, social networking sites have become a way of life rather than just networking purposes. Some of the features of social networking sites have become common among for more than 300 social networking sites that currently exist. Creating and sharing a personal file is a very basic feature of any social networking site, which normally includes pictures, personal information, hobbies, list of friends and websites [2].

Cyber harassment is referred to harassing or annoying someone with malicious intent via technology-based mediums such as social networking sites and online chat. The intention is normally to cause disturbance, anger griefs to the victims. Cyber harassment includes cyber-bully and cyber-stalking activities against potential victims. Motivation behind cyber harassment activities can be for various reasons. They can be for fun or as an entertainment to fulfill one's boredom or due to some personal matters such as for revenge, jealousy, anger, righteousness, and bigotry or simply to get the attention of someone. Sometimes it can be that the perpetrator has no motive at all and it just happens because they were in the wrong place at the wrong time [3].

2. Social Network Threats Analysis

The security landscape in the cyber realms has many changes in the past years. MyCERT has observed new attack trends and patterns under the cyber harassment category. An obvious trend we observed the use of social networking sites and online chat applications, as platforms to conduct various malicious activities towards victims, be it an individual, a brand or even an organization. This includes fake profiles, cyber extortion, scams, click-jacking, doxing, elicitation and phishing. The following sections discusses about the threats of fake profiles, cyber extortion and cyber harassment attacks originated from the act of misused social network sites performed by the perpetrators. Table 1 shows the number of fake profile and cyber extortion cases reported to MyCERT from 2014 until June of 2017.

Table 1: Statistics for fake profile and cyber extortion cases in Malaysia.

	2014	2015	2016	2017(June)	Sum
Fake profile	80	62	66	30	238
Cyber extortion	264	233	136	53	686
Both	5	7	6	3	21
Sum	349	302	202	86	939

Table 2: Statistics for social network related cases in Malaysia by application category.

Social Network Platform	2014	2015	2016	2017 (June)
Beetalk (mobile application)	1	-	-	1
Blog	-	2	3	2
Facebook	72	54	87	48
Forum	1	-	-	2
IMO (mobile application)	-	-	-	1
Imgur	1	1	-	-
Instagram (mobile application)	2	5	15	14
LINK (mobile application)	-	1	1	-

LINE (mobile application)	-	-	-	1
Linkedin	-	1	-	-
Skype	-	1	-	-
SKOUT (mobile application)	-	-	-	1
Tagged	2	1	-	-
Tinder	-	-	1	-
Tumblr	-	-	-	1
Twitter	1	4	8	3
Wechat (mobile application)	6	-	8	3
Whatsapp (mobile application)	1	1	7	6
Various SNS	261	228	123	45
Viber (mobile application)	-	1	-	-
YouTube	-	-	1	-
Unknown	1	2	8	6
Sum	349	302	262	134

2.1. Fake Profile

Fake profiles or fake accounts are carried out by perpetrators by stealing personal information of a user such as pictures, name, telephone number and use the information to create a new fake profile purportedly belongs to a particular user. This leads to doubts or uncertainty between the actual owners of the profiles. Profile cloning or Identity Clone Attack (ICA) is fast growing in most of social networking sites that cause insecurity among Internet users while using social networking sites.

The main objective of this attack is to get as much information as possible from victims' friends by masking as a victim under fake profiles and eventually gain the trust among the friends' circles via the fake profile. There are two types of this attack, profile cloning within a same social networking site and cross-site profile cloning involving multiple social networking sites [4]. In [5] in their paper titled Profile Similarity Technique for Detection of Duplicate Profiles in Online Social Network has proposed an approach that may help to detect as many similar social network profiles as possible based on the similarity of the profiles' attributes and conduct analysis on the profiles to find out whether it belongs to a similar or multiple person.

MyCERT received a lot of reports on fake profiles, especially in Facebook and Instagram. Based on the reports, almost all of the fake profiles involved in executing the cyber harassment. The perpetrator makes full use of this kind of profile to lure and trick their victims into handing them over their money or even sensitive pictures. Listed below are two real cases observed from our reported incident database:

- Case #1: Perpetrator creates a fake Facebook profile by using victim's personal photos and family. Then, harasser posted other unnecessary photos and bad statement in Facebook wall to defame victim.
- Case #2: Perpetrator creates a fake Facebook profile to be used in other fraudulent activities such as cyber blackmail scam, love scam, and fraud purchase. Fraudster creates the fake profile to avoid from easily being tracked by Law Enforcement.

Based on our analysis from reporting cases, there are many approaches used by the perpetrators to attack their victims. The first way is, the victim's fake account has been created by an individual that might be known and is believed to have had contact with victim such as an ex-boyfriend or a friend. The perpetrator adds victim's friends to make the account look realistic. Furthermore, the account is used to defame the victim by attacking somebody else either it is on a personal basis or on a public page.

The second approach is, the fake social network profile had been created by publishing victim's personal information namely telephone number and photo. The fake account with this information, usually created to offer sexual service with the purpose to slander or to harass victim. Figure 1 shows the flows of the steps used by the perpetrator to victimize their target.

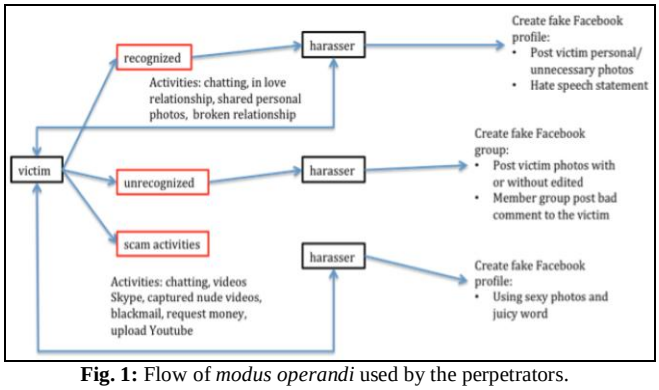

Fig. 1: Flow of *modus operandi* used by the perpetrators.

2.2. Cyber Extortion

Cyber extortion is referring to the act of using the cyber means to extort or threaten potential victims, mainly for malicious purpose. The ultimate purpose for this activity is monetary gain by creating fear and trauma in the victims. Extortionists are moving one step ahead by using various technologies to evade detections and camouflage their presence with TOR and virtual currencies such as Bitcoin. For the past years, MyCERT observed an increase in the number of cyber extortion incidents that involve cyber blackmail, which involves blackmailing, and extorting money from victims. Unsuspecting Malaysians continue to be victims, with some being threatened to have their nude photos or compromising videos released on YouTube and social networking sites if they do not pay up, within a certain period. Extortionists use social networking sites like Facebook, Tagged and online video chats such as Skype as the platform to carry out their activities [6]. In fact, it has become a global threat and has become quite serious where victims are threatened, extorted and has serious impacts on their reputation. Initially, the modus operandi will begin with getting to know victims via Facebook followed by video chat via Skype.

- Case #1: Perpetrator request friends with victim through Facebook. They chat through Facebook messenger then move to video Skype. Victim is in teased to unclothe while chatting same action with the perpetrator. Unfortunately, the perpetrator captures victim's nude videos. The victim is blackmailed for some amount of money or the nude videos will be uploaded to YouTube or any online video websites.

Based on our statistics and observation, the most common social networking platform used by the perpetrators is Facebook, however some are using Tagged. The perpetrator will then ask the victims to move to another platform that has the capability of recording video, i.e. Skype. The perpetrator disguised as an attractive young lady that the photos might have been copied from someone else's social network profile on the Internet.

The *modus operandi* is to lure the victims to undress themselves and to perform a sex act, while the perpetrator is recording the action without them knowing it. The victim is then told that the act has been recorded and will be uploaded on the YouTube, unless a sum of money is paid to withdraw it from being uploaded and spread among the victim's Facebook friends. Another approach used by perpetrators is by exploiting a victim's lost or stolen phone. Nowadays, smartphones carry gigabytes of private data including contact lists, photos and videos. With this data in their hands, the perpetrator contacts the victim and threat to spread the photos on the social media if the victim refuses to pay. They even contact the people in the victim's contact list to extort some money or threaten them.

Based on Table 1, cyber extortion is the highest cases being reported to MyCERT each year. Meanwhile, there are few cases that the victims are being extorted using victim's fake profile or the perpetrator is creating a fake profile to deceive their target and harassing the victim.

2.3. Cyber Harassment

This kind of threat involves the act of executing harassment towards individuals or organizations by using the Internet applications such as social networking sites (SNS) and messaging applications. The impact of this threat is very negative towards the victim's reputation and image. Even in some cases, the victim's psychology becomes affected and they feel unsafe and traumatic in using the Internet.

On a yearly basis, MyCERT received many reports from Malaysian Internet users that fall prey to this kind of attack. Table 3 shows the statistics of cyber harassment cases from 2014 until June of 2017 classified by categories. Based on the collected data from the reported incidents, we found out that cyberbullying and religious bullying are among the highest cases in Malaysia. We also found out that the victims are mostly youth and those with low awareness level of how to stay secure on the Internet. Figure 2 and 3 show two screenshots of chat sessions executed by the perpetrators.

Table 3: Statistics for cyber harassment cases in Malaysia for 2014 to 2017 (as of June).

Cyber Harassment	2014	2015	2016	2017(June)
Cyber Harassment -- Cyber Bullying	291	256	338	170
Cyber Harassment -- Cyber Stalking	9	5	14	8
Cyber Harassment -- Racial	20	1	1	3
Cyber Harassment -- Religious	10	26	111	165
Cyber Harassment -- Sexual	220	154	65	33
Total	550	442	529	379

Referring to Table 4, despite the finding from the platforms used in cyberbullying, nearly 46% of the reports were lodged by victims aged 26 to 40 years old. This significant trend shows youth between that ages are more likely experiencing cyberbullying compared to those in different age of groups. Only 9% victims in the age group 56 and above had experienced cyberbullying and occurred through multiple SNS platforms. As noted in this table, most victims aged below 18 years old had experienced cyberbullying from their personal activities.

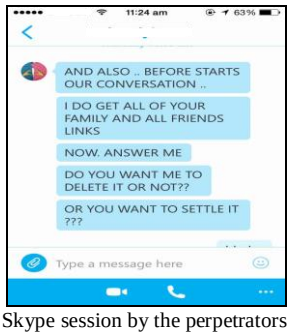

Fig. 2: Example of Skype session by the perpetrators towards the victim.

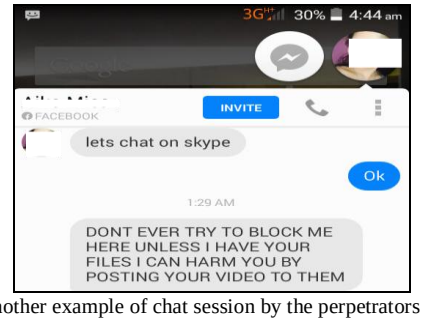

Fig. 3: Another example of chat session by the perpetrators to the victim.

Table 4: Statistics for age of group complainants for 2014 to 2017 (as of June).

Age Group	2014	2015	2016	2017	Sum
0-18 years	9	9	9	6	33
19-25 years	49	77	63	38	227
26-40 years	63	86	71	38	258
41-55 years	5	12	17	10	44
56 and above	0	0	1	4	5

3. Proposed Countermeasures

In this paper, we propose countermeasures that may help to mitigate the risks and potential threats to users who are engaged with social networks, such as cyber harassment, cyber bully, cyber stalking and fake profile. The countermeasures proposed are two-folds, addressing the social network providers and social network users.

3.1. Countermeasures Addressing Social Network Providers

- Social Network Provider must take appropriate measures to ensure the security of their application by means of tools and technology, from threats such as identity theft, fake profiles, fake registration, phishing and pharming. They must employ secure connections such as the Secure Socket Layer (SSL) for establishing an encrypted link between a web server and a browser that ensures all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.
- Social Network Providers must ensure users' data is safeguarded from compromise and misuse by perpetrators. It is recommended that Providers ensure that users have full control over their published data that can help to prevent exposure of data belonging to the users by perpetrators. Providers need to come up with a solution that requests the authenticity user's permission prior to publishing any data belonging to the user. In [7] had proposed the use of tagging mechanisms requesting user's approval as one of the approaches aimed at the achievement of this goal.

3.2. Countermeasures Addressing Social Network Users

- A social network user has full control of the type and level of the information they want to share. Sharing private and confidential information puts a user at risk and prone to attacks associated with social networks such as cyber harassment, cyber bully and fake profile. They must always read the Terms of Service before they share any information. It is recommended not to publish private information in personal profiles that could be seen by everybody including perpetrators.
- User awareness is another mechanism to protect users from becoming victim of cyber harassment. They need to be exposed to various tips and guidelines that provides a correct and secure method in using social networks. Government and corporate sectors should come together to educate users on best practices in using social networks through public talks, seminars, road shows and educational programs that could help to prevent threats harnessed from social networks.
- Organizations may conduct Threat Modelling of social networks and identify the potential risk to the organizations. Threat Modelling is a description of a collection of security aspects, a set of plausible attacks which can affect the performance of any computer system. This methodology allows security experts to identify security risks, verify an application's security architecture, and develop countermeasures in the design, coding, and testing phases [7]. Once identified the risk, necessary controls can be put in place as a preventive measure

against potential harms such as cyber harassment, fake profiles that can be harnessed from social networks.

Organizations may play a role in putting controls on the usage of social networks in the office such as blocking the application at network gateways. The less users exposed to social networks the less prone they are to become victims of cyber harassments and other threats such as cyber bully and fake profiles. This measure could be a result of Threat Modelling that had identified the risk and applying a control to the risk at perimeter level.

4. Conclusion

Social media applications are growing tremendously in Malaysia and has become a popular mean of interaction among Internet users. The statistics presented in the Case Study of this paper clearly indicates the popularity of Facebook, Instagram and Twitter for interaction compared to other channels. Due to their ease of use, popularity and wide coverage, they can be easily misused by perpetrators to conduct mischiefs online. The increasing number of incidents related to Cyberbully, Cyberstalking and religious-motive Cyberharassment together with the increase number of incidents communicated through the above-mentioned social media channels, shows the seriousness and high potentiality of cyberharassment threats to Malaysia internet users. The threat needs to be controlled and treated by deploying the countermeasures proposed in this paper. The countermeasures proposed are some of the effective mechanisms and techniques available in mitigating the threat, which is a combination of technical and social science perspective. The way forward is relevant parties such as Law Enforcement Agencies, NGOs, Schools, Government Agencies, Corporate companies should be part of the players in mitigating the threat in the country, such as to provide emotional support for victims, investigation and prosecution of perpetrators and improving current laws on cyber harassment, as a holistic approach in mitigating cyber harassment threats in Malaysia.

References

[1] Xiao, C., Freeman, D. M., & Hwa, T. (2015). Detecting clusters of fake accounts in online social networks. Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security, pp. 91-101.

[2] Priyanga, S., Priyadharshini, V. M., & Hariharan, N. (2015). Prevention of fake profile proliferation in online social networks. International Journal of Innovative Research in Science, Engineering and Technology, 4(6), 25-32.

[3] Chandrashekhar, A. M., Muktha, G. S., & Anjana, D. K. (2016). Cyberstalking and Cyberbullying: Effects and prevention measures. Imperial Journal of Interdisciplinary Research, 2(3), 95-102.

[4] Rizi, F., Khayyambashi, M., & Kharaji, M. (2014). A new approach for finding cloned profiles in online social networks. International Journal of Network Security, 6, 25–37.

[5] Nandhini, M., & Das, B. B. (2016). Profile similarity technique for detection of duplicate profiles in online social network. International Journal of Computer Science and Information Technologies, 7(2), 507–512.

[6] Ashford, W. (2015). DD4BC cyber extortion gang adds social media to arsenal. http://www.computerweekly.com/news/4500253322/DD4BC-cyber-extortion-gang-adds-social-media-to-arsenal.

[7] Sanz, B., Laorden, C., Alvarez, G., & G Bringas, P. (2010). A threat model approach to attacks and countermeasures in on-line social networks. Proceedings of the 11th Reunion Española de Criptografía Y Seguridad de La Información, pp. 343-348.