Emergence of Cybercrimes in Online Social Networks

Raenu Kolandaisamy, Heshalini Rajagopal
Institute of Computer Science and Digital Innovation, UCSI University, 56000 Kuala Lumpur, Malaysia

Indraah Kolandaisamy
School of Business Management, University Utara Malaysia 06010 Sintok, Kedah
E-mail: raenu@ucsiuniversity.edu.my

Abstract

The rise of social networking websites has been seen in recent years. Everyone will be spending most of their time on social networking websites such as Facebook, Instagram and Whatsapp. The great advantage that this social networking website offers benefited many of the users. It can help people to promote themselves or their business to gain more popularity and also customers through these social networking websites. There are many cybercrimes that can be identified which are identity theft, hacking, fraud and so on. The emergence of cybercrimes has created an awareness so that the users will know what the common attacks are and how they can be prevented from being lure and being a victim of this attack. This research will discuss about the attacks and how these attacks can be prevented by the users.

Keywords: Social Network, Cybercrimes, Digital World

1. Introduction

Social network has been growing in the 21st century and has become one of the trend that people use to communicate everyday. Social network is connecting with different individuals using the internet through social media websites [1]. It allows many individuals to be connected to each other and thus allowing many people to have communication with each other around the world. Social networking has been so popular because of the great ability and the features that it offers. The number of social networking sites has been growing from time to time. Some of the popular social media application and websites are Facebook, Whatsapp, WeChat, Instagram, Twitter, Google + and Skype. An example will be Facebook that have over 2 billions of active users each month based on Fig. 1 as of June 2017 [2].

Each of the social media platform have different features and design in it. There are many reasons why social networking has gain so much popularity over the years. The first reason will be the opportunity to meet new people. We live in a world that is full of different culture and environment thus meeting new people from different countries all over the world is indeed a great joy for many of us.

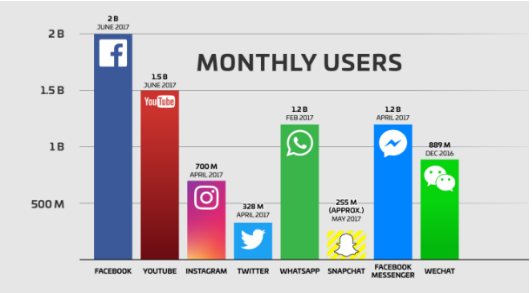

Fig. 1: Monthly users of social media applications

The second reason will social networking sites are user friendly and thus is easy to use. Most sites are developed with a very user friendly interface and is easy to navigate which require a little knowledge to learn. The third reason is that it is available to use on many platforms such as desktop computers, tablets and also smartphones with different operating system. The fourth reason is that social networking sites are free of charge to use and therefore many users will certainly want to try and use it [3]. Through gaining popularity to this sites, many also get the opportunity to advertise their product and services thus making social networking a good place to start and grow your business. The fifth reason is that social networking sites create the opportunity for graduates, businessmen and also

professionals to find their ideal jobs and also to meet the people that have the same interest as theirs.
The rise of social media certainly has a great impact on the community and the great benefits it has to offer but there also dangers in using social networking because of the large community it possesses and thus making user vulnerable to security threat and attacks. It can be shown that in recent years through social media that many have faced attacks such as scam and conned by users on social networking sites trying to impersonate another person seeking for donation and other personal information such as bank details and so on. There are very dangerous in the society and unaware users might be lured so this studies to help to increase the awareness of cybercrime in social network.
Cybercrime can be any activities that compromise on the security of the users and try to exploit another user using the internet. It is an illegal activity that involves the use of computer and the internet through a platform like social networking to gain or to cause destruction to another user on the that network. Cybercrime is the greatest attack based on the Fig. 2 that shows the motivation of the attackers [4].

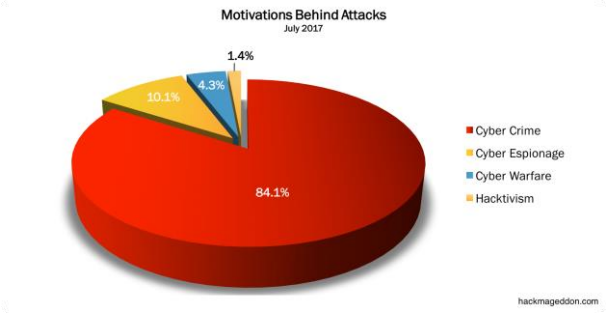

Fig. 2 Motivation behind attacks

Cyber criminal can be categorized into many aspect. It can be broken down into a few different parts which are

- A website lure a users to click on an image or a link to visit another website that can spread malware to the users computer to take control and gain information from the users computer.
- A scammer try to claim to impersonate someone to be a bank staff to gain personal information such as password or even donation by creating a fake account.
- The hackers hack your social networking account to use as a way to get details from close people like family.

The danger to the victim here is that, they can lose their information in a matter of minutes. It will be a big problem to many society and what's more dangerous is that one victim can lead another victim to be a victim. For example, a victim receive an email regarding a free gift that can be obtained if they follow the steps to complete it on a website, but he or she sends it to her many friends on Facebook thus making them to be a victim as well because of the person doing things unknowingly.

2. Literature Review

2.1. Detecting Compromised Accounts on Social Networks

Social networking is one of the most used website in today's internet world. Social networking is a website that uses the internet to bring people together to share information, ideas and also make new friends. This can also be known as social media. Everyone loves to use social media because it is convenient and free. Social media websites such as Facebook, Instagram, Twitter and Whatsapp can all be accessed on various platform such as smartphones, tablets and computers. This has been a great advantage to many users around the world. Social networking has been very demanding and popular but the ever increasing of cyber criminals activities are also increasing as well making it very dangerous.
The study on detecting compromised accounts on social networks by Manuel Egele, Gianluca Stringhini, Christopher Kruegel and Giovanni Vigna will be discussed. The act of compromising on social network accounts has been a great and profitable job that has benefit the cyber criminals. The reasons here is because the speed and reliability of social medias account. By targeting a social media account of a famous artist that have many followers and by sending out fake messages can be able to scam many thousands of users that have follow that famous artist. It is very dangerous because once an attacker managed to compromise a social network account, the person can use it for many purposes such as sending out spam messages to people or even phishing web sites link. It is a higher benefit for attackers to target large and popular company that has large amount of followers like news company.
Fake accounts and legitimated hacked accounts have different characteristic so the system is harder to detect because it is not the fake accounts that is created by a user, it has been a good standing account but it is being compromised. This research introduced COMPA which is basically a detection system that is designed to identify compromised social network accounts. COMPA is use to monitor the habits of the user in a social network account [5]. A person who uses social media like Facebook usually have a fairly stable behaviour from the messages that is being send or the amount of time that the person is active. How this works that COMPA will actually build a behavioural

profile for social network accounts and then it will start to monitor and compare the new messages that is being sent by the account, if it looks different from what it usually is then Compa will flag it as being compromise. There are two common use to detect compromise account and the first is call suspicious group. Suspicious group are those that send and do more than what the accounts normally do. For example, account A usually send out 50 messages a day and averages about 45 per month, but that particular month itself, it exceeded the regular threshold by sending over 500 messages a day. It can be easily be detected especially if the amount raise too significantly.The second is call bulk application. Bulk application are the one that send out large amount of messages with the same amount of text and words.

The studies have evaluated both social media websites which are Facebook and Twitter. The data collection method was to collect real time tweets from Twitter and ran Facebook experiments on a large dataset crawled in 2009. The advantages of COMPA is able to identify groups of compromised accounts that are to distribute malicious messages on this accounts.

The limitation of this studies is that if the attacker is aware of COMPA, the attacker learn about the victim's behaviour before compromising so that COMPA cannot detect the unusual behaviour of the account because of the similarity of the action that is being possessed by the attacker that imitate the action of the victim. Besides that, social networking sites are harder to gather data.

2.2. Cyberbullying detection in the Twitter network

The rise of social networking websites has been such a great impact to many users in the world. Many use this opportunity to gain new friends, establish new relationship and also to connected with family and friends. Although it has been seen by many as a benefit but the use of social networking websites has been so popular that many have use it in the wrong manner to abuse it and gain advantages over it but causing harm to another. The discussion in this literature review is by Mohammed Ali Al-garadi , Kasturi Dewi Varathan and Sri Devi Ravana which is about the experimental case of cyberbullying detection in the Twitter social network[6].

Firstly cyberbullying can be defined as the use of information and communication technology on the internet and it can on any social media platform for example Facebook, Twitter, Google+ and also Instagram to harass another user. This research and studies is to focus on how cyberbullying happens on Twitter. The study is to improve the detection rate on detecting cyberbullying on Twitter that has been done by detecting the use of offensive language on Twitter. The detection of of abusive language can include the use of acronyms and words that can increase the cyberbullying classifier. Cyberbullying can be also associated with the aggressive behaviour of the users on Twitter. As certain words can be harder to detect because the words needs to be read as a whole sentence to know whether it is offensive or not. In this case, plenty of information that needs to be utilized to achieve and accurate detection to says that the particular tweet is dangerous and abusive. The detection of vulgar words can also be used as this also a signal of offensive behaviour. The cyberbullies can also use many ways to tweet and of way is to use abbreviation or acronyms to shorten the sentence. The studies uses machine learning algorithms to detect the words with various method. They are four different ways that has been used which are NB, LibSVM, random forest and KNN. This are all the method that is used the various results and conclusions has showed that the study of abusive language and cyberbullying will required the machine to adapt and new learn words as time goes on because new vulgar words with abbreviation may be form and thus making it difficult to detect. The studies suggest that using other social medias can also improved the learning process of the system so that cyberbullying can be resolved and reduced in the community of social networking users.

2.3. Organised crime goes online: realities and challenges

The Internet is like a vast galaxy of interconnected networks that allows many transactions and events taking place virtually from the whole world - including cyber crimes and also Internet-facilitated organized crime. The study of the realities and challenges of organised crime online by the author Anita Lavorgna will be discussed.

Cyber crimes are known as a group of criminals that uses ICT infrastructure to commit crimes, such as phishing, malware injection, Denial of Service, and so more. However, in this world we are living in, organized crime groups (OCGs) have existed for long time and have conducted crimes offline. This paper mostly discussing on how these OCGs make use of Internet or online presence to evolve themselves in today's situation where everyone is more Internet-dependant.

The data for this paper are from interviews and also data collected from law-enforcement officials and experts researchers in the United Kingdom, United States, and the Netherlands. 120 case studies regarding crime with

the usage of Internet are also taken into the analysis of this paper.

This paper focuses on two types of OCGs, one is traditional business-style groups, the other is mafia-style groups. The type crimes committed by these business-style OCGs are identified - mostly on trafficking activities such as wildlife, human, psychoactive substances (drugs), and also fake medicines. These criminal activities are more to businesses motive and thus using the Internet to facilitate online. With the use of online social forums, instant messaging feature for example, it is easier for these crime groups to conduct and also expand their businesses ties with the client.

Mafia-style groups, however, were found to be still grasping on the use of Internet technologies for their criminal activities. Trafficking and gambling activities were their main focus. However, mafia-style groups as are mostly depend on a territorial and political trust, hence face-to-face interactions are needed. The highest hierarchy of this group were found to be mostly leaded by a leader who are not fancy of the use of the Internet. However, as these groups keeps evolving in the future, the usage of Internet in their criminal activities are to be expected as new generations will lead in the future.

The previous points discusses the reality of these OGCs. The challenges however, observed on legislation and policies for these Internet-mediated crimes. It is found that the regulatory policies regarding these crime activities via the Internet are not enough to control them. The instantaneous and universality of the Internet makes these inhibits these regulatory policies to fully take effect. Other challenges found for legislation and policies are such as different approaches applied in different countries as some of these countries have difference in experience in regards to tackling online crimes and carrying out investigations. [7]

2.4. Privacy and Security Issues in Social Online Networks

Social networking has becoming a necessity in today's society as more people in the world are having easier access to the Internet. However, this new necessity can bring a potential danger especially to new and also "naive" users of online social networks, especially teenagers. In this paper by Radhika Bhagat, Rajvi Modi, Palaumi Patel, and Harshil Joshi discusses about the potential privacy and security threats in social online networks today.

Users of online social networks were discussed in this paper. Most of the users using social network sites (SNS) to get informations and happenings all around them instantaneously. Personal information were propagated by them using SNS. Users of SNS tend to take security lightly and this poses security and privacy threat upon their account.

Among the security issues discussed in this paper are, firstly, identity theft. It is defined as an action of acquiring someone's identity without permission and misusing it for malicious purposes, such as fraud. The author(s) suggested that users of SNS should not simply accept unknown friend requests and check the requesting account beforehand for safety.

Secondly, phishing is also a security issue found in SNS. Preparators of phishing uses 'mock-up' websites to lure users into logging in and thus exposing their sensitive credentials such as login credentials. Author(s) suggested users to always use trusted devices to log in to accounts and be wary of unknown websites. Other security issues found in SNS are such as brute force attack, Sybil attack, and Trojan attack.

Privacy issues in SNS were also discussed in this paper. Privacy settings is said to be always overlooked by most SNS users therefore this poses a huge privacy risk to them as social networks get to hold users sensitive data. It is found that some users even share their sensitive data, whether aware or unaware.

Among privacy threats discussed are such as cyber stalking, whereby most SNS has made it easy for these lurkers to stalk users' profiles without adding them as friends. Author(s) suggested users to keep their profiles privacy mode hidden and only to be shown to trusted parties only. Secondly, cyberbullying also a privacy threat found in SNS. Cyberbullying example are such as commenting illicitly on people's photos or posts and also tarnishes one's reputation online, mostly anonymously. Author(s) suggested users to keep things shared on SNS away from third party users and also be wary of them.

Other privacy threat includes profile cloning, whereby preparators create another account with similar information as the users', and therefore performing malicious actions online to the victim's friends.[8]

2.5. Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing And Malware Networks

As we are living in a digital age, everything is adapting to it. Not just people, and organizations as a whole, but even cyber criminals too. The usage of digital means such as Internet, and its platforms such as forums, social networking services, has made it easier for individuals to get together and communicate anywhere and anytime. This paper, authored by E. Rutger Leukfeldt, Edward R. Kleemans and Wouter P. Stol, discusses about

cybercriminal networks applying social ties and/or digital ties for their activities and recruiting.

A social network usually formed by actor to another actor with ties between them that defining their connection and relationship. A social tie are usually formed via social contact, for example, meeting in a specific place such as cafes, to engage social activity. Digital tie can be formed virtually online without social contact such as using forums.

Social relationships are crucial in criminal networks. However, social relationships are highly clustered with existing relationships such as contacts from former workplace, friends, family, and these relationships are said to yield less opportunity. With Internet, the boundaries of traditional social network are blurred and "specific offender convergence setting" can take place via online forums where these cybercriminals can get together and share information online from different places and also recruit new members or enablers.

The origins and growth of cybercriminal groups were mostly investigated in this paper. The data for this paper is taken from 18 Dutch police files on cybercrimes that provides them with knowledge cybercriminal networks and its members.

Four models of growth were developed in this paper. It is found that cybercriminal networks' growth are associated with recruitments of enablers - professional and/or recruited. These enablers provides services to cybercriminals to give them access to useful and relevant information such as credit card information and postal information details. The four models of growth consists of the first stage, that is "entirely through social contacts", second stage "based on social contacts; forums for recruiting specialists", third stage "based on forums, with social contacts used to recruit local criminals" and fourth stage that is "entirely through forums".

It is found that most of the cybercriminal networks uses social contacts entirely (first stage) to grow their network and does not use online forums. However, in future, forums may become a more common place for the growth of cybercriminal networks in this digital era. [9]

3. Methodology

The methodology used in this paper are are as follows:

- Questionnaire
  A set of questionnaire created in Google Forms is distributed online for respondents to fill in. The respondents sample size is taken among students of UCSI University as a representative of the public society. The questionnaire would help to analyze the approaches and actions taken by the society in dealing with online social networks, especially in situations that may cause cyber crimes to take place.
- Social network visualization
  A Facebook dataset from Stanford Network Analysis Project (SNAP) are used to demonstrate and visualize how actors are connected in social network such as Facebook. [10] Social network analysis visualization tool used is Gephi.

4. Result and discussion

We have found that the problem with cybercrimes will continue to increase as more users increase in the use of social media. This is because the great number of users can be a good target for the hackers and attackers because it can be very lucrative if the hacker is being able to compromise millions of users at once. That is why online social media has also been a dangerous platform to know friends because of the use of a device and a face to face conversation has not been done and that makes it very difficult to know the real person's identity. The person can be a boy on Facebook talking to another person, but in reality she is a girl. That is really a very dangerous act and it can cause many unwanted things to happen on social media websites. Nowadays, because people are also attracted by free stuff and gifts only, it can be such an easy way to cheat people because of the lack of knowledge the users possess and thus it is very dangerous for users to click on links that link to malicious website that can harm the user's computers.

To find out how actors connected to each other in a social network, we have used a social network analysis tool software Gephi to visualize the network based on a dataset collection from Stanford Network Analysis Project (SNAP). This dataset is particularly from Facebook. As shown in Fig. 3 this is the result of the visualization projected from the dataset. The type of the dataset is undirected, it has 4039 nodes, and 88234 edges.

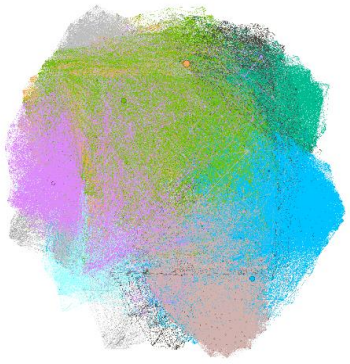

Fig. 3 Result of the visualization projected from the SNAP dataset

Fig. 4 shows our simulation on how a group of "rogue actors" can affect the social network. These "rogue actors" nodes are represented in color red. This shows that a small group of them can have quite a spread impact on the network. Note that this dataset is not a full dataset from Facebook - it is collected from SNAP survey participants on Facebook. However, a small dataset can be observed quite complex.

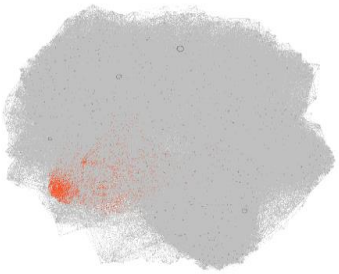

Fig. 4 Simulation on how a group of "rogue actors" can affect the social network

The questionnaire was distributed online and conducted via Google Forms. Over 35 respondents responded to the questionnaire. Questions asked were about their online social network service they are using, how do they use, how many connections they have, how do they react with unknown person on social network, and so on. The results are shown in the charts and graphs below. Based on the chart above in Fig. 5 asking about social network that is being used by the respondents and Facebook has the highest amount of users based on the survey done. It clearly shows that Facebook is still the most popular social network website that is use among the people.

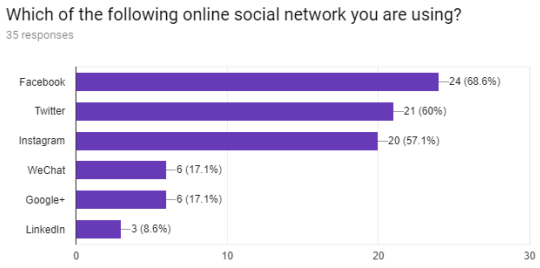

Fig. 5 Social Media used

The pie chart above in Fig. 6 shows that many people have many friend on social networking website and it can be clearly seen that many spend time on social networking site making new friends.

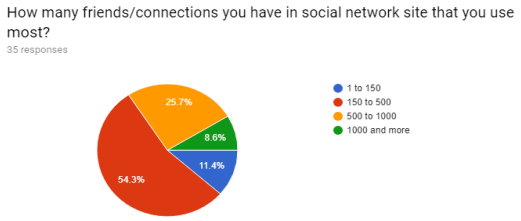

Fig. 6 Number of friends on social networking site

Fig. 7 shows that most of the respondents accepts friend requests even if they don't know the person well. Although the difference between those who answered Yes and No is quite minimal, this shows that there are people still doing that practice.

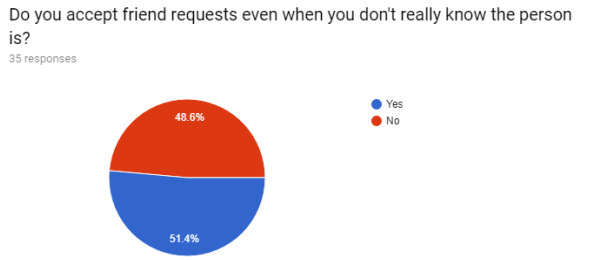

Fig. 7 Friend request acceptance

Fig. 8 shows that most of the respondents do get a private message from unknown person on online social networks.

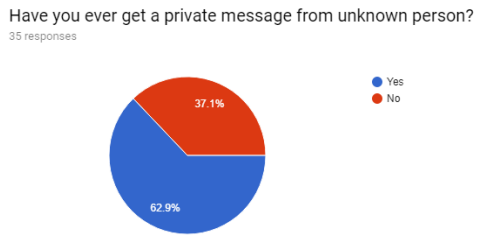

Fig. 8 Receiving private messages from unknown person on online social networks

Fig. 9 shows that many messages that is being sent to the user are mostly an advertisement with a link attached to lure the users to go to another website. The next is the attempt to get to know you more which is very common in social networking sites because is a platform to get to know more new friends. The last is just a simple link without any description.

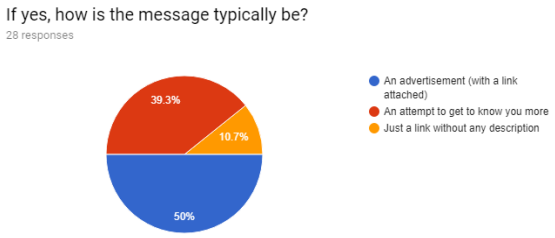

Fig. 9 The typical messages

Fig. 10 shows that many users will still click on the link even is a banking website. It shows that many users will click if the link looks trustworthy. Which the yes has the highest user.

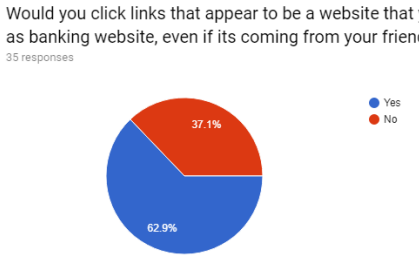

Fig. 10 Clicking links on website

Fig. 11 shows that many users are being added into unknown groups by other people that they do not even know.

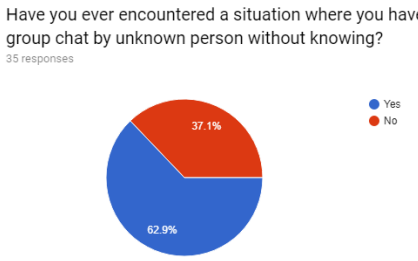

Fig. 11 Added to group chat by unknown person

Fig. 12 shows that there are people who are being tagged by others into a picture which their faces are not even in. This shows that many people are being by others as a way of advertising their product.

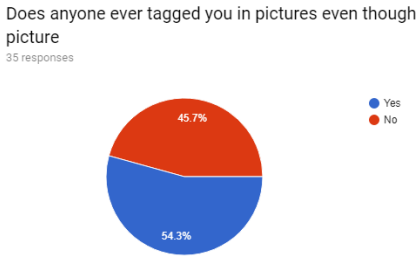

Fig. 12 Anonymous tagging

Fig. 13 shows that they are many people who use Facebook do not set their post to public because and prefer to be private. This is a good measure of the users to prevent unwanted use for comments by unwanted users.

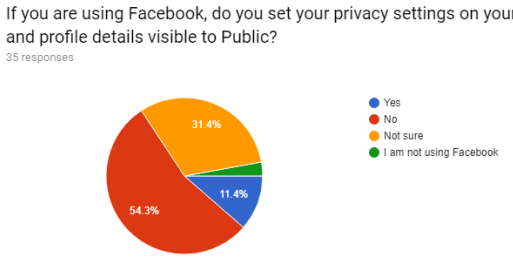

Fig. 13 Privacy settings

Fig. 14 shows that many people do not check and see who is the publisher of the content creator before allowing others to access their Facebook page and content.

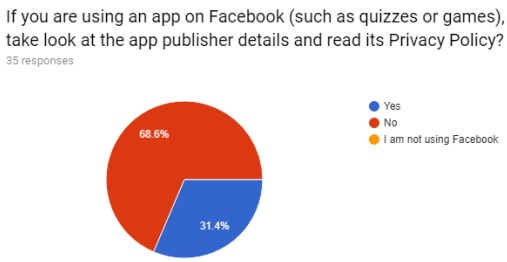

Fig. 14 Publisher details and privacy policy

Fig. 15 shows that many have not being cyber bullied on social network sites and that is a good thing.

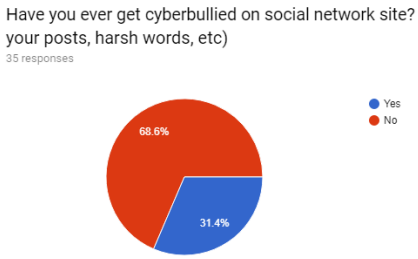

Fig. 15 Cyberbullied

Fig. 16 shows that they are many users who will just accept friend request without thinking twice whether the person is real or not. This is pretty dangerous as this can allow hackers to compromise other users.

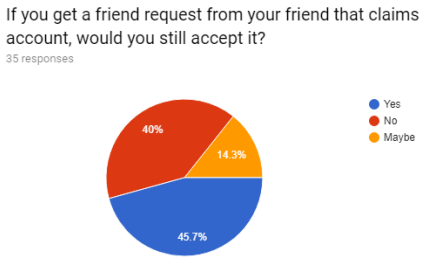

Fig. 16 Accepting anonymous friend request

Fig. 17 shows that many users are still very unaware that cyber crime is dangerous and this users will require need to have more knowledge if they want to keep themselves safe.

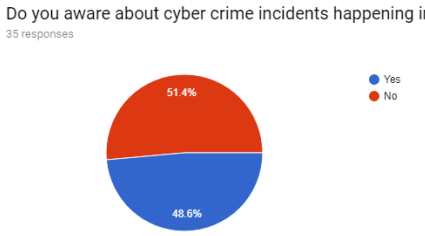

Fig. 17 Awareness on cyber crime

Fig. 18 shows that many are still in the middle and some still think that social networking websites is still unsafe and is dangerous to many people.

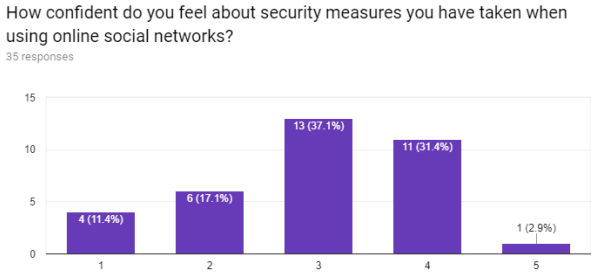

Fig. 18 Safety of social networking sites

5. Conclusion

Social networking has been really a good way to communicate with friends and family and thus make life happier and more joyful. This is because of the convenience that is offer and many users love using it and have spend hours and hours a day just to go through social media and looking at post posted by others. The security of this social medias websites has improved over the years but there are still many loopholes that be compromised by the hackers because of the lack of knowledge that the users have and thus making users more vulnerable to attacks. One common mistakes that most users make is to create a password that is similar to their birthday date or telephone number and that makes easy for many to easily compromise his or her account. Besides that, talking to an unknown stranger can also be very dangerous especially those who are seeking for new friends and are desperate, they tend to do things without thinking of the danger.

From the findings gathered in the previous section, it is apparent that because of the way on how online social networks users uses the platform, it contributes to the emergence of the cyber crime in online social networks.

References

1. What is social networking? - Definition from WhatIs.com", WhatIs.com, 2018. [Online]. Available: http://whatis.techtarget.com/definition/social-networking. [Accessed: 07- Mar- 2018].
2. J. Constine, Facebook now has 2 billion monthly users… and responsibility, TechCrunch, 2018. [Online]. Available: https://techcrunch.com/2017/06/27/facebook-2-billion-users/. [Accessed: 07- Mar- 2018].
3. M. Fita, M. Fita and M. Fita, 6 Reasons Why Social Networking is So Popular These Days |, Brandignity.com, 2018. [Online]. Available: https://www.brandignity.com/2012/11/6-reasons-why-social-networking-is-so-popular-these-days/. [Accessed: 07- Mar- 2018].
4. July 2017 Cyber Attacks Statistics, HACKMAGEDDON, 2018. [Online]. Available: https://www.hackmageddon.com/2017/08/24/july-2017-cyber-attacks-statistics/. [Accessed: 07- Mar- 2018].
5. Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna, Towards Detecting Compromised Accounts on Social Networks.
6. Kolandaisamy, R., Noor, R. M., Zaba, M. R., Ahmedy, I., & Kolandaisamy, I. (2019, July). Markov chain based ant colony approach for mitigating DDoS attacks using integrated vehicle mode analysis in VANET. In 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP) (pp. 1-5). IEEE.
7. A. Lavorgna, "Organised crime goes online: realities and challenges", Journal of Money Laundering Control, vol. 18, no. 2, pp. 153-168, 2015.
8. R. B. R. M. P. Patel and M. H. Joshi, "Privacy and Security Issues in Social Online Networks,", National Conference on Latest Trends in Networking and Cyber Security, 2017.
9. E. Leukfeldt, E. Kleemans and W. Stol, "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks", British Journal of Criminology, p. azw009, 2016.
10. J. Leskovec and A. Krevl, SNAP Datasets: Stanford Large Network Dataset Collection, 2014.

Authors Introduction

Dr. Raenu Kolandaisamy

He received his PhD from the Faculty of Computer Science & Information Technology, University Malaya in 2020. He is currently an Assistant Professor in UCSI University, Malaysia. His research interest areas are Wireless Networking, Security, VANET and IoT.

Dr. Heshalini Rajagopal

She received her PhD and Master's degree from the Department of Electrical Engineering, University of Malaya, Malaysia in 2021 and 2016, respectively. She received the B.E (Electrical) in 2013 Currently, she is an Assistant Professor in UCSI University, Kuala Lumpur, Malaysia. Her research interest includes image processing, artificial intelligence and machine learning.

Dr. Indraah Kolandaisamy

She is a senior lecturer in School of Business Management, College of Business, Universiti Utara Malaysia. Indraah A/P Kolandaisamy holds a doctorate in Management from Universiti Kebangsaan Malaysia in 2015. Her D.B.A work is on organizational citizenship behavior among public sector in Malaysia. She obtained her MSc (Management) and Bachelor in International Business Management (Hons) from Universiti Utara Malaysia respectively in 2007 and 2005.