International Journal of GEOMATE, Sept., 2017, Vol. 13, Issue 37, pp. 81-86
Special Issue on Science, Engineering & Environment, ISSN: 2186-2990, Japan
DOI: http://dx.doi.org/10.21660/2017.37.2801

ETHICS ON SOCIAL NETWORKING: A PRELIMINARY SURVEY IN THAILAND

*Lachana Ramingwong and and Sakgasit Ramingwong

Department of Computer Engineering, Faculty of Engineering, Chiang Mai University, Thailand

*Corresponding Author, Received: 16 June 2016, Revised: 11 Aug. 2016, Accepted: 18 Nov. 2016

ABSTRACT: The rapid growth of social networks and their users has been phenomenon. This brings numerous changes in everyday life, both positively and negatively. Ethics have become a major growing challenge in this area. Sensitive issues such as privacy, impersonation and cyberbullying are increasingly causing more damage to the community. This research reviews ethical issues on social networks. It also reports results from a survey on the most anticipated ethical concerns from the viewpoints of undergraduate students from Chiang Mai University, Thailand. Lost of privacy, misinformation and impersonation are anticipated as the worst ethical misconducted.

Keywords: Social networking, Ethics, Risks, Survey

1. INTRODUCTION

It is estimated that there are approximately 2.2 billion social network users worldwide in 2016 [1]. Compared to the past decades, this technology has brought numerous changes to global community [2], along with the rapid growth of smartphone users. Although social networking brings numerous benefits, it also represent an increasing number of inevitable risks [3].

There were more than 44.6 million Internet users In Thailand in 2014 [3]. This was roughly 65.7% of the total population of 67.9 million. The most popular social networking platform is Facebook with the total of 30 million active users. YouTube, twitter and Instagram are also well-known amongst the Thais with the total users of 26.2, 4.5 and 1.7 million, respectively. This high number of users are related to a number of undesirable ethical incidents which can also happen in other countries.

This research focuses on ethical risks which arise from the use of social networking. It identifies 15 sensitive issues, i.e. loss of privacy, identity theft, phishing, misinformation, malicious software, cyberbullying, hacking, piracy, plagiarism, spamming, trolling, clickbait, inappropriate contents, witch hunting and disagreement lacking dialectic. It discusses the characteristics and impacts of these risks based on cases from the use of social networks in Thailand, a developing Southeast Asian country. It also report results of a survey on the perceptions towards them from undergraduate students from Chiang Mai University.

The second section of this paper discuss ethical issues in social networking can cases in Thailand. The survey methodology and results are represented in the third section. Then, the fourth section discuss the results. Finally, the fifth section concludes the paper.

2. ETHICAL ISSUES ON SOCIAL NETWORKING

It is undeniable that there are risks from the use of social networking. This research mainly focuses on ethical risks which have impacts on individual level.

2.1 Loss of Privacy

Loss of privacy is arguably the most anticipated risks during the recent years. This can surface from various situations, such as leakage of personal information from the providers, either intentionally or deliberately. Emerging technologies such as the use of geolocation also adds the vulnerability to the users [4]. As a result, the social network users are left vulnerable from unsolicited acts. Advertisement is one of the most common form of unwelcome approach from loss of privacy [5]. Yet, it mostly provides minor disturbances. On the other hand, loss of privacy could lead to other more serious problems such as identity theft or social engineering which could lead to major loss of social status, money or life-threatening cases.

Thai Netizen Network reported that several privacy issues recently took place in Thailand [6]. For example, in 2013, an online payment system accidentally leaked the email list of its customers. In addition, there were cases that some companies disclosed their customer's information to their partners, resulting in involuntary activities. Leaked information from unprotected online databases or systems were also reported [6].

2.2 Impersonation

Impersonation or identity theft is an online mimicry of a person for indecent reason. Actually, this can be easily and very quickly done without gaining authentic information from the real users. Indeed, with appropriate information, identity theft can be even more convincing. Being a victim of identity theft leads to loss of money or compromised security [7].

There are a number of impersonation cases in Thailand. The objectives of this misbehavior vary from comedic to criminal. A wide range of impersonate identity is also found [8]. There have been cases which criminals fake identities of celebrities, businesspersons or government offers for a mass fraud. For example, there are more than 50 fake Facebook pages for a businessperson who is famous in lucky draw activities. Some of them edit their profile pictures so they are looked like a verified identity. Interestingly, some of them have more than 150,000 followers. These fake pages usually make the people believe that they somehow won a lucky draw and need to transfer a small amount of money to certain accounts to verify themselves [9].

2.3 Scamming and Phishing

Scamming and phishing involve online mimicry similar to impersonation. However, instead of an impersonation, this case escalates to the level of a business entity. In general, scamming and phishing can be seen in the form of a fake website or business contact which is directly copied from the authentic source. The offered appearance and feeling of the fake and the real services are indifferent. The only noticeable inconsistency is usually the URLs of the phishing sites which would slightly deterred from the genuine ones.

Online banking is one of the main target for scamming and phishing in Thailand. There have been reports on phishing sites which is visually a duplication of the authentic ones [10].

2.4 Misinformation

News and information circulate and penetrate extremely quickly in modern social networks. Misinformation denotes news and information which is incorrect, either intentionally or unintentionally. It is literally an upgraded version of traditional hoax with additional bad intentions. Spreading of misinformation lead to misconception towards knowledge, individuals, or perceptions. Social network users are vulnerable to misinformation since sharing them can be done very easily. Without careful considerations, misinformation from friends, networks or well-known sources can be quickly perceived as authentic. This deteriorates public knowledge as a whole. Unfortunately, spreading of corrective information seems to be slower.

In Thailand, despite there is a law against spreading of false information, misinformation is commonly circulated in social networks. Basic hoaxes like ‘using something to cure some disease’ or ‘something cannot be eaten along with something’ cases are there. The more serious misinformation is used for political intentions and this leads to major breakdown in general community.

2.5 Malicious Software

Viruses, worms, spywares and other forms of malicious software can cause damage to computer systems. Preventing selves from this unethical act can be complicated since new malicious software are released endlessly. More than 400 million malicious software elements were discovered in 2015 [11]. Amongst these malicious software, the latest form of attack is arguably the “ransomware” and it has recently become a major problem to the community [12].

There have not been reports on major malware cases in Thailand. However, attacks on individual level are found everywhere.

2.6 Cyberbullying

Cyberbullying is the abuse of social network to humiliate, harass or threaten another person [13]. Generally, this happens to younger persons and usually results in the victims’ deteriorated psychology. Serious cases of cyberbullying can lead to violence or even suicidal acts. Related misbehaviors, such as racism and sexism, may also be considered as cyberbullying in a broader context.

A report indicated that 35% of Thai youths involve in cyberbullying, either the actors or the victims [14]. Fortunately, no serious cases on cyberbullying have been yet reported. Nevertheless, this figure shows an alarming potential of this risk and highlights how quickly it should be mitigated.

2.7 Hacking

Hacking and other forms of technical attacks can cause major damage to computer systems. It could happen to anyone or any organizations. A number of hacking tools is distributed around the Internet so basic hacking, such as dictionary attack, can be performed rather easily without real technical knowledge. Serious incidents such as the hacking of major networks have been reported during the recent years [15]. These led to many related ethical risks.

Major hacking incidents also periodically affected Thailand. Recently, a group of Internet users showed dissident against a government policy by attacking several legislative websites [16]. The attack was, in fact, performed by the most basic action, i.e. normal but repeatedly refreshing of the websites. However, when this is done with voluminous users, it became a major distributed denial of service (DDoS) attack which ultimately crashed the systems. This shows the vulnerability of the systems and databases run by the government.

2.8 Piracy

The nature of sharing on the Internet usually cause violation in intellectual property rights. Certain download services, peer-to-peer protocols such as BitTorent are major threats to the copyrights owners.

It has been reported that software piracy is still common [17]. The use of unauthorized contents does nothing but damages to innovation industries.

Rates of illegal software installation in Thailand is gradually declining [17]. Yet, the rate of 69% illegal installation is still unacceptable. There are also a widespread of unauthorized content sharing amongst social networks and other online services which periodically leads to arguments on the society.

2.9 Plagiarism

Plagiarism is the act of taking certain contents and use them as own idea without a proper citation. It has been considered as one of the worst misconducts in academic society. With the current Internet technology and the enormous resources of knowledge, it is increasingly convenient to commit a plagiarism.

In Thailand, it is reported that the seriousness of plagiarism is well aware in the academia. However, due to certain excuses, such as language proficiency or imminent deadline, it is still conducted by a number of people [18]. Detection systems has been implemented in many higher study institutions with an intention to reduce this problem [19].

2.10 Spamming

Generally, the main objective of spamming is advertising. Apart from spam email which has been rather common since the beginning of the Internet, spamming on social network is increasingly committed. Unlike other ethical misconducts, spamming does not directly result in serious consequences. Most of the time, it is considered as an online nuisance. However, spamming can sometimes involve malicious software which further cause problems to the users.

There has been no reports on serious case from spamming on social network in Thailand. Yet, arguably the most impactful scenario is the spamming of chain marketing network which result in loss of money, time and opportunity.

2.11 Trolling

Trolling is an act of ignorance users who intend to incite the online community. Usually this is committed just for a pleasure. However, it is possible that the agitated conversation can lead to broader level of arguments and resulting in disharmony amongst the related users. It is reported that trolling can be found more easily on social networks which do not require real identity, such as Twitter [20].

Trolling is common in popular Thai websites. Many times, it caused commotions in the community. General successful trolling subjects in Thailand involve political views, academic institutes, sports, and celebrities.

2.12 Clickbait

Clickbait has recently been a technique to lure users to visit certain websites. It usually appears as a link with a very intriguing but incomplete name. After the user clicked the link, he or she will find a number of advertisement with the shallow or, many of the time, plagiarized contents. It is highly possible that clickbait may be associated with malicious software and consequently harm the users.

Clickbait has become an increasingly popular marketing technique in Thailand. It is astonishing to find that a clickbait website successfully became the second most visited websites of Thailand during the early of 2015 [21].

2.13 Inappropriate Contents

Inappropriate contents involve pornography, vandalism, violence, gambling and etc. which are deemed unsuitable to certain group of users or cultures. Obviously, these contents are spreading around the Internet and social networking sites. Installing certain mechanisms can partly help preventing such access. However, tools such as virtual private network can still allow users to retrieve inappropriate contents.

The Royal Thai Government has installed a national firewall which protect users against browsing to certain websites [22]. Yet, its effectiveness is still doubtful since a large number of inappropriate websites are still accessible.

2.14 Witch Hunting

Online witch hunting is a social trial on certain entity. It is similar to cyberbullying but with a larger group of accuser and virtually stronger consequence. Witch hunting is usually based on bias, agitation, speculation, or misinformation. Innocent persons can be wrongfully condemned from this unethical activity. Recent cases of witch hunting led to major false allegation on impeccable victims [23].

In Thailand, there have been cases on online witch hunting which involve personal behaviors, accidents, crimes and different political views [24]. Some of them lead to social sanction to certain persons or organization while some of them later judged not guilty by the court of laws.

2.15 Disagreement Lacking Dialectic

Disagreement lacking dialectic is an intensified version of online arguments. Unlike witch hunting or cyberbullying, this ethical issue involves a dispute of at least two parties who have completely different perceptions on the same subject and they are not listening to each other's opinion.

Disagreement lacking dialectic is commonly found in Thailand's major social network websites. Recently, the main debate revolves around political parties, celebrities, religions and spirits, and trendy events. It is unfortunate that most disagreement lacking dialectic do not end well with mutual agreements but rather loose ending arguments.

3. PERCEPTION ON ETHICAL ISSUES FROM UNDERGRADUATE STYDENTS, CHIANG MAI UNIVERSITY

To study the perceptions towards the ethical issues, a survey was conducted in Chiang Mai University. Three hundred and eighty seven undergraduate students who enrolled in the "Internet and Online Community" elective course participated in the study. The students were from various faculties and various study years. All of them were familiar to social networking and major online services.

Prior to the survey, the students joined a lecture on online ethics. All fifteen ethical issues in the previous section were discusses along with their case studies. After the session, the students were asked to identify their perceived worst ethical misconduct and reasons. Fig. 1 lists the ranked percentage summary of the answers. It is important to note that seven of the feedbacks contains more than one ethical issues therefore each item is counted as one separated feedback, resulting in a total of 397 feedbacks.

It can be seen from Fig. 1 that the worst perceived ethical misconduct is, not surprisingly, the loss of privacy. The participated students reveal that they fear that, especially according to case studies, the leak of their personal information can lead to several misfortunes. One of the major concern on this issue is the risk may not be caused by the users' careless but from the involuntary change in the providers' policy. Some of them also indicated that they were surprised to learn that normal social activities, such as posting status or photos with geolocation information, can unfortunately be used to initiate serious crimes.

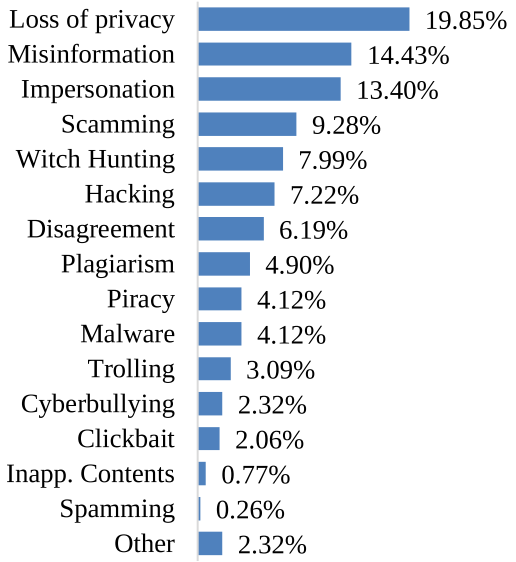

Fig. 1 Percentage of worst ethical misconduct perceived by undergraduate students from Chiang Mai University, Thailand.

Misinformation is ranked as the second worst ethical issues in social networking. This unexpected finding reflects the growing concern on abusing of social networks in Thailand. Two major scenarios in misinformation are specially denoted from the feedback. Firstly, the fault information on daily activities, especially on foods or medicines, such as the use of Formaldehyde for food preservation without evidence, may lead to major misconception. This, most of the time, can affect related businesses. A serious cases of this, such as a fault advertisement on weight-loss drugs, could lead to life threatening scenarios. The second misinformation case is related to politics. This exposes the current major unstable politics in Thailand where misinformation become an efficient tool to condemn the oppositions. More importantly, this case can be very detrimental because they are mostly created deliberately. The students were especially concern that social networks help spreading these cases of misinformation very quickly and widely.

The third and the fourth misconducts are related and may be even considered as the same issue from some perspective. If being counted together, impersonation and scamming will be ranked the most concerned ethical issue instead of loss of privacy. Yet, in this research, they are separated based on their practices. Impersonation, as a mimicry of a person, is perceived by the students as the third most serious misbehavior. Students commented that due to the ease of acting as another person on the social network, this risk is extremely apprehensive. The fact that it takes only minutes to almost perfectly duplicate an account makes them realize this imminent threat. On the other hand, scamming and phishing take considerable more efforts to make themselves credible. Students also indicated that it seems to be slightly easier to notice the unauthentic elements of these fraud. This includes suspicious URLs, emails, phone numbers or other means of contact.

Witch hunting is ranked fifth on the list. The participants denoted that the judging on other people by community bias is unacceptable. Some of them added that the result of witch hunting can be enormous to the victim, therefore, it is best to refrain from such actions. If inevitable, the students insisted that they will need information from various stakeholders before making the decision.

The sixth ethical issue, hacking, is a top concern for more than 7% of the participated students. Many of them reported that they fear of hacking because they feel this threat is out of their control. Yet, some of the students learnt that one of the easiest but effective basic mitigation towards hacking is the strength of their password and how easy the dictionary words can be hacked.

Disagreement lacking dialectic has been a common source of online arguments in Thailand. It is ranked ninth in this research. The students agreed that bias from different backgrounds or different perspectives can exacerbate the disagreement. This ultimately leads to disruption in the community. Few students suggested that such threat is best mitigated by disregarding the entire scenario. On the other hand, some other students argued that they would try to learn from all perspectives and support the most rational side of the argument.

Plagiarism is the tenth ranked ethical concern in this research. Several students admitted that they just realized the impact of plagiarism and why it is deemed unacceptable in the international level from the lecture. As a result, they promised not to commit this action and will help spreading the appropriate action against this case to their networks.

Other ethical issues were considered the worst misconduct by comparatively less students than the aforementioned items. Yet, it is undeniable that all of them can bring serious consequences and should all be mitigated. Apart from the previously discussed items, the students also proposed that some other issues, such as dishonesty and lack of moral judgment, could lead to undesirable outcomes.

4. DISCUSSION

The results of the survey depict how a group of Thai students perceived risks that came with the use of social networks and how significant those issues are to them. Loss of privacy, misinformation and impersonation, scamming and phishing are ranked on the top. The case studies on these issues can be found more often from news media including social media. When it became viral or spreads out on social networks, people feel its presence, and start to realize that these types of threats exist. Once the similar cases are speared on their social network feeds, they start to perceive its seriousness and significance of the problems. Because the negative effects of these issues to other individuals involved are usually made public on social networks, people can relate those effects to what may have happened to themselves if they come across such the cases. That makes them feel more vulnerable to those threats and lead to them relate to those issues more than the others.

On the contrary, witch hunting, hacking, disagreement lacking dialectic, plagiarism, piracy, malware, trolling and cyberbullying are the issues that mostly effects on particular groups of people such as political support group, sport fan group and users of the website. People who are not a part of such groups are unlikely to be affected. Therefore, the chance for them to realize the trouble of these issues are less than the issues listed on top. Moreover, the participants who took this survey are students whom may not have experience with witch hunting, hacking or disagreement lacking dialectic.

Clickbait, inappropriate contents and spamming are not considered the worse issues because the effects of the issues are not as serious as the others. Some people does not realize what appears on their social page as a spam or inappropriate. They rather get used to it or does not feel the appropriateness. Clickbait is not much of a big problem similar to spamming when a person does not feel it is a problem. Those who click through did because they were interested in what they see or read. So they are likely to accept the consequence.

5. CONCLUSION

The survey result reveals that the participated undergraduate students believed that loss of privacy, misinformation and impersonation are as the top most serious ethical issue in social networking. Issues ranked from the fourth place down to the floor include scamming and phishing, witch hunting, hacking, disagreement lacking dialectic, plagiarism, piracy, malware, trolling, cyberbullying, clickbait, inappropriate contents, spamming, respectively. It is interesting to repeat this survey in a boarder population and diverse culture, which will reflect the perceptions of the more general social network users.

6. REFERENCES

[1] Statista, “Number of Worldwide Social Network Users 2010-2019,” Statista, 2016. [Online]. Available: http://www.statista.com/statistics/278414/numb

er-of-worldwide-social-network-users/. [Accessed: 07-Jun-2016].

[2] Mao J and Shen Y, "Cultural Identity Change in Expatriates: A Social Network Perspective," Hum. Relations, vol. 68, no. 10, pp. 1533–1556, 2015.

[3] Digital Advertisting Association of Thailand, "Thailand Social Media Landscape," Digital Advertisting Association of Thailand, 2014. [Online]. Available: http://syndacast.com/wp-content/uploads/2015/01/Thailand-Social-Media-Landscape.pdf. [Accessed: 07-Jun-2016].

[4] Armerding T, "RSA: Geolocation Shows Just How Dead Privacy Is," CSO, 2016. [Online]. Available: http://www.csoonline.com/article/3040374/security/rsa-geolocation-shows-just-how-dead-privacy-is.html. [Accessed: 13-Jun-2016].

[5] Tucker CE, "Social Networks, Personalized Advertising, and Privacy Controls," J. Mark. Res., vol. 51, no. 5, pp. 546–562, 2014.

[6] Thai Netizen Network, "Online Privacy Violation in Thai Community," 2014.

[7] S. Hinde, "Identity Theft: Theft, Loss and Giveaways," Comput. Fraud Secur., vol. 2005, no. 5, pp. 18–20, 2005.

[8] Thairath Online, "Impersonation: It Can be Easily Done Online. Is This True?," Thairath Online, 06-Aug-2014.

[9] Komchadluek Online, "Warning on 21 Fake 'Ichitan' Facebook Pages," Komchadluek Online, 31-Mar-2016.

[10] Siam Commercial Bank, "Beware of Phishing," Siam Commercial Bank, 2016. [Online]. Available: http://www.scb.co.th/en/about-scb/phishing-mail. [Accessed: 13-Jun-2016].

[11] Symantec, "2016 Internet Security Threat Report," 2016.

[12] Trend Micro, "Ransomeware One of the Biggest Threats in 2016," Trend Micro, 2016. [Online]. http://blog.trendmicro.com/ransomware-one-of-the-biggest-threats-in-2016/. [Accessed: 14-Jun-2016].

[13] Bastiaensens S, et. al., "Cyberbullying on Social Network Sites: An Experimental Study into Bystanders' Behavioural Intentions to Help the Victim or Reinforce the Bully," Comput. Human Behav., vol. 31, pp. 259–271, 2014.

[14] DTAC Insight, "The Spreading of Cyberbullying: An Online Threat," Brand Buffet, 2016. [Online]. Available: http://www.brandbuffet.in.th/2016/02/cyberbullying-dtac-internet-behavior/. [Accessed: 14-Jun-2016].

[15] Broder JM, "Hacking Inquiry Closes With Mystery Unsolved," The New York Times, 18-Jul-2012.

[16] BBC News, "Thai Government Websites Hit by Denial-of-Service Attack," BBC, 01-Oct-2015.

[17] Business Software Alliance, "Seizing Opportunities Through License Compliance: BSA Global Software Survey," 2016.

[18] Charubusp S, "Plagiarism in the Perception of Thai Students and Teachers," Asian EFL J. Prof. Teach. Artic., no. 87, pp. 61–81, 2015.

[19] Nagi K, "Plagiarism in Education and What We Can Do About It," Nation Multimedia, 2012.

[20] Edwards J, "One Statistic Shows that Twitter Has a Fundamental Problem Facebook Solved Years Ago," Business Insider UK, 17-Apr-2015.

[21] Truehits.net, "Truehits Statistics," Truehits.net, 2015. [Online]. Available: http://truehits.net/. [Accessed: 14-Jun-2016].

[22] Technology Crime Suppression Division, "TSCD: Technology Crime Suppression Division," Technology Crime Suppression Division, 2016. [Online]. Available: http://www.tcsd.in.th/. [Accessed: 14-Jun-2016].

[23] BBC News, "Reddit Apologises for Online Boston 'Witch Hunt,'" BBC, 23-Apr-2013.