European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.10.02.40

ICH 2019
International Conference on Humanities

THE VULNERABILITY OF YOUNG WOMEN TO CYBERCRIME: A CASE STUDY IN PENANG

Norhayati Mat Ghani (a)*, Suriati Ghazali (b)
*Corresponding author

(a) Norhayati Mat Ghani, School of Humanities, Universiti Sains Malaysia, 11800, Pulau Pinang, nrhayatighani@gmail.com
(b) Suriati Ghazali, School of Humanities, Universiti Sains Malaysia, 11800, Pulau Pinang, suriati@usm.my

Abstract

Cybercrime is an important issue that is now often discussed by the global community. The Royal Malaysian Police (PDRM) reported that the number of cybercrime cases recorded from January to October 2017 is 8,313, showing that cybercrime is a very serious and worrying issue at the moment. For this reason, this study aims to examine the vulnerability of young women in Penang to cybercrime. 150 young women were selected using purposive and snowball sampling to answer a survey questionnaire, and five among them were selected to be interviewed. The results showed that 51.3 per cent of the respondents have been victims of cybercrime. From the seven types of cybercrime activities that young women often experience (i.e. sexual harassment, fraud, slander, blackmail, hacking, verbal abuse and bullying), sexual harassment and fraud are the most common cybercrimes encountered by the respondents. Descriptions of their experience with these two crimes were examined further through the interview. This study contributes to knowledge on the vulnerability of young women to cybercrime which can be extended to geography of crime studies.

Keywords: Cybercrime, young women, vulnerability, victim.

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The misuse of social media has created a new culture of cybercrime among the global community (binti Bidin et al., 2015; Termimi et al., 2013; Yar, 2012). Users of social media are potentially exposed to cybercrime, with women more likely to be targeted as victims. In other words, social media has led to an increase in women's vulnerability to cybercrime (Kamruzzaman et al., 2016; Ghazali & Ghani, 2018). *Vulnerability* here means that these women are exposed to the possibility of being attacked or harmed, either physically or emotionally. Social media platforms such as WhatsApp, Facebook, Instagram, WeChat and Twitter now allow women to meet anyone they want and this can lead to increased risk of cybercrime (Pitchan et al., 2017). It has become quite common for them, young women especially, to get acquainted with strangers on social media. After they have become acquainted in cyberspace, the cybercriminals will try to establish a romantic relationship with the victim before committing crimes such as cheating, extortion, bullying and sexual harassment (Guan & Subrahmanyam, 2009; Halder & Jaishankar, 2009; Mohamad & Tan, 2012). According to a statistics released by the Department of Commercial Crime, 8,313 cybercrime cases have been recorded by the Royal Malaysian Police throughout January to October 2017. This figure shows that cybercrime has become a very serious issue in today's society.

2. Problem Statement

Social networking sites have become part of people's lives today and this has encouraged new ways to communicate and share information. However, the misuse of social media has raised concerns over the consumers' safety, especially women's as they are the main users of social media (Greenwood et al., 2016; Lenhart et al., 2011). The involvement of young women in social media and their interest to use it has made them vulnerable to cybercrime, where 8 out of 10 women are reported to have been victims of cybercrime from using social networking sites (Tandon & Pritchard, 2015). The Cyber Security and Crime Division also reported that 70 per cent of cybercrime victims in Bangladesh are women, with 57 per cent of them between 18 and 25 years of age (Dhaka Tribune, 2019). The types of cybercrimes reported are fraudulent online purchases, hacking, sexual harassment, defamation, social media rape and the distribution of pornographic images (Boone, 2011; Jain et al., 2012; Reznik, 2013). Another frequent cybercrime aimed mainly at women is the "African scam", in which a man claims to be a wealthy European who is looking to have a relationship with a local woman. Later, he tricks the woman by saying that he had sent valuable items to the woman and asks the woman to deposit a certain amount of money into a bank account for the purpose of releasing the items from the customs (Ismail & Aziz, 2019; Mohamad & Tan, 2012).

These cybercriminal cases have caused a great loss to the victims. According to the Ministry of Communications and Multimedia, cybercrime has caused a loss of RM67.6 million based on 2,207 complaints received nationwide in the first three months of 2019. Three highest cases of cybercrime recorded are fraudulence via telephone calls resulting in the loss of RM26.8 million (773 cases), online shopping frauds amounting to RM4.2 million of loss (811 cases) and "African scams" resulting in the loss of RM14.9 million (371 cases) (Star Online, 2019). Cybercrime is a serious threat to young women as

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

they are often involved in online shopping activities and scams that specifically target them such as the African scam.

One of the reasons young women are vulnerable to cybercrime is that they are easily influenced by the features available on social networking sites such as the photo sharing feature (Ibrahim, 2014). According to a study by the Pew Research Centre (2013), 60 per cent of women like to share pictures on social networking sites, and this exposes them to cybercrime risks since the images can be accessed by anyone including cybercriminals for a variety of purposes such as hacking, editing and turning the photos into sexually explicit photos with the intention of threatening, bullying or disgracing the victims (Ebong et al., 2015; Smith et al., 2008), thus putting a pressure on them and causing them distress (Dewan Pelajar, April 2012).

Women are also more likely to have more faith in online shopping without taking into account the risks involved (Yazid et al., 2016). While making a purchase, most women buy based on the external form of the product or service such as pictures, textual information and video clips, which are not always the actual product description (Kolesar & Galbraith, 2000; Yazid et al., 2016). Their tendency to be attracted to advertisements on the social media results in them becoming victims repeatedly. In Malaysia, statistics shows that 3,821 online fraud cases were reported in 2017 (MyCERT, 2017). This figure has yet to include the many more cases that victims of online scams chose not to report. Monetary scams are expected to continue to grow along with further advancement of the technology and the internet.

Most studies discussed above focus on women in general, regardless of age group. However, studies focusing on young women's vulnerability to crime, especially those within the age of 18-29 years old, are still scarce. Since women of this age group form the largest proportion of the global internet users (Lenhart et al., 2010), including in Malaysia (Ibrahim, 2014), a study specifically investigating this age group's experience of being victims of cybercrime is important. Furthermore, there is a lack of discussion on the experience of young women who are victims of cybercrime in the Malaysian academia. Therefore, this study fills in the research gap on Malaysian young women's vulnerability to cybercrime. This study would contribute to knowledge on the vulnerability of young women to cybercrime and can be applied in geography of crime studies.

3. Research Questions

Based on the review of literature, this study asks two research questions:

1) What are the types of cybercrimes experienced by young women in Penang?

2) How are cybercrimes carried out on young women in Penang such as described by the victims?

4. Purpose of the Study

The usage of social media is very widespread nowadays, which has allowed many incidents of cybercrime to happen to women. The study reported in this paper aimed to look into the vulnerability of young women to cybercrime by identifying the types of cybercrimes they were victims of and examining some instances of the incidents.

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. Research Methods

5.1. Target participants

The target participants for this study are young women between the ages of 18 and 29, and this age group was selected based on the age group of the most active social media users (Ibrahim, 2014; Lenhart et al., 2010). Perrin (2015) also states that half of the smartphone users are young people between the ages of 18 and 30.

5.2 Sampling Method

The sampling methods used were purposive and snowball. The researcher selected 150 respondents to answer the questionnaires, and five of them were selected for in-depth interviews. Purposive sampling enabled the researchers to select the right respondents who belong to the particular age group this study was investigating, and snowball sampling method helped the researchers to use information from the respondents to find the next respondents (Ghazali et al., 2012) by having several key informants introduce the researchers to other respondents with similar experience on cybercrime. Among the aspects considered was that the respondents could provide information on cybercrime through their own experience.

5.3 Data collection and data analysis

Data was collected using the mixed method. Quantitative data were analysed to look at the number of respondents who have been victims of cybercrime and to identify the types of cybercrimes experienced by the respondents. Meanwhile, qualitative data from the interviews on their cybercrime experiences were analysed and interpreted using content analysis. The latter type of data was utilised to highlight the topic discussed in this paper, which is the cybercrimes experienced by young women based on the respondents' real-life experience and point of view (Ghazali et al., 2012; Robinson, 1998).

5.4 Research ethics

To keep the confidentiality of the respondents, the names and identities of the individuals who were interviewed have been concealed when writing this paper (Ghani & Ghazali, 2015).

6. Findings

6.1. Incidence of cybercrime among the respondents

This section presents the percentage of respondents who have had experience of being victims of cybercrime. Table 01 indicates that 51.3 per cent of the respondents have been victims. Previous studies have shown that the number of respondents who have been victims of cybercrime is more often greater than those who have not. The tendency of women to become victims of cybercrime is high because they are very active on social media where they share pictures, videos and information (Greenwood et al., 2016; Ibrahim, 2014; Lenhart et al., 2011).

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Table 01. Number of respondents who were victims of cybercrime

Have the respondents been victims of cybercrime?	Total	Percentage
Yes	77	51.3
No	73	48.7
Total	**150**	**100**

6.2. Types of cybercrime that occurred among the respondents

This section analyses the rate of occurrence of seven types of cybercrimes among the respondents, namely sexual harassment, fraud, slander, blackmail, hacking, verbal abuse and bullying. Table 02 shows that the cybercrime with the highest rate of occurrence is fraud, by a total of 34 respondents. Most of the respondents said that they were scammed when they bought goods online and when they participated in online dating. This finding is supported by van Wilsem (2011) who states that online shoppers are highly at risk of becoming victims of fraud. Online fraud occurs when an internet user scams another person by selling goods or services that do not exist or are not as what the seller had promised to the buyer, and it causes a loss to the buyer (Cross et al., 2014). MyCERT (2017) reports that there have been 3,821 cases of online security incidents related to frauds including online shopping frauds, and the number of occurrences of such cases is expected to increase in the future.

Sexual harassment is the next highest occurring cybercrime, as experienced by 33 respondents. According to Wery and Billieux (2017), cyber sexual activities have increased drastically online and are frequently discussed in the community. The respondents said that the cybercriminals attempted to rope them into sexual activities such as engaging in explicit conversations, sharing sexual images and encouraging them to have sex. According to Wolak et al. (2004), most sex crimes are initiated by adult men through the internet; they use this medium to meet and seduce women, especially adolescents, and encourage them to have sex. There are also young women who have been exploited or persuaded for sexual purposes such as being forced to dress or pose sexually in front of a webcam, or asked to have sex (Halder & Jaishankar, 2009).

Meanwhile, 20 respondents claimed to have been victims of slander. Studies have shown that slander is caused by relationship problems, such as refusing to be a lover to a man, being defamed by friends and being accused as a homewrecker. As a result, the respondents have been slandered and humiliated on social networking sites.

Table 02 also shows that 5 respondents admitted to being victims of hacking. The most common type of hacking young women are subjected to is the stealing of pictures they posted on social media accounts such as Facebook. In this study, the respondents' photos were stolen and edited into obscene and sexually explicit photos for the purpose of threatening the victims. This occurrence corroborates a statement by the National White Collar Crime Center (2011) that social media is considered as a "gold mine" for criminals who would take advantage of the personal information users post on social media. Disclosing information such as pictures and personal information can pose a threat to the victims as their pictures can be stolen and edited by the cybercriminals, and then used to threaten the victims.

Meanwhile, 12 respondents indicated that they have been victims of blackmail on social sites. There are cybercriminals who take advantage of the victims by editing their pictures and threatening to

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

distribute the edited nude images if they do not pay some amount of money. There were also 12 respondents who claimed to be victims of online verbal abuse. Social media provides the channel for people to respond negatively to posts by insulting, cursing and hurling abusive words. Wolak et al. (2006) explain that the internet gives power to users to threaten other users by humiliating, harassing, verbally abusing and intimidating victims. One of the respondents was verbally abused online because of a misunderstanding caused by a Facebook post she had made, and she was also accused of being the trigger of the arguments and disputes over that Facebook post.

From the survey, four respondents confessed to have been victims of cyberbullying. Past studies found that young women became victims of cyberbullying because of what they had shared on their social media: status, pictures, events or activities such as going on a holiday or receiving presents or awards. The act of sharing information online opens up opportunities for the community to give negative comments to victims even though the sharing could have been done with a positive intention (Fauzi, 2017).

Table 02. Types of cybercrime that occurred among the respondents

Type of cybercrime	Total
Fraud	34
Sexual harassment	33
Slander	20
Verbal abuse	12
Blackmail	12
Hacking	5
Bullying	4

6.3. Description of cybercrimes that occurred among the respondents

This section discusses the respondents' vulnerability to cybercrime that led them to being victims of the crimes of fraud and sexual harassment. These two crimes were chosen to be studied in depth because they have the highest rate of occurrence among the respondents of this study (refer to Table 02). Five respondents were selected to share their experiences of fraud and sexual harassment through social media. As mentioned before, most frauds happened to them through online shopping and online dating. In the following excerpt, Respondent 1 described how she had been scammed by an online seller when the clothes she received were smaller in size than the measurements advertised by the seller. This made the clothes unusable because they could not fit her. The respondent also expressed her regret for making the purchase online.

> "*I was scammed when buying clothes from an online seller. The blouse I ordered was not same as what I received… When I received the clothes, they were really small and did not follow the size provided by the seller. I regret buying this online. If I had bought the clothes in a store, I would've received better clothes.*" (Respondent 1, aged 21)

The response above shows that there are online sellers out there who provide inaccurate information about the goods they sell. If the information had been presented correctly, the buyer would not have had problem evaluating the items they wish to purchase as they do not have to worry about

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

trusting the reliability of the information. This finding is supported by Yazid et al. (2016) and Button et al. (2014) who explained that the problem often encountered by online shoppers is that the attributes of the products received are different from the specifications given online, and therefore shoppers do not receive the products as promised by the sellers. As such, the advent of social media as a popular platform for shopping also brings problems such as fraud (Talib & Rusly, 2015).

The same issue was mentioned by Respondent 2. She relayed her experience of becoming a victim of an online shopping scam from buying a fake coffee product, in which the seller did not provide any information on the product. In the interview, Respondent 2 said that she only realised she had bought fake coffee product after tasting it. She explained that the coffee packs she purchased were different compared to the ones she had bought previously in terms of the packaging and the taste. The respondent was suspicious of the genuineness of the product; in the end, she threw away that coffee because she was worried it would cause some bad effect to her body. The following is an excerpt of the interview with Respondent 2:

> "*Before this, I always drink Perla Coffee; it suits me because it makes my skin smoother and brighter. I bought this from a different seller, not the one I bought before because this seller gave fast response. I bought up to 3 boxes to keep them for future use. When the items arrived, I felt weird because the packaging of the box and the taste were completely different from the one I drank before. I only drank one sachet of coffee and then threw the rest away. Before anything happens to my health, I should stop drinking it.*" (Respondent 2, aged 24)

Apart from online shopping scams, cases of online dating scams or African scams are alarming, and this number is increasing every year (Pitchan et al., 2017). Mohamad and Tan (2012) explain that syndicates from abroad scam women for various purposes such as extortion, sex trafficking and money. Young women become victims because they are more trusting of other people, even those who are strangers to them. Respondent 2 told how her adopted sister had been a victim of this scam orchestrated by a syndicate from overseas:

> *"My adopted sister was deceived by a fraud syndicate from abroad. He claimed to be from a European country; they met each other through Facebook. They were chatting for two weeks and the man asked her to marry him. My adopted sister is a widow. She is still young, and she has two kids. She felt lonely and tried to find a new husband. Within a month, the man said he had posted some wedding items such as diamond rings, wedding dresses, shoes and many more but the goods were detained by the customs. He asked my adopted sister to pay RM1000 to get the items released from the customs. Then, he asked for another RM4500. Later, he asked a few times more, and the total loss was RM11,000. She'd borrowed money from family members, relatives and a loan shark to get the money. She couldn't get the money to pay the loan shark, so the loan shark took her house as payment. Currently, she and her family members are living at her friend's house. She has made a police report, and the police said there were 20 cases reported recently.*" (Respondent 2, aged 24)

The response above illustrates how African scams are carried out by syndicates preying on women. The credulity of the victims towards their contacts in social media leads the victims to be easily deceived. Although they only became acquainted in a short period of time, the criminals managed to gain

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

the trust of the victims. As seen in this case, within two weeks of chatting, the cybercriminal had proposed marriage to the victim. A month later, the criminal claimed he had sent wedding gifts such as diamond rings, wedding dresses and shoes to the victim. The victim was asked to deposit some money to release the items from the customs and some additional costs before the items could be delivered to the victim. As a result, the victim even went to the extent of borrowing money from a loan shark just to get the items promised by the criminal. The victim also lost her parents' home after not being able to pay its mortgage. The experience of Respondent 2's adopted sister reflects how young women are particularly vulnerable to becoming victims of fraud. This is because they are easy to trust new people they meet on the social media, and can be persuaded to part with their property and money for the sake of the perpetrator (Mohamad & Tan, 2012).

Besides that, young women are also vulnerable to sexual harassment when they use the social media. According to the respondents, the most common kind of sexual harassment experienced by them is receiving pornographic messages and pictures from other users. One instance is Respondent 3's experience:

> "*I received explicit pictures through WeChat from a stranger. When I was online, the guy suddenly sent me an explicit picture. He didn't write any caption and just sent me that picture. I was shocked at the time, but I still didn't block him. I thought he mistakenly sent me the message. The second time I was online, once again he sent me an explicit picture, and he used an explicit picture as his profile picture. I was so scared and kept immediately blocked him.*" (Respondent 3, aged 21)

Findings from other studies have shown that social media apps like WeChat allow strangers to access the contacts of anyone near to them. Through the WeChat app, users can track other users within 20 km simply by pressing the *People Nearby* button (Liu, 2019). This shows that social media apps enable users to become victims of cybercrime whereby the users could connect with strangers without needing to know the other person's name or phone number. The respondent explained in the interview that she was sexually harassed when another user had sent sexually explicit images to her repeatedly. This harassment caused the respondent to feel scared and forced her to block that individual and turn off the People Nearby function through her WeChat account. This incident shows that by using social media apps, young women are vulnerable to cybercrime risks.

In addition, Respondent 4 revealed that when she first started to use social media, she liked to upload pictures there and post updates so as to allow her online friends to like the pictures and leave comments on the respondent's wall. However, the respondent also received sexually explicit comments after uploading the pictures and updates. The following is an excerpt from the interview with Respondent 4:

> "*When I first started to use social media, I liked to add friends even though I didn't know them. It used to be fun when I have a large number of friends in my friend list. At that time, I didn't think about the effects of social media. I posted a lot of pictures at that time and updated anything that I have done and planned to do. After that, there were some online friends who I did not recognise suddenly liking my pictures and sent sexually explicit messages. For example, he said you are beautiful, your body is sexy, and I love to see your smile and all that. If he didn't pay attention to*

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

our physical, why would he send such messages? I was very scared and immediately blocked the individuals who sent me those sexually explicit messages." (Respondent 4, aged 24)

The above response clearly shows that the respondent experienced sexual harassment while using social media. Praising the body of a woman and talking about sex are blatant acts of sexual harassment. According to Ismail et al. (2001, as cited in Wilson, 1995), sexual harassment can be non-verbal (the display of images, whistles, sexual gestures, etc.), physical (not necessarily touching the victim) and/or verbal (obscene comments about clothes, looks or actions). This finding coincides with Fairbairn's (2013) study that explains that adolescents and young women are more likely to be victims of sexual harassment through the activity of uploading pictures on their social media accounts. Young women who have no problem updating personal activities they have done and their special moments on the social media makes themselves vulnerable to social media crimes.

Meanwhile, Respondent 5 reported that she had received a sexually explicit message from a Facebook friend she knew for quite some time. According to the respondent, at the beginning of her friendship with this user, they only had normal interactions, and he did not show any suspicious behaviour. However, after being friends for a while, this user started to show his real intention by sending sexually explicit messages and making a sex video call to her. This behaviour is explained by Wolak et al. (2004) and Yar (2006) in which during the early stage of the introduction, sexual offenders will try to establish a relationship by asking about normal things and acting normally when interacting with the victims. Only after establishing the relationship will the sexual offender attempt to encourage the victim to engage in sexual relations and show his sexual misconduct behaviour to the victim. The following is an excerpt detailing the harassment Respondent 5 had experienced:

"I have received sexually explicit messages from my Facebook friend. When we first became friends, we just had normal chats about ordinary things and I thought he's a good person. We chatted several times because I felt that he did not show any weird behaviour. After a while, he started acting weird and he sent me a message asking me to have sex with him. He also made a video call to me; he had made several video calls to me before but we had normal conversation, but later he started to show his real behaviour. In the last video call before I blocked him, he showed his genitalia to me and played with it" (Respondent 5, 22).

The above response shows that the development of social media has changed the attitude of even the Eastern communities who previously considered sexual behaviours and discussion on sex as a taboo in the society. However, due to inappropriate use of the social media, immoral and outrageous acts that violate Eastern values, customs and religions such as showing genitals to other people are becoming rampant. Social media entices the users to commit inappropriate and immoral behaviours and it influences the sexual behaviours of members of the society. However, the respondents who were interviewed did not respond to the sexual requests of the perpetrators. The respondents also expressed feelings of fear and worry for being victims of sex crimes that caused them to block the perpetrators.

7. Conclusion

The results of this study's survey have shown how more than half of the respondents were vulnerable to cybercriminal activities, with fraud and sexual harassment being the most common crime

they had experienced, followed by slander, verbal abuse, blackmail, hacking and bullying. The subsequent interview also revealed the victims' experience of the cybercrime and their fear, anxiety and regret over what had happened to them. These findings corroborate the observation that the involvement of young women in social media has given rise to the possibility of them being exposed to cybercrime risks.

One major contributor to this situation is that messaging apps and social networking sites nowadays are equipped with advanced, multifarious functions that allow users to connect with anyone including strangers, thus increasing the risk of users becoming victims of insult, slander, and defamation by other users. Another important factor to the problem faced by young women in the cyberworld is their own behaviours and attitudes. Their gullibility and lack of awareness and information in regards to the cyber environment leads to them becoming victims of fraud such as online shopping scams and the African scam. They are easily beguiled by advertisements of new products and can be too trusting of other people who they meet in the virtual world. Furthermore, their fondness for uploading pictures on social networking sites exposes them to the risk of sexual harassment, hacking and slander. Sharing their personal lives on the internet also exposes them to the risk of getting insults and criticism from other users.

However, this study only focused on young women from 18 to 29 years old, and this age group majorly comprises social media users. Therefore, the findings may not be able to represent women of other age groups. Besides that, the findings of this study emphasised more on cyber frauds and sexual harassment since these crimes had the highest occurrence among the respondents sampled in this study.

Despite the limitations, this study is able to contribute to knowledge on young women's vulnerability to cybercrime in the Malaysian context, and can be extended to geography of crime and social media studies. The findings may serve as a guide for governmental and non-governmental agencies to execute appropriate policies and measures to prevent cybercriminal activities from becoming more endemic among young women. Further research is suggested to be conducted on cybercrime against children, which are increasing today due to children's widespread accessibility to the internet and social media that potentially exposes them to cybercrime. This is because children would be even more vulnerable to cybercrime, and their usage of social media has led to attempts at grooming children and exploiting them for inappropriate purposes.

Acknowledgments

The authors gratefully acknowledge Universiti Sains Malaysia for funding this research through the RU-Team Grant for the project entitled "Spatial Inequalities – Framing Phenomena, Formulating Policies" (1001/PHUMANITI/856002), and the Geran Pembangunan Siswazah (308/ALHUMANITI /415403).

References

binti Bidin, A., binti Syed Nong Mohamad, S. N. A., & binti Mohamad, A. (2015). Intipan Siber: Jenayah Baru Dalam Masyarakat Kontemporari [Cyber stalking: A New Crime in Contemporary Society]. *Jurnal Islam dan Masyarakat Kontemporari, 11*, 12-25. https://journal.unisza.edu.my/jimk/index.php/jimk/article/view/134

Boone, J. (2011). *Criminal use of social media. National White Collar Crime*. www.iacpsocialmedia.org/Portals/1/documents/NW3CArticle. pdf

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall. Australian & New Zealand. *Journal of Criminology, 47*(3) 391–408. https://doi.org/10.1177/0004865814521224

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends & Issues in Crime and Criminal Justice*, 474.

Dewan Siswa. (April 2012). *Antara buli siber dengan gangguan siber* [Between cyberbullying and cyber harassment]. http://dwnsiswa.dbp.my/wordpress/?p=397

Dhaka Tribune. (2019, April 1). *Rise in cybercrime worries women*. https://www.dhakatribune.com/ cybersecurity/2019/04/01/rise-in-cybercrime-worries-women.

Ebong, W. H. W, Yaakob, Z., Rohani, Z. H., Abidin, M., & Ibrahim, F. (2015). *Kajian tinjauan: Buli siber di kalangan mahasiswa universiti teknologi Malaysia* (pp. 1-18) [Survey study: Cyberbullying among student of University of Teknology Malaysia]. Retrieved from http://eprints.utm.my/id/eprint/61429/1/WanHassanWan2015_KajianTinjaunBuliSiberDiKalangan Mahasiswa.pdf

Fairbairn, J. (2013). *Sexual violence and social media,* (August Edition). Retrieved from http://www.violenceresearch.ca/sites/default/files/FAIRBAIRN%2C%20BIVENS2013_0.pdf

Fauzi, N. (2017). *Penggunaan media sosial dalam dunia tanpa sempadan: suatu kebaikan atau keburukan)* [The use of social media in a borderless world: Good or bad]. http://www.ilkap.gov.my/download/kertaspenyelidikan/PMSDDTS18122017.pdf

Ghani, N. M., & Ghazali, S. (2015). Tindak balas pengguna youtube terhadap kes buli dalam kalangan remaja di Malaysia [Youtube users' response to bullying cases among teenagers in Malaysia]. *Sains Humanika, 6*(1), 9–17.

Ghazali, S., Mapjabil, J., Nor, A. M., Samat, N., & Jaafar, J. L. S. (2012). Difusi ruangan budaya transeksualisme dan imaginasi geografi pelajar lelaki berpenapilan silang di universiti tempatan Malaysia [Spatial Diffusion of Transsexualism and Geographical Imagination of the Cross-dressed Male Students in Malaysian Local Universities]. *Journal of Social Sciences and Humanities*, *7*(1), 252-266.

Ghazali, S., & Ghani, N. M. (2018). Perception of female students towards social media-related crimes. *Pertanika Journal of Social Science and Humanities, 26*(2), 769-786.

Greenwood, S., Perrin, A., & Duggan, M. (2016). *Social media update 2016: Facebook usage and engagement is on the rise, while adoption of other platforms holds steady.* http://www.pewinternet.org/2016/11/11/social-media-update-2016/

Guan, S. S. A., & Subrahmanyam, K. (2009). Youth internet use: Risks and opportunities. *Current Opinion in Psychiatry*, *22*(4), 351–356. https://doi.org/10.1097/YCO. 0b013e32832bd7e0

Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. *Temida*, *12*(3), 5–26. https://doi.org/10.2298/TEM0903005H

Ibrahim, M. (2014). Wanita dan penggunaan media sosial [Women and social media user]. *Buletin Persatuan Wanita UKM* (Suaranita). Vol. 69. http://www.ukm.my/sukmanita/files/Suaranita-Bil-69.pdf

Ismail, Z., & Aziz, A. (2019). Jenayah cinta siber di Malaysia: suatu penelitian terhadap pengalaman mangsa [Love Scam in Malaysia: The Exploration of Victim Experiences]. E-Bangi *Journal of Social Science and Humanities, 16*(4), (1-10).

Ismail, Z., Mohd, H., Malik, A., & Achro, M. (2001). *Gangguan seksual di tempat kerja: Definisi, kesan dan langkah mengatasinya [Sexual harassment in the workplace: Definitions, effects, and measures to overcome]*. http://repo.uum.edu.my/449/1/Zakaria_Ismail.pdf

Jain, M. R., Gupta, P., & Anand, N. (2012). Impact of social networking sites in the changing mindset of youth on social issues – A Study of Delhi-NCR Youth. *Journal of Arts, Science & Commerce,* 3(2 Part 2), 36-43.

Kamruzzaman, M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cyber crime in South Asia. *American Journal of Information Science and Computer Engineering, 2*(4), 22-28.

Kolesar, M. B., & Galbraith, R. Y. (2000). *A services-marketing perspective on e-retailing: implications for e-retailers and directions for further research, 10*(5), 424-438. https://doi.org/10.1108/10662240010349444

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011). Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of" Digital Citizenship". Pew Internet & American Life Project. http://www.pewinternet.org/files/old-media/Files/Reports/2011/PIP_TeensKindnessCrueltySNS_ ReportNov2011_FINAL110711.pdf

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). *Social media & mobile internet use among teens and young adults. Pew Research Center.* http://www.pewinternet.org/files/oldmedia/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf

Liu, X. (2019). Privacy exposure on WeChat from users' perspective: A study among the university students in China. https://api.semanticscholar.org/CorpusID:210553457

Mohamad, R., & Tan, S. M. (2012). Tipu alaf baru [Scam! new millennium]. *BULETIN ICT*, Edisi 2/2012. http://www.treasury.gov.my/pdf/buletin ICT/Edisi22012.Pdf

MyCERT. (2017). *MyCERT incident statistics.* https://www.mycert.org.my/statistics/ 2017.php

National White Collar Crime Center. (2011). Criminal use of social media (2011). https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/Criminal%20Use%20of%20Social%20Media.pdf

Perrin, A. (2015). Social media usage: *2005-2015 65% of adults now use social networking sites – a nearly tenfold jump in the past decade*. Pew Research Center. http://www.pewinternet.org/files/2015/10/PI_2015-10-08_Social-Networking-Usage-2005-2015_FINAL.pdf

Pitchan, M. A., Omar, S. Z., Bolong, J., & Ghazal, A. H. A. (2017). Analisis keselamatan siber dari perspektif persekitaran sosial: Kajian terhadap pengguna internet di Lembah Klang [Analysis of Cyber Security from the Perspective of Social Environment: A Study of Internet Users in Klang Valley]. *Journal of Social Sciences and Humanities, 12*(2), 16–29.

Reznik, M. (2013). Identity theft on social networking sites: Developing issues of internet impersonation. *Touro Law Review,* 29(2), 455–483.

Robinson, G. M. (1998). *Methods and techniques in human geography*. Wiley.

Smith, P. K., Nahdavi, J., Carvalh, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyber-bullying: its nature and impact in secondary school pupils. *Journal Of Child Psychology And Psychiatry*, 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Star Online. (2019, April 24). *RM67.7mil lost due to cybercrimes early this year*. https://www.thestar.com.my/news/nation/2019/04/24/rm676mil-lost-due-to-cybercrimes-early-this-year

Talib, Y. H. A., & Rusly, F. H. (2015). Falling prey for social media shopping frauds: The victims' perspective. *Proceeding of the International conference on E-Commerce* (pp. 1-7). Sarawak, Malaysia. https://www.researchgate.net/publication/286921423_Falling_Prey_for_Social_ Media_ Shopping_Frauds_The_Victims'_Perspective

Tandon, N., & Pritchard, S. (2015). *Cyber violence against women and girls: A world-wide wake-up call.* https://en.unesco.org/sites/default/ files/gender report2015final.pdf

Termimi, M. A. H., Rosele, M. I., Meerangani, K. A., Marinsah, S. A., & Ramli, M. A. (2013). Jenayah siber: Pengelasan di antara Al-Jaraim dan Al-Jina'I menurut sistem perundangan Islam [Cybercrime: Classification between Al-Jaraim and Al-Jina'I according to Islamic legal system]. *International Seminar on Islamic Jurisprudence in Contemporary Society*, 539–551. http://eprints.um.edu.my/id/eprint/13068

Wery, A., & Billieux, J. (2017). Problematic cybersex: Conceptualization, assessment, and treatment. *Addictive Behaviors*, *64*, 238–246.

Wilsem, J. (2011). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European sociological review, 29*(2), 168-178.

Wilson, F. M. (1995). *Organization Behaviour and Gender*. McGraw Hill.

Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization of youth, five years Later*. http://www.unh.edu/ccrc/pdf/CV138.pdf

https://doi.org/10.15405/epsbs.2020.10.02.40
Corresponding Author: Norhayati Mat Ghani
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, *35*, 424.e11–424.e20.

Yar, M. (2006). *Cybercrime and society*. Sage.

Yar, M. (2012). E-Crime 2.0: the criminological landscape of new social media. *Information & Communications Technology Law, 21*(3), 207-219.

Yazid, Z., Wel, C. A. C., & Omar, N. A. (2016). Persepsi mahasiswa terhadap urusan pembelian atas talian [University Student's Perspective on Online Transaction]. *Jurnal Personalia Pelajar*, *19*(2), 17-25.