INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 9, (2023) E-ISSN: 2222-6990

Women's Engagement in Social Media and their Susceptibility to Cybercrime Victimisation

Norhayati Mat Ghani
School of Education, Universiti Sains Malaysia, 11800 Pulau Pinang

Mohd Azmeer Abu Bakar
School of Humanities, Universiti Sains Malaysia, 11800 Pulau Pinang
Email: azmeerm@usm.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i9/18415 DOI:10.6007/IJARBSS/v13-i9/18415

Published Date: *08* September 2023

Abstract

Women are active participants in the world of social media, using platforms like Facebook, Instagram, Twitter, TikTok, and more to connect, share, and communicate. Women often use these platforms to share their experiences, sharing photographs and statuses, engaging in online shopping activities, and establishing new connections. Unfortunately, women also face higher susceptibility to various forms of cybercrime victimization due to the dynamics of online spaces. Women can be targets of online harassment, including cyberbullying, threats and sexual harassment. The objective of this study is to investigate the propensity of adolescent females who fall prey to cybercriminal activities as a result of their engagement with social media platforms. The research employs for quantitative and qualitative method. A total of 137 young women (18 – 29 years old) completed a survey questionnaire, while ten individuals were subjected to in-depth interviews. Random and purposive sampling methods were employed in this study to acquire a study sample from the women who stay at Penang, Malaysia. This study employs descriptive analysis and content analysis as the primary methods of analysis. The study revealed that there were two specific behaviours that rendered women susceptible to cybercrime. Specifically, 55.5% of the participants fell victim to cybercrime as a result of engaging in chatting activities, while 48.1% of the respondents experienced victimisation due to browsing Facebook activities. Based on the research findings, a major percentage of participants (42.2%) indicated that they have experienced cybercrime due to easy accepting new friends thru Facebook. Further research can be conducted pertaining to vulnerable groups, specifically children and the elderly, who experience victimisation in cybercrime. This behaviour could potentially be attributed to the susceptibility of children, who are vulnerable to being exploited and groomed in the online environment. The incidence of cybercrime targeting older people also is on increasing in Malaysia. Hence, it is imperative to conduct a comprehensive examination of this vulnerable groups. This study makes a valuable contribution to the existing body of knowledge on the

current cybercrime landscape targeting young women. Its findings have the potential to assist stakeholders in effectively managing and mitigating the risk of young women falling victim to cybercrime.
Keywords: Activities, Young Women, Victimization Tendencies, Cybercrime, Facebook

Introduction

Social media serves as an online platform for individuals to engage in interactive communication (Steinkuehler and Williams, 2007; Mustafa, 2016). The utilisation of social media platforms holds significant importance within contemporary society, particularly in facilitating interpersonal connections. According to the Department of Statistics Malaysia (2020), there was an observed increase in household access to internet users from 87 percent in 2018 to 90 percent in 2019. Furthermore, the report reveals a notable surge in internet usage within Malaysia, with figures rising from 81 percent in 2018 to 84 percent in 2019. The proliferation of internet usage has led to its widespread adoption across various demographics, encompassing women as well. Maznah (2014) posits that women are inclined to utilise social media platforms as a means of establishing connections, as they perceive these platforms as affording them the autonomy and flexibility to select and engage with virtual acquaintances at their discretion. Nevertheless, it has been observed that women are more susceptible to falling prey to cybercrime because of their engagement with social media platforms (Madden and Zickuhr, 2011; Greenwood et al., 2016). The perception of women as the more vulnerable gender often results in their selection as primary targets in criminal activities, including those facilitated through social media platforms (Agenda Daily, 2021). According to the research conducted by Yar (2012); Asyraf et al (2013); Asiah et al (2015), the emergence and proliferation of new media networks have given rise to a prevalent culture of cybercrime within global society, with a particular focus on its impact on women.

The concept of cybercrime encompasses illicit activities conducted through internet networks and computer software (National Crime Prevention Council, 2012). There exist six distinct categories of cybercrimes that frequently target women in Penang, specifically encompassing personal data protection, social media crimes, telecommunications fraud, e-finance fraud, cyber love scams, and online purchases (Table 1). According to the data presented in Table 1, telecommunication fraud emerges as the most prevalent form of cybercrime affecting women, with a total of 275 reported cases in the year 2019. Cyber love fraud, with a total of 120 reported cases, ranks as the second most prevalent form of criminal activity. Online purchase fraud ranks as the third most prevalent type of fraud, with a total of 71 reported cases. According to the data released by the Commercial Crime Investigation Department, it can be observed that all three categories of cases in Penang have exhibited an upward trend on an annual basis.

Table 1
Incidences of Cybercrime Targeting Women in Penang, 2019

Incidences of Cybercrime	Ethnics				
	Malay	Chinese	India	Others	Total
Protection of personnel data	-	1	-	-	1
Social media crime	3	-	-	-	3
Telecommunication fraud	89	166	13	7	275
E-banking fraud	13	10	1	2	26
Cyber love scams	45	62	4	9	120
Online purchase scams	31	32	4	4	71
Total	**181**	**271**	**22**	**22**	**496**

(Source: Contingent Police Headquarters, Penang, 2020)

The susceptibility of women to cybercrime is shaped by their patterns of usage and the extent of their freedom to establish connections with individuals on social media platforms (Madden and Zickuhr, 2011; Greenwood, Perrin, and Duggan, 2016). The utilisation of social media platforms, such as the act of sharing personal information, has been identified as a factor contributing to the erosion of privacy among women (Yar, 2012). This includes the public display of various personal details, such as phone numbers, complete names, familial information, residential addresses, educational institutions, as well as personal photographs and videos. The disclosure of personal information can potentially furnish cybercriminals with valuable data, thereby rendering users vulnerable to the perils of cybercrime. According to Greenwood et al (2016), there is a notable prevalence of young women in the utilisation of social media platforms, particularly Facebook. Comparatively, 53% of women and 47% of males utilised Facebook in 2017. 51 percent of women and 49 percent of males use Twitter. While Instagram users also demonstrate that more women (68%) than males (32%%) use the app. According to a survey by The Department of Statistics Portal (2019), more than half of all female Facebook users worldwide have experienced cybercrime, including online abuse. According to Winkelman et al (2015), cyber harassment includes online threats, cyberbullying, sexual harassment, and other forms of online abuse.

Women have been victims of cybercrime in several recorded incidents. For instance, Tandon & Pritchard's (2015) study indicated that 8 out of 10 women reported becoming victims of online crime because of using social media. According to reports, women make up most cybercrime victims—70% of them—and they also suffer the most—57% of them are between the ages of 18 and 25 (Dhaka, 2019). The amount of cybercrime recorded in Penang likewise rises yearly. Compared to 715 occurrences in 2018, a total of 895 incidences of internet crime were recorded in 2019. Meanwhile, from January through March 10, 2020, a total of 231 instances of cybercrime were recorded. Statistics for 2020 indicate that cybercrime is occurring more frequently since there have been 231 incidents reported in only the first two months. 2,239 different instances of cybercrime were recorded in 2022 (Contingent Police Headquarters, Penang, 2022). According to Boone (2011); Rohani and Tan (2012); Zulkufli and Azmi (2019), sexual harassment, defamation, threats, and hacking are among the cybercrime activities that often affect women. Even though communication technology is evolving quickly, society is still unaware of cybercrime. People join social networking sites as they become more popular without understanding the dangers and drawbacks of doing so. As a result, research is required to examine how women utilise social media and their propensity to become victims of online crime.

Literature Review

Digital media has a significant impact on how individuals communicate, make online purchases, and share information. According to Asyraf et al (2013), women primarily utilise social media for sharing, social interaction, online applications, and online transactions. The involvement of women online through the above activities makes them vulnerable to the risk of cybercrime and cybercriminals also easily target them as victims (Boone, 2011; Destiana et al., 2013; House of Lord, 2014; West, 2014). According to a study by the Pew Research Centre (2013), 60 percent of women like to upload photographs to social networking sites. This poses a threat to women, as they are more likely to become victims of hacking, slander, swearing, threats, and bullying (Smith et al., 2008). In addition, some women are extremely forthcoming with personal information, leaving them vulnerable to cybercrime and identity theft (Halder and Jaishankar, 2009). According to the Institute of Youth Research Malaysia (IYRES) (2017), young women are the most common victim of cyberbullying symptoms. Young women are susceptible to cyberbullying due to a lack of experience with the internet or a lack of knowledge of its risks (Bridging Refugee Youth and Children Service, 2009).

Moreover, young women are frequently targeted for sexual harassment (Pollack and MacIver, 2015). They are exploited by being persuaded to disrobe, pose sexually in front of a webcam, or be prompted to engage in sexual activity (Halder and Jaishankar, 2009). The actions were then recorded and shared on social sites such as pornographic websites, as well as with the woman's friends. Before being sexually exploited, the victim undergoes a process known as sexual grooming. Sexual grooming is a process by which sex offenders prepare young victims by bonding them and gaining their trust prior to exploiting them (Yar, 2006; Asmidar et al., 2018). When youth are curious, cybercriminals lead them to sexual conversations that lead to sexual relationships (Yar, 2006; Pollack and MacIver, 2015; Asmidar et al., 2018).

In addition to allowing communication with new friends, social media can also strengthen user relationships (Sheldon, 2009; Herring and Kapidzic, 2015). Social media users frequently engage in virtual messaging, including conversations with strangers (Neelamalar and Chitra, 2009). The user-friendly design of social media makes it simple for women to accept online friend requests by clicking the 'accept friend request' or 'add friend request' button, without having to know the actual identity of the individual. Existing social media networks can connect women to users from diverse demographics, including those of different genders, ethnicities, religions, and ages, within virtual communities. In fact, their contacts include both known acquaintances and new, unidentified peers. Meeting new people on social media is dangerous for young women, and many cases involving social media meetings have been reported to date (Rohani and Tan, 2012; Aziah, 2014; Pitchan et al., 2017). Dating especially with men, makes women vulnerable to fraud, sexual harassment, cyber harassment, slander, and hacking (Chow, 2015; Osman and Hafizan, 2018). Indirectly, the act of receiving contacts and participating in online conversation activities makes women susceptible to cybercrime (Halder and Jaishankar, 2009; Guan and Subrahmanyam, 2009). This study investigates how women's participation in social media contributed to their becoming victims of cybercrime.

Methodology

This study takes an inductive approach to data collection and interpretation by identifying the activities involved and their cybercrime susceptibility. Based on the literature review, pilot survey, and Facebook-related cybercrime observations, the researcher developed open-ended and closed-ended survey questions. The question consists of three parts: Part A: Respondent background, Part B: Social media activities among young women, and Part C:

Cybercrime types. The questions were designed to determine the use of social media among women and susceptibility to cybercrime.

Purposive sampling was used to select only those respondents who fulfilled the intended criteria (Colonius, 2006). In this study, only young women between the ages of 18 and 29 who have an active Facebook account and reside in Penang were selected. According to Greenwood et al(2016), Facebook is currently one of the most popular social networking platforms among users. The Statistics Portal (2019) reports that more than half of the world's female Facebook users are victims of cybercrime. Therefore, the respondents' selection of Facebook as their social networking platform is highly relevant to this study.

In addition, the study employed a method of random sampling because young women who use Facebook include those who have and have not been victims of cybercrime. Therefore, this method can help determine the number of young female Facebook users in Penang who have been victims of cybercrime. This study uses quantitative method, and a total of 137 respondents were chosen to complete the distributed survey. The researcher determined the number of chosen respondents using the sample size determination method. The sample size for this research is determined by the number of cybercrime victims in Penang in 2022. According to a report from the Contingent Police Headquarters, in 2022 there are 2,239 victims of cybercrime. Consequently, the determination of measure Calculation of the sample is based on the following formula:

Determination of Sample Size
n=N/ [1+N (e2)]
Where n = required sample size
N= total amount (sample frame)
e = confidence level (error limit)
Source: http://www.raosoft.com/samplesize

The actual sample size of cybercrime victims in Penang in 2022, with a 90% level of confidence, is only 66 individuals, based on the sample calculation formula provided above. According to the sample size determination technique, the target group consists of 66 individuals; however, the researcher has collected a total of 137 young women to represent the number of women who use Facebook. The researcher determined that the number of respondents exceeded the actual sample size because there were also young female victims who did not disclose the crime to the police. As a result, a larger number of respondents than the sample size was selected as a replacement for those who did not report the cybercrime. According to this figure, 75 respondents have been victims of cybercrime, while 62 have never been victims. In-depth interviews were also conducted with a total of 10 respondents who had been victims of cybercrime.

The quantitative data were descriptively analysed using Statistical Package for the Social Sciences (SPSS), whereas the qualitative data were analysed using content analysis. The study also prioritised research ethics, such as obtaining the respondent's consent before they filled out the survey form and maintaining the respondent's confidentiality, i.e., not displaying their personal information such as their name, age, and place of residence (Ghazali and Ghani, 2018).

Finding and Discussion

Respondent Profile

Table 2 shows the demographic profile of the respondents, involving 137 young women. The respondents consisted of four age categories and the most numerous were those between the ages of 21 and 23 years which was 36.5 percent. While the least respondents involved in the study were in the age category of 27 to 29 years which is 10.9 percent. The level of education shows that most of the respondents are from diploma graduates which is 33.6 percent. While 25.5 percent of respondents are Malaysian Student Certificate (SPM) graduates, and 30.6 percent are undergraduate and postgraduate graduates. The fewest respondents were from Malaysian Higher Education Certificate (STPM) graduates, which was 10.2 percent of respondents. As for socio-economic status, it shows that students who are still studying (school, college, university) are the most likely to answer the survey form, which is 48.9 percent of respondents. While 38.7 percent of respondents are already working, and 12.4 percent are those who are waiting for exam results/looking for work/housewives. The study respondents mostly consisted of those who were still single which was 84.7 percent, while only 15.3 percent were married.

Table 2
Demographic Profile of Respondents

Demographic Profile (N=137)	Total of Respondents	Percentage %
Age Group		
18 – 20 years	33	24.1
21 – 23years	50	36.5
24 – 26 years	39	28.5
27 – 29 years	15	10.9
Education Level		
SPM	35	25.5
STPM	14	10.2
Diploma	46	33.6
Bachelor	42	30.6
Social Economic Status		
Still studying	67	48.9
Working	53	38.7
Waiting for exam results/looking for a job/housewife	17	12.4
Married of status		
Single	116	84.7
Married	21	15.3

Activities engaged by respondents while using social media

The study identified four social media activities that put women at risk for cybercrime which are chatting, Facebook browsing, online shopping, and online dating. According to 77 respondents (56.2%), chatting is the primary activity respondents engage in when utilising social media. 44 respondents (57.1%) said they had been victims of cybercrime because of frequent online chats, whereas 33 respondents (42.8%) said they had never been victims (Table 3). In addition to chatting online with known individuals such as family and friends, they connect with strangers on Facebook (Table 4). Chatting online increases the probability

that young women will become victims of cybercrime, including sexual harassment. As reported by Respondents 1 and 2

> "...I knew an individual at my workplace who was so shy. We've exchanged messages a few times...at first, this guy's messages are commonplace - hello, how are you, have you eaten? However, after I've known him for a while, he likes to ask me sensitive questions. I initially believed he was joking because he doesn't speak much at work, but on social media he began using obscene language. He asked me what size bra and what colour bra and panties I am currently wearing. He also stated that he enjoys viewing my breasts when I'm walk. I was furious, timid, and promptly blocked his phone number. (Respondent 1, aged 29 years)

> "I received an offensive Facebook message from a friend. When they were first getting to know each other, he engaged in normal conversation and posed normal questions. We message so frequently that I feel very at ease with him and consider him to be an honest person. Eventually, however, he sent me a message inviting me to have sexual relations. He has also made several video calls to me. During a video conversation, he displayed his penis. I was stunned and terrified. After that, I block his number" (Respondent 23, 22 years old).

Online chatting exposes respondents not only to sexual harassment, but also to other cybercrimes, including fraud, defamation, threats, bullying, and cursing (Table 4). This finding is supported by Sawyer & Chen (2012), who state that social media users utilise the network for a variety of purposes, with relationship building and interaction being the primary ones. The existence of online groups enables them to communicate with family and friends (Ulrika, 2013). However, this virtual chatting also introduces them to various types of individuals and groups, including those who specifically target women.

Table 3
The types of activities respondents often to do when browsing social media and cyber crime

The types of activities respondents often to do when browsing Facebook	**Facebook (n=137)**					
	Victims		**Not become victims**			**Percentage (%)**
	Total	**Percentage (%)**	**Total**	**Percentage (%)**	**Total**	
Chatting	44	57.1	33	42.8	77	56.2
Facebook browsing	26	48.1	28	51.8	54	39.4
Online shopping	5	83.0	1	16.7	6	4.4
Total					137	100

Table 4
Types of social media use activities and types of cybercrimes that occur.

Types of activities using Facebook	Explanation about the activities	Types of cybercrimes
Chatting	• Chat with people they know (family, friends) • Chat with unknown friends (new friends)	Cheated, sexually harassed, slandered, threatened, bullied, insulted
Facebook browsing	• Search for information, play online games, upload photos, comment on your own or friends' photos and update personal information	Cheated, sexually harassed, slandered, threatened, bullied, hacked
Online Shopping	• Make purchases through online	Buying fake products, not receiving the goods purchased and the buyer giving inaccurate information about the goods sold.

Note: The data in the table is based on in-depth interviews with 10 respondents

Facebook browsing activities is the second most common activity, according to 54 respondents (39.4 percent). Table 3 demonstrates that out of 54 respondents, 26 respondents or 48.1% stated that they frequently use Facebook and confessed to having been a victim of cybercrime, while 28 respondents or 51.8% stated that they had never been a victim of cybercrime. Table 4 displays the respondents' Facebook browsing activities, such as searching for information, playing online games, and viewing the activities of peers through uploaded videos and images. In their free time, respondents also use Facebook to upload photos, leave comments, and update their location information. These activities cause them to become victims, such as those who have been deceived, sexually harassed, defamed, threatened, bullied, or hacked (Table 4). Activities such as uploading photos give opportunities for other users to engage in illegal behaviour, such as stealing photos of respondents, editing photos to create pornographic images, and using photos for defamation and bullying. According to Respondents 3 and 4, the following:

> "... I post a status update on my Facebook wall, and someone screenshot the status and it goes viral. On Facebook, I was criticised, insulted, and harassed by other users because of that status. This incident embarrasses and humiliates me..." (Respondent 3, age 24).

> "...my Facebook friend wants me to be his girlfriend, but I refused. He then slandered me out of anger. He stole my Facebook photo, edited it, and added a caption that said I'm a deceiver who likes to play with men's emotions, so don't trust me. Many of my Facebook friends believed the caption, and a few of them commented negatively on it. I am embarrassed in front of my friends, family, and relatives who saw the post he wrote" (Respondent 4, 24 years old).

The third activity frequently engaged in by respondents is online shopping. According to the study, only six respondents (4.4 percent) preferred this activity. Of the six respondents who like this activity, five (83.0 percent) reported being victims of cybercrime, while only one (16.7 percent) had never been victimised (Table 3). This category of respondents is frequently the victim of a cybercrime such as fraud when making a purchase. This finding is also supported by Van Wilsem (2011), who states that active online product purchasers experience a high risk of becoming fraud victims. The study found that respondents were victims of fraud, such as receiving counterfeit products, not receiving purchased goods, and purchasers providing false information about the sold goods (Table 4). This is what Respondents 5 and 6 stated:

> "Someone sent me a Facebook message advertising affordable pants. I am interested in purchasing these pants. Before I paid, she was courteous and asked what size, colour, and style I desired. After the payment was made, she remained silent. She did not respond when I asked her repeatedly when she planned to post" (Respondent 5, 21 years old)

> "I fell victim to fraud while purchasing a shirt on Facebook. Before I purchased the shirt, the seller treated me with kindness, but after deposited the money I asked her when she would ship it, she remained silent. I waited a week, asking days, but she did not respond. It appears that she has blocked me on Facebook" (Respondent 6, age 25).

The way that receiving new contacts online

In addition, activities that are often done by women who tend to be victims of cybercrime are through activities to get to know and receive new friends. The study found that there are five ways respondents receive new contacts (Table 5). First, it's easy to accept new friends. Second, respondents like to add friends only when first using a social media account. Third, respondents investigate first before accepting (approve) a new contact. Fourth, respondents accept new friends because they have a specific purpose. Fifth, respondents do not entertain friend requests from strangers. In addition, Table 6 includes data on how to receive new contacts and the types of cybercrime committed against young women.

Table 5
Ways of receiving new Friends on Facebook and cybercrime.

The ways of receiving new friends	Victims		Not become victims			Percentage (%)
	Total	Percentage (%)	Total	Percentage (%)	Total	
Easy to accept new friends	25	47.2	28	52.8	53	38.7
Likes to add friends at the beginning of using Facebook	9	75.0	3	25.0	12	8.7
Investigate new friend background before accepting them	18	62.0	11	38.0	29	21.2
Accepting new friends because of certain interests	8	50.0	8	50.0	16	11.7
Does not accept friend requests	15	55.5	12	44.4	27	19.7
					137	100

Table 6
Mode of receiving new contacts and types of cybercrime.

The ways of receiving new friends	Explanation of the type of cybercrime that occurred to the respondent
Easy to accept new friends	• Cheated by online sellers. • Cheated by a male acquaintance. • Victims of sexual harassment • Pictures are hacked then changed to sexy, pornographic images. • Being harassed by unknown men in a way that wants to get to know each other. • Victim of defamation • Bully victim
Likes to add friends at the beginning of using Facebook	• Cheated by online sellers. • Cheated by a male acquaintance. • Victims of sexual harassment • Bully victim • Victim of defamation
Investigate new friend background before accepting them	• There are users who use fake accounts and deceive respondents. • Being harassed by unknown men in a way that wants to get to know each other. • Victim of slander

Accepting new friends because of certain interests	• Cheated by new friends especially in the matter of purchasing goods on Facebook. • Bully victim
Does not accept friend requests	• Receive obscene messages from strangers/spam

* The data based on in-depth interviews with 10 respondents. There are respondents who are victims of more than one category of cybercrime such as victims of fraud and victims of sexual harassment.

The study found that most respondents easily accept new contacts when using Facebook, as stated by 53 respondents (38.7 percent) (Table 5). Respondents tend to be victims and not victims due to the easy acceptance of new contacts. 25 respondents (47.2%) who readily embrace new contacts have been victims of cybercrime, while 28 respondents (52.8%) say they have never been victims. Although more respondents in this category stated that they had never been a victim, the number of those who had been a victim was also high and almost the same number. Most respondents who easily accept new friends tend to be victims such as being cheated by online sellers, cheated by male acquaintances, victims of sexual harassment, victims of hacking, victims of harassment by unknown men, victims of slander and victims of bullying (Table 6). This study is supported by Rohani and Tan (2012) who stated that chat rooms on social sites are the main place for criminals to find and deceive women.

In addition, a total of 29 respondents (21.2%) stated that they investigate the background of new friends before accepting them, such as by viewing profiles, photos, and mutual friends of the person who invited them to become friends. Although this category of respondents investigates potential companions before accepting them, the majority remain victims. 18 (62%) of the 29 respondents in this category reported having been victims of cybercrime, while 11 (38%) said they had never been victims (Table 5). This is due to irresponsible Facebook users who create fake accounts to cheat them. The respondents also claim that they have been victims of harassment, such as males wishing to make acquaintances with respondents.

In addition, 27 respondents (19.7 percent) indicated they do not receive friend requests from other users. Despite not accepting friend requests, 15 respondents (55.5%) reported having been victims of cybercrime, whereas 12 respondents (44.4%) had never been victims (Table 5). These individuals are victims of cybercrime, including receiving obscene messages from strangers and spam (Table 6). In addition, 12 respondents (8.7 percent) said they only like to add friends when they first start using social media. This is done to increase the number of contacts upon account registration. Table 5 reveals that nine respondents (75%) who like to add peers when they first use social media have been victims of cybercrime, while only three respondents (25%) have never been victims.

Next, a total of 16 respondents (11.6 percent) accepted new friends based on shared or similar interests. Despite this, eight respondents (50%) in this category claimed they had been victims of cybercrime, while the same number of respondents (50%) stated they had never been victims (Table 5). This category of respondents became victims of cybercrime, such as being defrauded by new friends, particularly in the matter of purchasing a collection of items of interest on Facebook, and bullying (Table 6). Even if they only accept friend requests from individuals who can contribute something to them, such as ideas and information, some are still at risk of becoming victims of cybercrime.

Conclusion

This study found that women's online activities such as chatting, browsing Facebook, making purchases using Facebook, and accepting friends online tend to put them at risk for cybercrime. Among them, women are susceptible to becoming victims through actions such as sharing personal information and making new male friends. Some women have fallen victim to men's lies, sexual harassment, hacking, and extortion after meeting with an unknown man online. Women are especially susceptible to cybercrime, even though they take precautions to avoid becoming victims, such as ignoring friend requests and investigating the background of contacts before becoming friends. This demonstrates that cybercriminals are very smart and employ a variety of methods to attract women as their victims. This study contributes information about cybercrime that occurs because of Facebook use, carelessness, and the inherent vulnerability that makes women easy targets. Hence, it is recommended that future research endeavours undertake a thorough investigation encompassing both male and female youth participants in the domain of cybercrime. Such an inquiry would aim to discern prevailing patterns and facilitate the development of preventive measures by relevant stakeholders, thereby mitigating the perpetuation of this criminal activity.

References

Agenda Daily. (2021). *Jenayah Siber, Wanita lebih Terdedah Masuk Jerat*. Retrieved from https://www.agendadaily.com/isu-semasa/jenayah-siber-wanita-lebih-terdedah-masuk-jerat/.

Asiah, B., Aishah, S. N. S. N. M., & Akmal, M. (2015). Intipan siber: Jenayah baru dalam masyarakat kontemporari. *Jurnal Islam dan Masyarakat Kontemporari, 11(3),*12 – 25.

Asmidar, A. Z. R., Kamaluddin, M. R., Wahab, S., Anita, D. A. A., Zarina A. L., & Rathakrishnan, B. (2018). Kerentanan kanak-kanak Malaysia terhadap pengantungan seksual dalam talian. *Jurnal Psikologi Malaysia, 32(3),* 91 - 108.

Asyraf, A. T. M., Rosele, M. I., Meerangini, K. A., Marinsah, S. A., & Ramli, M. A. (2013). Jenayah siber: Pengelasan di antara Al-Jaraim dan Al Jina'i menurut sistem perundangan Islam. *International Seminar on Islamic Jurisprudence in Contemporary Society*, 539 –551.

Aziah, M. A. N. (2014). Kesan media sosial kepada rumahtangga. *Buletin Persatuan Wanita UKM (Suaranita), No. 69*. 54-60

Boone, J. (2011). Illegal use of social media. National White-Collar Crime. Retrieved from www.iacpsocialmedia.org/Portals/1/documents/NW3C Article.pdf.

Bridging Refugee Youth & Children Service. (2009). Refugee children in U.S schools: A toolkit for teacher and school personnel. United States Conference of Catholic Bishops. Washington, DC.

Colonius, A. (2006). *Ibu tunggal Melayu di negeri Pulau Pinang: Satu kajian status sosial-ekonomi dan sokongan sosial*. Master Thesis. School of Humanities, Universiti Sains Malaysia, Pulau Pinang.

Dhaka, T. (2019). Rise in cybercrime worries women. Retrieved from https://www.dhakatribune.com/cybersecurity/2019/04/01/rise-in-cybercrime-worries women.

Malaysian Department of Statistic. (2020). Laporan Survei Penggunaan dan Capaian ICT oleh Individu dan Isi Rumah 2019. Retrieved from https://www.dosm.gov.my.

Destiana, I., Salman, A., & Rahim, M. H. A. (2013). Penerimaan media sosial: Kajian dalam kalangan pelajar universiti di Palembang. *Jurnal Komunikasi Malaysian Journal of Communication, 29(2)*, 125 - 140.

Ghazali, S., & Ghani, M. N. (2018). Perception of Female Students towards Social Media-Related Crimes. *Pertanika Journal Social Science & 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. *Pew Research Center*. Retrieved from 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.

Halder, D., & Jaishankar, K. (2009). Cyber socializing and victimization of women. *Temida, 12(3),* 5 – 26.

Herring, S. C., & Kapidzic, S. (2015). Teens, gender, and self-presentation in social media. In Wright, J. D (ed.). *International Encyclopedia of Social and Behavioural Sciences, 2nd edition* (146 –152). Oxford: Elsevier.

House of Lord. (2014). Social media and criminal offences. The Select Committee on Communications. 1st Report of Session 2014 – 15.

Madden, M., & Zickuhr, K. (2011). 65% of online adults use social networking sites. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2011/08/26/65-of-online-adults-use social networking-sites/.

Maznah, I. (2014). Wanita dan penggunaan media sosial. *Buletin Persatuan Wanita UKM* (Suaranita), Bil. 69.

Mustafa, S. E. (2016). Penggunaan laman sosial dan impaknya terhadap hubungan persahabatan dalam talian. *Jurnal Komunikasi Malaysian Journal of Communication, 32(2),* 65 – 81.

National Crime Prevention Council. (2012). Cybercrimes. Retrieved from http://www.ncpc.org/resources/files/pdf/internet-safety/13020-Cybercrimes-revSPR.pdf.

Neelamalar, M., & Chitra, P. (2009). New media and society: A study on the impact of social networking sites on Indian youth. Retrieved from http://www.ec.ubi. pt/ec/06/pdf/neelamalar-new-media.pdf

Ghani, M. N., & Ghazali, S. (2015). Tindak Balas Pengguna YouTube Terhadap Kes Buli dalam Kalangan Remaja di Malaysia. *Sains Humanika. 6(1),* 9–17.

Osman L., & Hafizan, M. S. F. (2018). Sanggup merana dek mewah seketika. Berita Harian. Retrieved from https: //www.bharian.com.my/wanita/lainlain/2018/07/451524/ sanggup-merana-dek-mewah-seketika.

Pitchan, M. A., Omar, S. Z., Bolong, J., & Ahmad, A. H. (2017). Analisis keselamatan siber dari perspektif persekitaran sosial: Kajian terhadap pengguna Internet di Lembah Klang. *Journal of Social Sciences and Humanities, 12(2),* 16 – 29

Pollack, D., & MacIver, A. (2015). Understanding Sexual Grooming in Child Abuse Cases. *ABA Child Law Practice, Vol. 34(11). 236-244*

Rohani M., & Tan, S. M. (2012). Tipu alaf baru. BULETIN ICT, Edisi 2/2012. Retrieved from http://www.treasury.gov.my/pdf/buletinICT/Edisi 22012.pdf.

Salmah, O. (2015). Pengaruh Peranti Teknologi Kepada Perkembangan Sosial Dan Permasalahan Kesihatan Kanak-Kanak. Retrieved from file:///C:/Users/DrNorhayati/Downloads/Pengaruhteknologikepadakanak2-11april.pdf.

Sheldon, P. (2009). Maintain or develop new relationships? *Rocky Mountain Communication Review, 6,* 51–56.

Smith, A., & Anderson, M. (2018). Media social use in 2018. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/.

Steinkuehler, C., & Williams, D. (2006). Where everybody knows your (screen) name: online games as"third places." *Journal of Computer-Mediated Communication, 11*, 885 – 909.

Tandon, N., & Pritchard, S. (2015). *Cyber violence against women and girls: A world-wide wake-up call*. Retrieved from https://en.unesco.org/sites/default/files /genderreport2015 final.pdf.

West, J. (2014). Cyber-Violence against women. Batteres Women's Support Services. Retrieved from http://www.bwss.org/wp-content/uploads/2014/05/ CyberVAWReportJessicaWest.pdf%0Ahttp://site.ebrary.com/lib/uwo/docDetail.action ?docID=0886270.

Winkelman, S. B., Early, J. O., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring cyber harassment among women who use social media. *Universal Journal of Public Health, 3(5),* 194 – 201.

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

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

Zulkufli, I., & Azmi, A. (2019). Jenayah cinta siber di malaysia: suatu penelitian terhadap pengalaman, mangsa. *Journal of Social Science and Humanities 16(4),* 1-10.