Journal of Contemporary Islamic Studies
Vol. 8, Issue 2 (2022) 41-54
https://doi.org/10.24191/jcis.v8i2.3

Cybercrime Through Love Scams: What Women Should Know?

Farah Safura Muhammud[1*], Hamizah Muhammad[1]

[1]Academy of Contemporary Islamic Studies, Universiti Teknologi MARA Terengganu, 23000 Dungun Campus, Malaysia

[*]Corresponding Authors
farahsafura@uitm.edu.my

Received: 26 July 2022
Accepted: 5 October 2022
Online First: 1 November 2022

ABSTRACT

Due to various technological advancements in the modern era, cybercrime has become a global issue. Since the outbreak of the COVID-19 pandemic, most jobs and transactions have been done virtually, compromising our global cyber security. Many people are unaware of this alarming situation leading them to become victims of cybercrime, especially the vulnerable groups of the elderly, children, and women. This conceptual study discusses the scammers' modus operandi for monetary deception or militants' recruitment through love scams. The discussion then continues with the factors that lead women to become potential victims, from the personality aspects, characteristics, and impacts after being victimised. This study concludes that precautious steps are necessary to avoid becoming a potential victim of cybercrime, and coping with the aftermath is equally important.

Keywords: *COVID-19, cybercrime, cyber security, love scams, women issues*

PENERBIT PRESS
UNIVERSITI TEKNOLOGI MARA

INTRODUCTION

Amidst the COVID-19 pandemic, computer and internet use is on the rise. The internet has become part and parcel of daily life. The advent of teaching and learning approaches at home, e-commerce, online banking, and e-filing expose humans to the borderless virtual world, leading to direct access to its deception and abuse. Cybercriminals are targeting children and women as the easiest victim. If looking at the rise of money laundering crimes at stake, targeting women will double the profit. Women who are active online users on various platforms, including online dating, social media, and online shopping, are vulnerable to cybercrimes. The word cyber from cybercrime means the virtual world, the internet. At the same time, the word crime means evil. According to Hashim (2019), cybercrime is all kinds of crimes in the virtual world by abusing the benefits of developing increasingly sophisticated information technology. This crime is committed by irresponsible individuals or groups seeking profit in a wrong way and is prohibited by Islam. Cybercrime describes various types of illegal activities that occur in cyberspace, such as hacking systems and sabotaging communications (Hamsi et al., 2015).

PROBLEM STATEMENT

Based on 2018 statistics, the Commercial Crime Investigation Department (JSJK), Royal Malaysian Police (PDRM), revealed that the total losses due to criminal fraud increased by 55.5 percent nationwide compared to 2017. The increase involved a loss of more than RM224.6 million with 4,965 cases recorded compared to the previous year, which was RM99.9 million with 4,178 cases due to the Macau Scam.

According to Malaysia Communications and Multimedia Deputy Minister Datuk Zahidi Zainul Abidin, 5,697 incidents of cybercrime were reported to Cybersecurity Malaysia from January to August this year, a 22 percent increase from the same period last year. Cases have increased significantly since the Movement of Control Order (MCO) implementation, with 3,906 complaints lodged to the Cyber999 Help Centre from March 18 to June 30, representing an increase of more than 90% over the same period last year.

Felmlee et al. (2016) agree that females are more frequently victimised than males. Whitty (2018) found that 60% of women have more historical evidence of romance scams than men, most of whom are middle-aged and well-educated. Unlike Hamsi et al. (2015), the victims' weaknesses and the ICT application advancement are the causes that expose the victims to cybercrimes.

Meanwhile, Saad et al. (2018) found that people who are vulnerable to cybercrimes in Malaysia are between the age of 25 to 45 years, educated, lack computer skills and awareness of cyber-fraud, married people and employed with salaries of more than RM2001 per month. This evidence shows that educated and married career women are highly targeted to be victimised. These women are deceived for money as they have access to a certain amount of salary or spouses' income. Money is the main agenda that is easily transferred and manipulated. Former Deputy Home Minister I, Datuk Seri Ismail Mohamed Said, announced 481 cases of love scams resulting in fraudulent claims of RM18.1 million. This amount has alarmed the government and society that there is a need to combat these cybercrimes.

Another issue related to cybercrime that exclusively affects Muslim communities is the catfishing strategy to attract people to join the Daesh militants. It is a recruitment tactic through social media targeting women by promising a peaceful Islamic community, romance, and a marriage to a jihadi, a so-called warrior entitled to Jannah. Becoming a wife or bearing the child of a warrior is considered righteous and is rewarded with Jannah. According to Mohsina (2017), there is a growing trend of female jihadism in Bangladesh. Even women's roles in jihadism have changed from peripheral roles to more assertive roles, including suicide bombers, combatants, recruiters, preachers, and propagandists. Women who feel isolated and removed from their non-Muslim community are fond of the promises of welcoming the Muslim community offering companionship, like-minded friends, and being appreciated by someone (Blaker, 2015). Therefore, this study aims to explain the rise of cybercrime cases, which affected women the most, and have incurred losses in the forms of financial and loss of relationships (Whitty, 2015 & 2018). This study also focuses on love or romance scams, the factors of women victimised by the swindlers they love, and the love scam's psychological impacts.

LITERATURE REVIEW

Islamic Perspective on Cybercrime

Cybercrime is listed as a serious crime in this country. Digital or cybercrime has a greater effect on the target of bullying than physical bullying. Since cybercrime is more common in the virtual environment than in the real world, victims of cybercrime are more likely to suffer from severe depression. As a result, to solve the issue, the government must take a major and decisive step in addressing the symptoms of cybercrime to prevent future tragedies (Hashim, 2019). Islamic law on cybercrime has been stated in specific and authentic sources. Sources such as the Quran, Hadith, *Ijmak* and *Qiyas*, the primary sources in Islam, have stated the law for this crime. The issue of cybercrime has been touched on in the Qur'an regarding human behaviour. This is because when people forget the law of God, then they will exceed the limits and follow their desires. Allah SWT said, which means:

> "And verily, We have sent down to you verses of evidence explaining the laws of command and prohibition, and examples of the stories and news of those before us, and advice and instruction for those who (want) be pious" (Al-Nur, 24: 34)

Islam has developed the fundamental principles for organising human life so that every human being receives the rights that he or she deserves, with no space for oppression and exploitation by any party acting unilaterally. The evolution of time and reality today leads to the existence of cybercrime in various forms. This necessitates the investigation of the crime from the current legal perspective in Islam. If a person knowingly accesses a device, computer network, or computer system without the owner's effective permission. In that case, the person commits an offence for trespassing on someone's property, i.e. computer hardware or software. If a criminal were to gain access, it would be unauthorised. Is not allowed to monitor the type of access to the software or data in question. Unable to obtain permission from an individual entitled to access the software or data is also wrong in Islam. In the verse of the Qur'an:

> "O believers! Do not enter houses other than your own until you have sought permission and greeted their inmates" (Al-Nur: 27)

> "O believers! Avoid immoderate suspicion, for in some cases suspicion is a sin, Do not spy on one another" (Al-Hujurat: 12)

Allah decides in these verses that if one enters the house of another, he should seek the owner's permission beforehand. According to Islamic rules, a person cannot enter another person's property without permission. This is the Islamic approach to rights to privacy. Hence, despite curiosity and suspicion, he is not allowed to spy on the secrets of another, even those concealed or kept inside computers. In the hadith, Prophet Muhammad (PBUH) said:

> "It is better for a Muslim to mind his own business" (Al-Muatta: 1604)

> "Permission is for having a look" (Al-Bukhari: 5887)

The Prophet tells us that good Muslims will leave other people's affairs alone. Islam prohibits searching and digging into other businesses, including spying on information in their computers. Permission is primarily needed beforehand. Therefore, one is not permitted to enter another person's property without permission.

Scammers' Modus Operandi

One of the recorded love scam cases occurred in Penang; a retired teacher lost RM512,316.18 of her life savings to a Macau scam syndicate earlier in 2020. While in Kelantan, a retired woman was deceived and lost RM500,000 to a man she had befriended on Facebook. The man claimed to work in the oil and gas industry in the United Kingdom. The man told the victim that he wanted to give her RM650,000 after one month of online friendship. According to Hamsi et al. (2015), these love scam cases explain that scammers set up fake identities at online dating and social networking sites, then make contact and develop an intimate online relationship with the victims. After some time, they create a situation in the urgent need of money, and the victims make several transactions. Until the victims feel

doubtful, the scammers disappear with their promise. It was reported in December last year that a 73-year-old woman lost RM61,000 to a man she met online after falling into a love scam (Bernama, 2020).

According to Alavi et al. (2020), the perpetrators use different strategies to lure the victims into the trap, including making a fake profile, offering sweet promises, sending gifts, and impersonating a tax agency representative. They also consider the use of sorcery. Other than social media platforms, women are trapped by the love scam while using online dating platforms. The study by Shaari et al. (2019) found that the scammers use three stages of strategies as follows:

Stage 1: INITIAL STAGE - Setting up Contact and Establishing Strategies

This stage involves scanning the profiles to see the potential of becoming a partner based on cultural background, profession, education, image, and friends/ associates. Criminal profile analysis found that scammers upload fake profile pictures of a rich and luxurious life with exaggerated information. It would be even more suspicious if the person mentioned that he is an Asian, has a small number of Asian friends, or maybe a European with a small number of European Facebook friends. Some scammers include interesting stories together with an introduction to the background.

Stage 2: PRE-ATTRACTION STAGE–Gaining Trust, Developing Personal Relationships, and Grooming Process

At this stage, scammers pretend to be good friend, romantic or religious, who is eager to know more about the victim. To strengthen the relationship and build trust, the scammer will use religious expressions (e.g. “Assalamualaikum.” or “Allah SWT bless you.”), words that indicate trustworthiness (e.g. “Trust me.” or “I believe in you”), express attraction (e.g. “I miss you every day.” or “You are my type.”), and prioritise the victim (e.g. “This is only for you.” or “...wherever you go.” or “now or never.”)

Stage 3: HOOKED –Maintaining the Scam, the Bait, and the Execution

This stage is the phase when monetary requests are made using several techniques. The scammer’s writings also are more aggressive, forceful, and

rude. Alavi et al. (2020) found the following scenarios as frequently used by scammers:

1. the promise to send gifts yet having insufficient money for the immigration tax

2. stranded at the airport/customs/immigration office

3. have financial problems and need immediate cash

4. had an accident and needed to pay compensation

5. one of the family members was diagnosed with a severe illness

Unlike scammers who aim for money, the militants have a different agenda; the person himself/herself. Recruiting women is more accessible with women recruiters as it establishes comfort in conversation (Blaker, 2015). Other ways to attract educated middle-class women to join the extremists include spreading propaganda online through images and videos and creating a solid emotional feeling toward other Muslim victims (Mohsina, 2017). According to Jawhar (2016), the Daesh group recruits people through the following social media platforms:

i. JustPaste.It - calls for jihad by sharing images and texts through a link that a password is used to protect to enhance the links' security.

ii. Twitter - A so-called cleric/religious teacher uses his account to post the ongoing conflicts in Syria and Iraq and the calls for hijrah to an Islamic State.

iii. Instagram - posting pro-Daesh images and videos, including the ongoing battle in Syria and Iraq, projecting Daesh's success and the comfortable life an Islamic State can offer.

iv. Tumblr consists of blogs of fighters sharing their experiences in Syria and Iraq.

v. VK (Vkontakte) - a social networking site that is almost similar to Facebook, a platform in which the Daesh group provides a guide to making hijrah or migration to the Islamic State, including the necessary equipment and baggage to bring along during the migration.

vi. Facebook - a platform to spread Daesh's propaganda and facilitate recruitment.

Factors of Women's Victimisation

Even though Van de Weijer and Leukfeldt (2017) argue that personality traits are not related to the cause of being victimised, they found that those who scored higher for emotional stability were less likely to become the targets. Whitty (2015) found that romance scammers target middle-aged and well-educated women because they are more impulsive, trustworthy, and have an addictive disposition. Like the militants' agenda, young and educated women from middle-class backgrounds are influenced by Islamic State propaganda, attracting women to be equally treated as contributors to establish a utopian society governed by the Shari'ah law (Mohsina, 2017).

Individuals with higher scores on "openness to experience" also have higher chances of becoming victims of cybercrimes (Van de Weijer et al., 2017). The readiness to accept challenges or open oneself to new relationships also costs other aspects of life. Women face censorship, sexual harassment, or cybercrime challenges while making intimacy online through reciprocal visual and textual self-disclosure (Golzard, 2015). Based on the study of Whitty and Buchanan (2018), participants also admitted that they had performed sexual acts in front of the webcam. Participants from the study of Aurora and Scheiber (2017) blame women themselves for the real reason of exposing themselves to cybercrimes, for example, sending nude

photos to their boyfriends. Cyber aggression victims were also coerced, blackmailed, and threatened by their partners (Felmlee et al., 2016).

Even though Saad (2018) believes that scammers target married women as the victims, according to Hamsi et al. (2015), scammers prefer unmarried women looking for partners. It is due to the growing number of dating-match websites, online social networks, and chat rooms. The dating market can be a competitive site where people compete to become or search for highly valued potential partners (Felmlee et al., R,2016); therefore, the act of exposing personal information to attract potential partners is manipulated by scammers. These women also have become a target for the militants. With the purpose of looking for a life partner, the vulnerable victims are easily attracted to the prospect of an adventure or a potential religious husband (De Leede, 2018)

Impacts After Being Victimised

Besides being financially affected, the victim also suffers psychological impacts after realising that a love scam has deceived her. Whitty and Buchanan (2015) found that women who had demonstrated sexual acts in front of the webcam felt gang-raped in cyberspace, which finally produced similar psychological impacts to the actual rape, including shame, guilt, and sexually violated. Victims are emotionally pressured when the scammer use photos and personal information to blackmail them to extort more money (Saad et al., 2018). Aurora and Scheiber (2017) highlight the suicide of 17-year-old Julia Rebecca after posting her sex videos online.

Even worse, a person who has already migrated to the so-called Islamic State cannot even change her fate and be locked up abroad. There were also women caught as soon as they reached the airport. Imprisoned is another consequence that a woman would face for an attempt to marry a jihadi and travel to the Islamic State. Four women were captured and believed to travel to Syria (Lewis, S, 2016). Unfortunately, these women did not realise the situations awaiting them. An interview with the refugees in al-Hawl Camp, Syria, reveals the hope to return home of a 20-year-old college student smuggled into the Islamic State (Callimachi et al., 2019). After being married to three warriors, she regrets her decision and decides to return. Then she surrendered to the coalition forces fighting ISIS and became a detainee in a refugee camp in north-eastern Syria.

Discussion on What Women Should Do?

While surfing the internet, especially when using social media, Hamsi et al. (2015) proposes that:

1. Women must avoid revealing too detailed personally identifiable information, for example, home addresses, work specifics, and family information, through profiles and photo identification at a very early stage.

2. Ask about the person's background and investigate his information on websites to check for conflicting information.

3. Be wary of any financial assistance.

4. Create a unique password that is not incorporated with publicly known information

5. file a complaint soon as they feel they have been victimised

The following monitoring and analytic tools in the table help women examine the effectiveness of the counter-messages and analyses of social media platforms.

Table 1: Monitoring and Analytic Tools (Jawhar, J 2016)

No.	Tools	Purpose	Nature	Cost
1.	Google Alerts	Notify users of new Internet content based on the user's keywords through email.	Monitoring	None
2.	Google Analytics	Measure how the audience is interacting with users' website content and track downloads and video plays, among others, on the page	Analytic	None
3.	Google Trend	Analyse Google search terms based on interest which could provide data based on region and country	Analytic	None

4.	Boardreader	Monitoring keywords and contents on forums.	Monitoring	None
5.	Omgili	Monitoring keywords and contents on a forum, message boards and discussion threads	Monitoring	None
6.	Social Mention	Monitors and analyses data and influences social media platforms based on four elements: strength, sentiment, passion, and reach.	Monitoring/ Analytic	None
7.	Twazzup	Track the name or term on Twitter.	Monitoring	None
8.	HootSuite	Allows people to schedule messages for future publishing.	Analytic	None
9.	Klout	Measures the influence and impact of users' links, recommendations, and interactions across different social media platforms.	Analytic	None
10.	Monitter	Allows users to key in up to three keywords and monitor what is being said on Twitter in real-time.	Monitoring	None

Finally, besides the suggestions mentioned above, victims can lodge reports to the police and other relevant agencies. Ensure all documents needed are kept safe. The Commercial Crime Investigation Department (CCID) only received a portion of reports as victims felt ashamed to admit being scammed, or some victims are still not realised that they were victimised. The dating apps also provide precautionary measures to protect the users by providing a self-reporting tool to report individuals requested for money. Spend some time reading the terms provided by the apps (Saad et al., 2018).

CONCLUSION

Due to the Movement Control Order (MCO), people spend too much time at home and get easy access to the internet. The time paid online is over-

limited, which exposes people to cybercrime. Women looking for partners are easily deceived, mainly when the scammer fulfils the persona of their dream. Exposing themselves by sharing personal information, identifiable pictures and videos make women more vulnerable to criminals. There are 14 steps the scammer uses to attract women. Therefore, other than equipping themselves with IT knowledge, women should also learn the scammers' strategies. In circumstances that hold the query of being victimised, women should be aware of the signs and immediately lodge a report.

ACKNOWLEDGEMENTS

We thank the anonymous for their useful suggestions.

CONFLICT OF INTEREST

The authors declare no competing interests, such as financial or personal relationships, regarding the writing of this article.

AUTHORS' CONTRIBUTION

Author 1 designed the study, gathered the literature, and wrote it. The co-author analysed the documents and reviewed the article.

REFERENCES

Alavi, K., Mahbob, M.H., & Sooed, M.S.A 2020. Strategi Komunikasi Penjenayah Cinta Siber terhadap Wanita Profesional. Malaysian Journal of Communication, 36(3)

Aurora, P. & Scheiber, L. 2017. Slumdog Romance: Facebook Love and Digital Privacy at the Margins. 39(3)

Bernama. (2020). Pahang Woman, 73, Loses RM61,500 in Love Scam. New Straits Time. Retrieved from nst.com.my/news/crime-courts/2020/12/650682/Pahang-woman-73-loses-rm61500-love-scam.

Blaker, L. (2015). The Islamic State's Use of Online Social Media. The Journal of the Military Cyber Professionals Association, 1(1), 1-9

Callimachi, R. & Porter, C. 2019. 2 American Wives of ISIS Militants Want to Return home. The New York Times. Retrieved from nytimes. com/2019/02/19/us/Islamic-state-american-women. Html.

De Leede, S.Western. 2018. Women Supporting IS/ Daesh in Syria and Iraq- an Exploration of Their Motivations. International Analysis of Criminology, 56(12)

Felmlee, D. & Faris, R. 2016. Toxic Ties: Networks of Friendship, Dating and Cyber Victimization. Social Psychology Quarterly, 79(3)

Golzard, V. & Miguel, C. 2016. Challenges and Opportunities for Muslim Women in Iran. Middle East Journal of Culture and Communication, 9(2), 216-233

Hamsi, A.S., Bahry, F.D.S., & Tobi, S.N.M. 2015. Cybercrime Over Internet Love Scams in Malaysia: A Discussion on the Theoretical Perspectives, Connecting Factors and Keys to the Problem. Journal of Management Research. 7(1), 27-39

Hashim, H. 30 July 2019. Undang-undang antibuli siber. Didapatkan dari Sinar Harian: https://www.sinarharian.com.my/article/40553/ KOLUMNIS/Undang-undang-antibuli- siber

Jawhar, J. (2016). Terrorists' Use of the Internet: The Case of Daesh. Malaysia: The Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs.

Lewis, S. 2016. 15 Suspected ISIS Members Planning Terror Attacks Have Been Arrested in Malaysia. TIME. Retrieved from time.com/4271704/ Malaysia-arrested-15-isis-members-terror/.

Mohsina, M. (2017). Growing Trends of Female 'Jihadism' in Bangladesh. Counter Terrorist Trends and Analyses, 9(8), 7–11.

Nasir, A.A. 2019. Women in Terrorism. Counter Terrorist Trends and Analyses. 11(2).

Saad, M.E., Abdullah, S.N.S.H. 2018. Cyber Romance Scam Victimization Analysis Using Routine Activity Theory Versus Apriori Algorithm. International Journal of Advanced Computer Science and Application. 9(12), 479-485.

Shaari, A.H., Kamaluddin, M.R., Paizi, W.F., & Mohd, M. 2019. Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims. Gema Online Journal, 19(1), 97-115.

Tsai, F. S., Etoh, M., Xie, X., Lee, W. C., & Yang, Q. 2010. Introduction to mobile information retrieval. *IEEE Intelligent Systems* (1), 11-15.

Van de Weijer, S.G.A. & Leukfeldt. 2017. Big Five Personality Traits of Cybercrime Victims. Cyberpsychology, Behaviour, and Social Networking, 20(7).

Whitty, M.T. & Buchanan, T. (2015). The Online Dating Romance Scam: The Psychological Impact on Victims-Both Financial and Non-financial. Criminology & Criminal Justice, 16(2)

Whitty, M.T. 2018. Do You Love Me? Psychological Characteristics of Romance Scam Victims. Cyberpsychology, Behaviour, and Social Networking, 21(2).