WOMEN'S INVOLVEMENT IN CYBERCRIME: A PREMILINARY STUDY TYPE (METHOD/APPROACH)

Article · January 2015

CITATIONS
0

READS
329

5 authors, including:

Muhammad Ikhlas Rosele
University of Malaya
28 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Mohd Anuar Ramli
University of Malaya
118 PUBLICATIONS **41** CITATIONS
SEE PROFILE

ISSN 2349-4379

WOMEN'S INVOLVEMENT IN CYBERCRIME: A PREMILINARY STUDY

Muhamad Asyraf Ahmad Termimi, Muhammad Ikhlas Rosele, Khairul Azhar Meerangani, Syamsul Azizul Marinsah & Mohd Anuar Ramli

Postgraduate student, Department of Fiqh and Usul, Academy of Islamic Studies, University of Malaya

newasyraf@yahoo.com

Postgraduate student, Department of Fiqh and Usul, Academy of Islamic Studies, University of Malaya

Ikhlas.rosele@yahoo.com

Postgraduate student, Department of Fiqh and Usul, Academy of Islamic Studies, University of Malaya

rahza_8811@yahoo.com

Postgraduate student, Department of Fiqh and Usul, Academy of Islamic Studies, University of Malaya

kehak@yahoo.com

Senior Lecturer (Ph.D), Department of Fiqh and Usul, Academy of Islamic Studies, University of Malaya

mohdanuar@um.edu.my

ABSTRACT

Cyber crimes is a new millennium threat to society nowadays which brings by developments of technology and information. Various forms of cyber crimes exist either theft and fraud involving money and property or safety threat involving contamination of dignity. Therefore, this study will identify cyber crimes related to women in Malaysia for cases of theft and fraud of money and property through cyberspace. Cyber crimes will be identified and classified according to cases that often occurred in Malaysia and legal protection provided to the victim. The results showed lack of awareness about cyber security transactions and the provision of existing law that exists for cyber crime cause women to be victims of cyber crime.

Indexing terms/Keywords

Cyber crime, women, law, Malaysia.

Academic Discipline And Sub-Disciplines

Women Studies; Religion & Society

SUBJECT CLASSIFICATION

Crimes Subject Classification; Womens Subject Classification

TYPE (METHOD/APPROACH)

Literary Analysis

ISSN 2349-4379

INTRODUCTION

Today's rapidity of science and technology is an undeniable fact. It has offered various advantages and benefit to everyone who make use of it. Likewise is the case for the utilization of the cyber world that is born from the advancement of science and technology. It has been given attention by the society today because of the many advantages that will be acquired, among them is to facilitate affairs and time saving. However, despite the advantages offered, it is still exposed to various risks and harmfulness for its consumers.

Cyber consumers are also easily exposed to become victim to cybercrime carried out by irresponsible people (Ahmad Shawal, 2012). Cybercrime is a form of criminal behavior which uses any type electronic device through internet connection service which enables a criminal behavior being carried out, whether it involves an individual or a group of people and is able to transcend limitation from one country to another, in periods that are short and without reserved limitation (Anita & Nazura, 2004).

Cybercrime causes loss or damage to the equipment, data and information that involves a computer's software or processing; whether from a virus attack, invasion (unauthorized access and use) and information theft on a computer or electronic device that becomes the target (Rusli, et.al, 2003). Cybercrime that exists today is no longer confined only to the use of computer as a tool in committing crime, but instead, cybercrime today is also defined as crime which occurred in the internet or cyber world, which involves fraud and contriving trick (Anita & Azura, 2004).

Group categorised as cyber criminal on the other hand is those having inverse thinking about the diversity of ICT usage (technodystopianism), which regards the cyber world as a platform to create wealth and pleasure. They use the cyber world to commit crime like hacking, transmit viruses, mailbomb, pornographic image, poison-pen letter and so on (Jalaluddin, 2008).

Their targeted victims on the other hand, are generally irrespective of level of society, sex and age. But the victims are definitely those who had used the services in the cyber world for various purposes, like socializing, trading, doing a transaction and various other work affairs. In the year 2011 alone, as much as 6586 cases occurred which caused losses amounting to RM 80.5 million (see schedule 1).

Schedule 1: Cybercrime Statistic 2007-2011

Year	No. of Cases	Losses (RM)
2007	1139	RM 11.4 Million
2008	1821	RM 12.9 Million
2009	3863	RM 22.3 Million
2010	6167	RM 63.0 Million
2011	6586	RM 80.5 Million

Sources: (DSP Mahfuz; Syahidi, 2012)

Women are among those that are easy to become victims of cybercrime, because besides negligence, cyber criminals are also targeting women as victim of their act. Therefore, this study tries to identify several factors and reason of women's involvement in cyber world and why they are trapped especially as victims of cybercrime. This study also recommends a few safety measures for women, from being victims of crime.

WOMEN AND CYBER WORLD

In line with today's modernization, activities happening between communities are not just limited to those in the real world; in fact, they have passed over another new boundary where they can perform various activities in the virtual world. Women are among those that are not exempted in contributing to this virtual involvement, in fact, they are among the cluster's that have recorded high virtual site usage. There are a few activities that they carried out, which can be summarized as follows:

1- Sharing

They like to share certain matters, whether involving information, knowledge or talent, and their own ideas. This sharing, whether in the form of writings that are much disseminated through blogs or in visual form (Thomham, S., 2007) like the making of video, audio and broadcasted picture which showcases singing, speaking and acting talents that can be disseminated through Youtube, Instagram or 4shared sites. Such sharing is favoured because it can highly transcend targets without having to show oneself in a huge audience or various locations. They could also promote themselves and being recognized faster without having to highly utilize resources such as energy, time or finance.

2- Social Interaction

Apart from that, they also use cyberspace as a platform to connect with friends, acquaintances or as a means to seek acquaintance (Paasonen, S., 2005). They can share activities, discussing on information and further expanding their existing social network. Facebook and Twitter are among the applications that obtains highest reception because of the recorded huge number of access and consumers. Hence, this facilitates further interactions that occurred, because some of them are more comfortable with this method where they do not have to go through any inconveniences which might arise if the interaction is done outside the virtual world. Besides that too , they also felt that their privacy is more assured, where they can use a different identity (Paasonen, S., 2005) if they are not yet prepared to show their real identities.

3- Online Applications

There is a few online applications like the cyber games and certain contest that also motivates women to be involved in the cyber world. Innovation occurring in this area had given many attractive options to women until some of them reached an extent of addiction with a few particular applications, and have neglected their responsibility and other assignments. This matter usually involved game application, moreover, if the online game enabled them to play together with their other virtual friends (Framme, J. & Unger, A., 2012). Likewise, with certain applications considered as fulfilling their desire, such as tourism application, cooking recipes and fashion that could be downloaded easier, and especially for android software users through google playstore application just by using their smartphone.

4- Online Transactions

They are also making the virtual sites as an arena to further expand their businesses. Easy business transactions (Huddleston, P., 2011) have motivated them to involve themselves in this area more actively because their consumer does not have to go out to get their essential goods and thus able to save time for the more important matter. For traders on the other hand, apart from being able to promote advertisement and operate their businesses in a wider framework, they can also continue their task at home without having to neglect the household demand, where any choice and transaction can just be done online. This is because this area is usually monopolized more by married woman and for them to become a full-time housewife.

CAUSES OF CYBERCRIME

Various forms of cybercrime occurring among cyberspace users nowadays and it is being heard almost every day of cyber crime cases reported by the victim. After examining the reports of the cases of the victim involved, several points have been identified as the reason and motivation behind a cyber crime.

1. Duped by Attractive Advertisement Offers

Various advertisements of various services or products in the cyber medium offering price that is much cheaper than the market price, and great promotion. Most cyber consumers do not investigate beforehand of the company's background or cyber trader before making purchases online. It has been reported before of a buyer who was cheated by a seller when making a purchase of three mobile phones because of the buyer was impressed with the cheap price offered through online purchase. This caused the victim to suffer losses amounting RM3,250 when the victim only received stone mortar sent by the seller (Mohamad Fahd, 2012).

2. Lack of Knowledge in Doing A Safe, Online Transaction

Most cyber consumers do not know how to do online transaction safely because of lack of awareness on computer safety. They thought that online purchase is as the same as purchasing at any store or supermarket, without them realizing that the online transaction is more dangerous. This is because there is a higher possibility of theft of confidential information, like the theft of their password and electronic banking information. Sensibility on the statistics and risk of the occurring cybercrime is also less because they take the said issue lightly.

3. Do Not Know the Allocated Legal Channel

Many victims of the cyber criminal did not know what they should do when they were cheated as they made online purchases. Most of them did not report their case to the authority like the Royal Malaysian Police or Malaysian Communications and Multimedia Commission, because they thought that cybercrime is only a petty crime and it is difficult to trace the criminal. Whereas, if they had given the cooperation to the authorities, their case can possibly be resolved based on the information given to the authorities. Most of the victims preferred sharing their case of being scammed online through social media or through their personal blog.

4. Greedy and Wanting to Gain Easy Profit

Human's natural tendency to be greedy and wanting something easily without having to go through hassle are among the cause of cybercrime occurrence. It is due to this attitude that the victim was frequently being cheated by the cyber criminal that took advantage of this opportunity by introducing various investment schemes, or hire for a service like typing data or other assignment. This is where if a person wants to join, that person must pay a registration fee, which qualifies the person to enrol or join (Nazura & Anita, 2002). Finally, after the registration and doing the requested assignment, they felt being cheated when they did not receive any payment from the organiser with various excuses given. In fact, to make matters worse, the organiser to an investment scheme was missing together with the investment money and the victim was left frustrated and suffering loss.

ISSN 2349-4379

MEASURES TO PREVENT CYBERCRIME

Cybercrime, which involves women in Malaysia can be prevented if several measures are taken and are given attention. Among the steps that can be adopted by the society, especially the ladies in overcoming the cybercrime, is the necessity to have a high level of awareness of the risk of this cyber threat. This situation is obvious, especially when they are using their personal computers. The ladies need to have a sense of responsibility to ascertain that their computer is guaranteed to be safe from viruses or elements that could jeopardize the security of important personal information. To avoid women from becoming victim of cybercrime, measures proposed are:

1. Get further and detailed information on the security of online shopping, 'chatting', e-mail and spam, and online scams.

- The challenges of the global era today show that consumers prefer doing transaction online. Various transactions, whether transaction of trading, rent, bill payment, etc., use internet as the medium. Consumers, particularly women should wisely investigate and analyse a product sold online before a transaction is carried out to avoid the victim from being cheated.
- Apart from that, women consumers are advised to read the disclaimer before filling any online form because any legal dealing online must be enclosed with this statement. If a disclaimer is not attached, consumers are advised to continue to leave this transaction.
- Limit online purchases and ensure that the websites visited use safety standards such as SSL (Secure Socket Layer), iVEST and digital signature. At the same time as well, consumers are constantly advised to observe the URL link in the email received. Make sure that the attached URL is an original URL. The email address used to send the email must also be an official email address, like www.ips.um.edu.my for example. If the email used is from a free email service like gmail, yahoo, MSN and so on, you should ignore the email.

2. Legal enforcement should be tightened so that it can be parallel with the current situation that is more challenging, with various cybercrimes that are increasingly sophisticated.

- Nowadays, various laws have been created and enacted in Malaysia in efforts to instil the culture of cyber security. Among them are the Computer Crime Act (Act 563), Optical Disc Act 2000, Digital Signature Act (Act 562), Telemedicine Act 1997 and Communications and Multimedia Act 1998 that are able to curb information thought to be able to commit cybercrime to Malaysian society.
- Realizing the implication of cyber threat, the government took ICT safety measures since year 1997 by establishing MyCERT and NISER in 1998 to provide consultancy services related to the security of ICT system network to the public and private sector. Such safety guarantee is greatly needed because the expenditure in ICT system network is high, reaching billions of ringgit. Global awareness on cyber threat, on the other hand has prompted the government to establish the **Institute of International Multilateral Partnership Against Cyber Threats** (IMPACT) in 2006.
- Nevertheless, as if for the sake of just proving that the country has particular procedures to screen the negative activities of cyber criminal, the existence of the current cyber law is not yet capable to curb or eradicate cyber crimes that are getting smarter and rampant. Malaysian cyber law is seen as not yet extensive enough and encompasses all aspect. Incident like sabotaging by spreading pornographic pictures that jeopardizing someone's dignity, especially women, was an inhuman act. Money theft through transaction by electronic transfer, pin number theft, credit card numbers, stealing data from database are rampant activities. However the country's existing cyber law is unable to prevent such cases.

3. Bank should also ensure that all matters prepared are guaranteed to have high security features such as the digital certificate from Malaysia Cybersecurity.

- This certificate is able to ensure that every website forgery is identified immediately. Hence, this setting can foil the attempt of irresponsible individual from committing cybercrime.
- Among the functions of Cybersecurity are ensuring cyber emergency reaction security and digital forensic, quality management of cyber security, professional development in the field of information security and outreach or public awareness (public awareness), Dasar Keselamatan Siber Nasional implementation, national technical coordination centre for the aspects of cyber security, research and risk of cyber threat study.

LEGAL PROVISIONS ON CYBERCRIME IN MALAYSIA

Looking at the threat brought by the result of technological and information advancement that is hitting the whole world, various countries has enacted acts and cyber law for their own countries in ensuring that there is an existence of control and protection for consumers from being victim to cyber criminals that are always posing security threat through cyber mediums. Malaysia is also among the countries that are not exempted in the enacting of cyber related acts since the beginning of technological and information development in this country. This is to ensure that there is rule of law and harmony among society, especially to tackle cybercrime and abuse which occurred through cyber medium. Among the related special acts are:

I. Computer Crime Act (1997)

II. Communications and Multimedia Act (1998)

III. Consumer Protection (Electronic Trade Transactions) Regulations 2012

All acts were enacted and improvements were carried out from time to time in line with the technological and communication development to tackle the increasingly challenging and worrying misconduct and abuse particularly pertaining computer security and towards computer users. Acts and rule enacted are suitable with the change of time and era, and in line with the emergence of various new cybercrimes that always came up with various modus operandi. They also became the reference for cyber crime cases which occurred in Malaysia where they were usually read together with other criminal codes in court for crime conviction.

CONCLUSION

It is no longer deniable that today, many have fallen victim to cybercrime, whereas crime like this is difficult to be retained. Women are also not spared from being the target of criminal in fact they have already been targeted as victim. The fact is Islam has outline a few general guides for its ummah to always be vigilant, not to believe matter without proof, avoid sales and purchase of goods that are of unknown nature and condition, to look after social boundaries, to not be too enthusiastic with opportunities offered by any party and so on. Islamic religion also denounces crime acts by imposing punishment whether in the world or in the afterworld. Islam forbids an act like stealing, cheating, raping and disturbing the peace of other people.

REFERENCES

[1] Ahmad Shawal A. 2012. Facebook, Manfaat atau Mudharat. In. Melati Sabtu (Ed,), Penulisan Ilmiah Kolej Komuniti Temerloh. Temerloh: UPeN, KKTM.

[2] Mohd Dahlan A. M. & Ida S. 2010. “Jenayah dan Masalah Sosial Di Kalangan Remaja: Cabaran dan Realiti Dunia Siber”. Paper Presented at Jenayah Cyber dan Isu Pemerdagangan Manusia di Malaysia, 26 Aug 2010, Resital Hall, Universiti Malaysia Sabah, Kota Kinabalu.

[3] Anita A. R. dan Nazura A. M. 2004. Jenayah Berkaitan Dengan Komputer Perspektif Undang-Undang Malaysia. Kuala Lumpur: Dewan Bahasa dan Pustaka.

[4] Rusli H. A. et al. 2003. Teknologi Maklumat dan Penggunaannya. Petaling Jaya: Prentice Hall Pearson Malaysia Sdn. Bhd.

[5] Jalaluddin A. M. 2008. Siber Urbanisme: Pemikiran Melayu Tentang Bandar Pintar. Sari, (26), 111-125.

[6] DSP Mahfuz A. M. “Cybercrime: Malaysia”. Accessed at February 04 from; http://www.skmm.gov.my/skmmgovmy/media/General/pdf/DSP-Mahfuz-Majid-Cybercrime-Malaysia.pdf ;

[7] Syahidi Bakar April 2012. Masyarakat Perlu Tangani Jenayah Siber. Utusan Malaysia.

[8] Thornham, S. 2007. Women, Feminism and Media. Edinburg: Edinburg University Press Ltd.

[9] Paasonen, S. 2005. Internet, Women and Cyberdiscourse. New York: Peter Lang Publishing.

[10] Framme, J. & Unger, A. 2012. Computer Games and New Media Cultures : A Handbook of Digital Games Studies. New York: Springer.

[11] Huddleston, P. 2011. Consumer Behaviour : Women and Shopping. New York: Business Expert Press.

[12] Mohamad Fahd Rahmat 2012. “Aduh! Galaxy lesung batu”. Accessed Jun 10 2013 from, http://www.hmetro.com.my/articles/20120110050106201201100501 06/Article

[13] Nazura A. M. & Anita A. R. 2002. “Permasalahan Frod/Penipuan dan Komputer : Sejauh Manakah Penyelesaiannya?”. Malayan Law Journal (1).

[14] Computer Crime Act (1997)

[15] Communications and Multimedia Act (1998)

[16] Consumer Protection (Electronic Trade Transactions) Regulations 2012