PalArch's Journal of Archaeology of Egypt / Egyptology

THE SOCIAL RISKS OF ELECTRONIC EXTORTION

Hiba Abdul Mohsin Abdul Kareem

Assit. Lecturer, Women's Studies Center, Baghdad University, Iraq

Hiba Abdul Mohsin Abdul Kareem , The Social Risks Of Electronic Extortion , Palarch's Journal Of Archaeology Of Egypt/Egyptology 18(4). ISSN 1567-214x.

ABSTRACT:

The blackmailthat girls are exposed to is the most dangerous form of cyber blackmail prevailing in society. It is one of the hidden crimes with wide-ranging social dimensions. The cases of blackmailing against girls by blackmailers of different forms become the top news and social networking sites.Accordingly, this shows the importance of the topic of this study, as it affects not only the girl but also all members of her family due to living in an Eastern society subject to authentic social traditions and customs. In this regard, cyber blackmail is one of the main risks facing social media users who do not have sufficient knowledge of information security.Thus, they will fall victim to various types of cyber blackmail, especially if the girl is threatened with private family photos or scandalous clips and pictures or private conversations, whether between the blackmailer and the victim or the girl's private conversations. So,hecoerces her using various ways and means, whether financial or moral.Hence, the problems of the Internet become increasing despite the rapid technological development prevalent in most Arab and Western societies. The electronic mobs' exploitation of personal accounts, especially those related to girls, as being targeted by those criminal groups, is performed using blackmailing with several social and psychological dimensions. Because of the importance of the topic, the efforts of the Iraqi Ministry of Interior are continuing to pursue and arrest the blackmailers who targeted teenage girlsafter deceiving them and obtaining their private pictures, then blackmailing them to obtain money or forcing them to do indecent acts that negatively affect the girl and her family. This research therefore attempts to identify the most important social risks of cyber blackmailing against girls, and to highlight the role of social awareness in confronting it.

INTRODUCTION:

In recent decades, the world has witnessed a major revolution of information technologies in all fields, and it became difficult to dispense with their services. However, it also contributed to the emergence of a new form of crimes committed by some users of this technology, which are characterized mostly by the seriousness and ease of committing them. By clickingthe mousebutton, the blackmailer can browse many accounts and websites of people, especially girls. This type of crimes iscalled cybercrimes. Some traditional cyber criminals have left off the crime of stealing credit cards and identification information, and turned to a simpler way, which iscyber blackmailing. They use threats containing selfies, or digital films of the victim to demand money instead of stealing them. Cyber blackmailing is a new and alien phenomenon to Iraqi society, which has occupied all the media as well as public opinion. Therefore, it become widely mentioned to tell us many painful stories about the reality of this crime. Girls often fall victims to such crimes, and the blackmailer begins to use all possible and impossible means to stalk the victims and reach his goals by coercing them. The victim often responds to him because of the fear of shame that will affect her and her family if she does not respond to hisdemands.He threatens her to publish pictures or videos or declare a secret information if she does not pay him money or do immoral acts.Consequently, the female is the most targeted by blackmailers.

A. Theoretical Section:

1. Research Problem:

Since the last decade of the 20th century, the world has witnessed a significant developmentin the field of information and communication, resulting in a series of repercussions at all social, economic and technical levels. This has led to the emergence of the phenomenon of blackmail, which is an alien and new phenomenon to society due to the continuous progress of these means.This phenomenon increases with the increase of social networking sites.This in turn increases the blackmailer's chance to obtain information about the victim and her personal pictures and threaten her to publish these pictures in immoral situations or force her to pay money or commit immoral crimes in the absence of religious and moral awareness of the blackmailers. Accordingly,the problem of this research lies in that many social risks result from cyberblackmailingagainst girls.

2. Research Objectives:

This research aims at:

1. Identifying the causes of the spread of cyber blackmailing phenomenon.
2. Defining the most prominent risks caused by cyber blackmailing.
3. Providing community awareness about the risks of cyber blackmailing.
4. Developingsuggestions and recommendations to reduce this phenomenon, preventand manage it.

3. Research Significance:

The importance of this research is highlighted by the implications of the spread of cybercrimes in society as an emerging development. Therefore, the theoretical and practical importance of research is embodied in the emergence of cyber blackmail in Arab-Islamic societies in generaland in Iraqi society in particular.This shows the

originality of this study, considering that our society is known for itscustoms, traditions and social norms and conserving of all that is exposed to reputation and honor, especially the victims of this crime are often girls.

A. Concepts and Scientific Terms:

1. Social Risks:

Linguistically, riskmeans be on the verge ofthe end, so it is said he takes a risk, a riskysituation (e.g. blackmail).Riskrefers toa serious situation,the possibility of having something bad as a form of misfortune, and a condition that suggests anxiety and fear (Abu Musleh, 2006, p. 34). Many Western scholars including Giddens, Luhmann, Alain Touraine and others have referred to this term. Individuals expect that the risks are related to places of earthquake, highlands or contaminated places. However, the reality is different, as the risk is every threat to which a human being can be exposed, whether it is a financial or moral threat. Giddens (2003, p. 43) states that our world is threatened by many of the risks we have created by ourselves, such as technological development that is being misused by mean people.

Luhmann (as cited in Wallace & Wolf, 2012, p. 122) defines the risk as the potential harm to the individual by external influences, i.e.,it is not done by the individual, such as an earthquake or the threat by the blackmailers. As for social risk, it is a threat to a large number of people, even if at first glance it appears to be intended directly at a particular person. It often affects societal values. There is a correlation between risk and threat. Threat means a person's expressly stated intention to causea physical harm to him or society, and thus it poses a risk as it moves from possibility to reality. These threats, which turned to risk experienced by a girl in case ofcyber-blackmailing, may pose psychological and social crises that are difficult to be disposed of (Beydhoun, 2012, p. 264). Procedurally, social risk can be defined as a risky threat directed at a person (represented by girls) carrying many social threats, such as fear of revealing a particular secret or publishing a video or selfies that have social consequences affecting the girl and her family and therefore affect the entity of society. Blackmail is thus one of the most common social crimes that has a negative impact on the social environment.

2. Cyber Blackmail:

Linguistically, blackmail is to obtain money or benefit from someone under coerce and threat to expose a secret or to reveal information harmful to reputation(Al-Afriqi, 1990, p. 312).In law, it is defined as a crime committed against a person to force him to hand over money, or to sign a document due to being threatened with the disclosure of a particular matter or to charge him with a crime(Kareem, 1987, p. 11). It is to threaten to disclose certain information about a person, or to do something to destroy the threatened person, if the latter does not respond to the blackmailer's demands.This information is usually embarrassing, personal or of has a socially destructive nature. It is a form of cybercrimeswhere the crime is carried out through modern technology.It represents offences committed against individuals or groups motivated by harming the victim's reputation or having a material or moral harm using online social networks (e.g., chat rooms, e-mail, mobile phone, and computer). Types of cyber blackmailinclude:

a) Financial blackmail: money is requested from the victim in exchange for not revealing her secrets.
b) Emotional blackmail: it is by forcing the victim to carry out the blackmailer's wishes by committing sexual acts. This is usually done through demand, resistance, pressure, threat and submission.
c) Moral blackmail: it is done by threatening through the use ofabstract means like the use of harsh language in threatening and promising to reveal the victim's secret, regardless of its type whether pictures, videosetc.

As for the procedural definition of cyber blackmail against girls,it refers to the practice of pressure, threat and coercion against the girl by a blackmailer to achieve his criminal purposes, aiming at having afinancial or moral benefit. It may be done through one of the social and electronic media, such as Facebook, chat rooms, telegrametc., putting the victim in trouble.Therefore, she either submits to his demands or exposes herself to social scandal in case of refusing to respond to his demands.

B. Literature Review:

Csonkp (2002) studied cybercrime, aiming at identifying online crimes in terms of their causes and effects, cyber criminals and their characteristics. The sample consisted of (358) U.S. institutions including government agencies, banks, financial and health institutions and universities. This study used the descriptive method, survey, the comparative method, and the historical method. The researcher employed interviews, observation and the questionnaire as statistical tools for collecting data. This study demonstrated the risk of cybercrime and the increase in the financial and moral losses. It showed that (85%) of the institutions were exposed to cyber breaches in previous years, and (64%) of them suffered from financial losses of approximately $378 million. It revealed that the majority of the study sample represented by (94%) of American institutions experienced virus attacks in various criminal ways. With regard to the source and nature of the attacks, the study indicated that the largest proportion of such attacks represented by (25%) were carried out outside institutions in 2000, and the rate of increase in attacks was (7.5) per year. Finally, the study stated that the percentage of employees who abused the Internet for personal benefits was (19%), ranging between the misuse of email and uploading pornography on the internet.

In 2010, al-Shamrani conducted a survey on the phenomenon of blackmail in Saudi society from the viewpoint of criminal control officers. This study aimed at determining the reasons that led to the spread of cyber blackmailing in society as well as identifying the means and forms used by blackmailers who abuse the electronic sites to blackmail girls. The researcher employed the descriptive method in his study. The sample consisted of (220) officers in charge of criminal control in the police station of Riyadh city. The researcher used the questionnaire, interviews and observation as statistical tools for collecting data. The study showed that the family disintegration and the lack of control of their children is one of the most important reasons that led to the spread of cyber blackmail. It confirmed that improving the standard of living of individuals and caring for the poor families is one of the most important factors to confront blackmail in society. In addition, the blackmailed girls' fear of scandal when reporting to the security authorities and the negative attitude of the society towards the victim when revealed on social networking sites are among

the most important obstacles that limit the effectiveness of confronting crime in Saudi society. The study demonstrated that the threat to publish the picture, secret conversation or information by phone is one of the most important ways of blackmailing the victim.

Musab (2017) carried out a study entitledthe crime of cyberblackmailingagainst girls: a social survey in Baghdad from the perspective of lecturers and students of Baghdad University. This study attempted to define cybercrime and its characteristics in general. It aimed atidentifying the most prominent manifestations of the crime of cyber blackmailing and determining the factors leading to the exacerbation of the crimes of cyber blackmailing against girls through social networking sites. The sample of this study consisted of (500) lecturers and students selected purposefully fromBaghdad University including four colleges: Media, Law, Engineering Khwarizmi and Science.In addition, some interviews were conducted with students in various departments. The study also used a range of statistical means to achieve the objectives of the study.The study found that most participants who were blackmailed are students represented by (88.9%) and most of them are female, while the teaching staff only (11.0%) of them were personally blackmailed. It indicated that (71.0%) of the students emphasized the weakness of sanctions and legal legislation, while (77.0%) of lecturersemphasized the importance of curiosity and exploration, which werethe top reasons leading to the crime of blackmail in the society. Facebook ranked the first in terms of the sites through which the students were exposed to blackmail (66.9%). As for lecturers, their response was limited to four sites where they were blackmailed, namely, Facebook, Messenger, WhatsApp,and Viber, and Facebook came the first (53.8%). The study showed that financial blackmail is the most common form of blackmail to which the participantswere exposed.It revealed that (74.5%) of the students stressed the need to spread and activate religious discourse, whereas (86.0%) of lecturersemphasized the need to embrace the girl and provide her with passion and kindness to avoid falling into the trap of blackmail.

D. Data Analysis:

1. Reasons for the Spread of Cyber Blackmail

a) Weakness of religious faith: this isbecause of poor adherence to the provisions of Islam, especially the lack of commitment to perform duties, which are one of the most important factors affecting the orientation towards committing criminal behavior. Religion contributes to maintaining the cohesion of society as well as enabling its members to adapt to life conditions and crises due to the changes occurred in most societies in general and Iraqi society in particular in various aspects;in addition to the social, economic and political view that has led to a change in the lives of individuals.So, some of them have forgotten Allah, and hence He makes them forgettingtheir selves. They started to earn money illegally and commit sins without shame (Al-Rubaie, 1998, p. 13).
b) Misuse of modern technology: misuse of the Internet, lack of sufficient knowledge of modern technologies and ignorance in their use are one of the most important reasons leading to the victim's fall in the blackmailer's trap. In addition to the diversity of social media, including visual means, which is done by opening cameras to see each other, recording, and keeping videos in certain files to be used later. These means led to the ease of penetration of personal information, especially with the global developments in the field of

electronics, conversations and correspondence facilitated by networks by downloading files including Facebook, Twitter etc. (Muhammad, 2009, p. 37).

c) Emptiness: depriving children of love and passion by their parents is the reason behind their search for satisfying their emotions and desires in love, appreciation and praise outside the home. This results in a defect in the communication relations between family members. Therefore, it is necessary to improve the role of the family through:embracing the children; meeting their basic needs such as food and drink;increasing their religious faith; respecting their feelings and appreciating them; guiding them towards using their free time in useful activities such as sports and education; and ensuring that they are not exposed to sexual excitement that may lead them to criminal behavior and exploitation by bad friends (al-Heet, 2015, p. 44).
d) Poverty: the low living standard of the family greatly affects the commission of crime. When the income of the family is low and does not meet their basic needs, this may lead to unethical behaviors such as robbery, fraud, blackmail and other criminal means in order to satisfy their needs and obtain money. Unemployment also plays an influential role in attracting young people towards such behaviors. In addition to the absence of self-censorship and having bad companions whosupportcommitting unethical behaviors (Al-Quraishi, 2011, p. 235).
e) Love of experience, imitation, influence, and bad friends: undoubtedly, company has a big role in the influence, as Almighty Allah says:

- (And (remember) the Day when the Zâlim (wrong-doer, oppressor, polytheist) will bite at his hands, he will say: "Oh! Would that I had taken a path with the Messenger (Muhammad صلى الله عليه وسلم)) (Chapter: Al-Furqān, 27).

In the absence of self-censorship, bad companions play an effective role in the process of cyber blackmail. For example, a girl may blackmail her friend who trusted her and sent her personal pictures or family videos whenquarrelling (Amin, 2006, p. 98).

f) Failure to take caution to discover this crime when it occurs: most individuals who use the Internet do not use safety software and techniques to be protected against penetration and spying. This entails failure to discover the crime committed on time,which will undoubtedly obstructthe confrontation of this crime (Al-Shanawi, 2008, p. 65).
g) Failure to report the crime of cyberblackmail for fear of the scandal that will affect the girl and her familyis one of the reasons for the spread of such crimes.

2. The Risks or Consequences of Cyber Blackmail:

a) Social risks: the spread of this crime is a violation of the civil peace, as it is a risk and a threat to the individual and the family and therefore society. The number of young men and girls who are reluctant to marry because of the secrets revealed to the society by blackmailing has increased.Injustice and oppressionalso become common because the victim remains under the control of the blackmailer.
b) Psychological risks: these risks are represented by such effects as mental disorder, anxiety, fear and depression affecting the victim, and result in a troubled and depressed personality, and may reach to thinking about suicide to

get rid of the scandal that affected her and her family because of cyberblackmail (Al-Badina, 2014, p. 89).

c) Security risks: the crime of cyberblackmail is one of the most serious crimes threatening the entity of society and its security. The victim may be exploitedto commit a crimein favor of the blackmailer, such as robbery, murder, threats and coercion to do immoral acts.

3. Community Awareness about the Risks Of Cyber Blackmail:

a) The family must strengthen the religious faith, warn against inattention and familiarity with frankness by conversation with children, especially girls. This is done through proper social upbringing as the basis that protects children from delinquency and crime.
b) One should becautious when using mobile devices, especially in the filming of females because the device may be lost or stolen by abusers.With the warning not to put the memory cardin the phone during its maintenance because some workers in these stores exploit thepictures and apply the software to retrieve the deleted content. Additionally, there should be a strict control of movies and publications imported from abroad and films that encourage criminality.
c) One should communicate with the concerned authorities in case of blackmail, with the need to be honest with the mother and father when informing them about the matter in order to confront the blackmailer and not to communicate with him under any threat, and to hold him accountable by law (Al-Jarisi, 1999, p. 73).
d) The school should have an effective role as being one of the effective institutions in society. It is the second entity after the family and media in the formation of a conscious mentality for individualsthrough the standards and values provided by the educational system for generations. At the same time, it is the solid foundation for the establishment of social security through which social and moral values are acquired and developed as well as to reduce the degree of aggressiveness of individuals (Al-Sa'adawi, 2004, p. 19).

By looking at some studies in this field, some types of electronic theft were identified, through which electronic extortion is likely to take place.

One of these types is identity theft, which is one of the types of cybercrime that is widespread on Facebook on a large scale, so the hacker breaks into the information of a person's profile after stealing information from the Internet and employing it for inappropriate or unlawful purposes. Because of the large number of Facebook users, the user’s identity theft has become easy and can be accessed and fake accounts created through it. This results in a state of insecurity.

The results of one of the studies conducted in Saudi Arabia indicate that electronic blackmail is a major threat, as it is linked to the violation of their privacy. e .(Al-Makramia, 2015 , p. 22)

In this context, the Iraqi government has taken appropriate measures to control cyber blackmail. It has created free hotlines to follow up on blackmail cases and explain all the conditions of the case to the competent authorities via numbers (533) and (131) as an attempt to deter blackmailers and to educate all members of society on these important issues.

4. Preventive methods:

There are some methods and ways in which a person, and a woman in particular, can protect and protect themselves from the dangers of social media, in which electronic blackmail is the most severe and most dangerous of these:

a) Protecting your personal information and data, and not giving it to anyone, especially the personal card numbers and bank card numbers, or the password for your personal account on Facebook. (Khalifa, 2016, p. 119)

b) Using the privacy settings of social networks, to make your data safe from hackers and vulnerable souls. (Radi, 2003, p.24)

c) Using unfamiliar and strong passwords, so that they are difficult to penetrate. (Rahmeh, 2007, p.74)

d) Avoid sharing private and personal details, including news, photos, or video clips, especially for families. (Shalaby, 2008, p.65)

e) Always be careful, and do not respond to any messages or electronic links sent to you, as this may be a trap for penetrating your personal account, stealing your important and private data, or information related to your business. Then you are exploited, bargained, and blackmailed. (Johannes, 2015, p. 278)

f) Follow up on children on an ongoing basis, and try to save them and intervene at the appropriate time, especially if they show suspicious symptoms, such as anxiety and fear. (Al-Azza, 2015, p. 23)

The Most Important Conclusions:

1. Cyberblackmail is a form of cybercrimes.It is carried out using information networks, theft and fraud.
2. The crime of cyberblackmail often causes other crimes, such as adultery, murder, theft and different forms of violence.
3. Cyber blackmail has many ways and means.
4. Cyberblackmail is considered a cross-border crime, as theblackmailer may be in a country and the victim in another country.

Recommendations and Suggestions:

1. Raising the level of social awareness of the vulnerable groups represented by girls, as an attempt to prevent the risks of cyber blackmail. This is done by giving them more support and encourage them to be honest and allow the family dialogue by holding seminars and conferences to educate families about it.
2. The proper use of social media by all family members, and not to post and share personal pictures via Facebook, Instagram, WhatsApp etc. due to theirundesirable social and security implications.
3. Strengthening family ties and preventing family disintegration, with continuous follow-up of children, especially at critical age stages, and not drifting behind globalization in a chaotic way, because this contributes to the destruction of the family entity and the loss of children, especially girls.

4. Activating the role of community police and publicizing the free numbers by the State in all government institutions and satellite channels.This is done in cooperation between the Ministry of Interior and the Ministry of Communications and the relevant authorities.
5. Holding seminars and workshops within schools for raising awareness of the risks of exposure to cyber blackmail, in cooperation between the school administration and a representative of the Ministry of Interior and an expert in the field of electronic technologies and communications.
6. Do not keep any bank accounts, personal or family photos or secret information on any account, whether on computers or mobile phones as all of these devices have become connected and can be hacked by blackmailers, making the subject extremely dangerous.
7. Enacting and activating the implementation of laws on cybercrime in a scientific and legislative way, taking into account the type of crime committed and its consequences. This is done in cooperation between the Ministry of Justice and the Ministry of Interior.
8. Increasing the activation of the mechanisms of international cooperation by signing agreements with countries that criminalize this type of crime, because this constitutes a protection network at the domestic and international levels of State.
9. Informing the official authorities in case of exposure to cyber blackmail via the numbers available by the security authorities.
10. Highlighting the issue of cyber blackmail by the official satellite channels, and building bridges of trust and cooperation between citizens and the security services.

CONCLUSION:

In conclusion of this research, it can be said that electronic blackmail is one of the most dangerous crimes currently prevalent in most societies. This is due to the rapid developments of technology, to the frequent use of technical systems for communication and information and to the increase in the number of people who use the Internet around the world, and for this we see an increasing increase in the rates of cybercrime of all kinds and forms. This requires specialists in this field to find new and successful ways to control these crimes, and it requires us as researchers to address such sensitive topics affecting the security and safety of society in order to reach constructive solutions and solutions to the problems resulting from these crimes. Which has become Alaa a direct attack on the family and this in itself requires the development of feasible plans for people to increase the sense of community security. It also requires officials to move towards getting rid of the reasons behind the commission of these types of crimes. Involving youth in programs and projects that are beneficial to them and their community.

REFERENCES:

Holly Qur'an.

Al-Azza, S.(2015) . Parental Guidance, Its Theories and Treatment Methods, House of Culture for Publishing and Distribution, Amman .

Abu Musleh, A. (2006). Dictionary of sociology. Amman, Jordan: Mashreq Cultural Press.

Al-Afriqi, A. (1990). Tongue of the Arabs, 1st ed. Beirut, Lebanon: al-Fikr Press.

Al-Badina, D. (2014). Cybercrimes: Concept and causes. In Scientific Forum, Crimes Created in the Light of Regional and International Changes and Transformations, Faculty of Strategic Sciences, Amman.

Al-Heet, A. (2011). Crimes of defamation, insult and contempt committed through electronic media - Internet, mobile phone network, traditional media and publications: a comparative legal study. Amman, Jordan: Culture Publishing and Distribution Press.

Al-Jarisi, K. (1999). Perversion of youth. Riyadh, KSA: Mishkat Islamic Library.

Al-makrami, H. (2015). Online Self-disclosure across cultures : a study of facebook use in saudi Arabia and Australia . phd thesis . queenslandunirersity of technology , Australia .

Al-Quraishi, G. (2015). Criminology, 1st ed. Jordan: Safaa Publishing and Distribution Press.

Al-Rubaie, F. (1998). Impact of some social and economic variables on crime in Iraq (PhD. Thesis). University of Baghdad, Iraq.

Al-Sa'adawi, S. (2004). Values and their relationship to some behavioral problems among second-stage students (Master thesis). Ain Shams University, Egypt.

Al-Shamrani, A. (2010). The phenomenon of cyber blackmail in Saudi society from the perspective of criminal control officers (Master thesis). Nayef Arab University for Security Sciences, KSA.

Al-Shanawi, M. (2008). The new fraud crimes. Egypt: Law Books Press.

Amin, A. (2006). Falsifying the awareness of young people between globalization and new agitators. Egypt: The Egyptian General Book Authority.

Beydhoun, A. (2012). What do you say? Common and real in the conditions of women. Beirut, Lebanon: Al-Saki Press.

Csonkp, P. (2002). Internet crime, the draft council of Europe convention on cybercrime: A response to challenge of crime in the age of internet computer law. Security Report, 16(5).

Giddens, A. (2003). A wild world: How globalization is reshaping our lives? Translated by: Abbas Kazim. Beirut, Lebanon: Arab Cultural Center.

Johannes , M . (2015) .lived experiences of divorced women in rural Ethiopia , international journal of political science and development , vol 3 .

Kareem, A. (1987). Dictionary of Legal Terms, 1st ed. Cairo, Egypt: Arab Renaissance Library.

Khalifa, I . (2016) . Social Media - Modern Online Change Tools, Arab Group for

Training and Publishing.

Mohammed, N. (2009). Information Crimes. Riyadh, KSA.

Musab, N. (2017). The Crime of cyber blackmail against girls: A field social study from the perspective of lecturers and students of Baghdad University.

Radi, Z . (2003) . The Use of Social Media in the Arab World, Education Magazine, Issue 15, Al-Ahliyya Amman University, Amman.

Rahma, A . (2007) . The Internet and the Techno-Social System, Center for Arab Unity Studies, Beirut.

Shalabi, K . (2008).the press report and its Islamic regulations, Al-Hilal House and Library, Beirut.

Wallace, R. & Wolf, A. (2012). Contemporary theory of sociology. Translated by Mohammed Abdul Kareem Al-Hawrani. Amman, Jordan: Majdlawi.