Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 3, 6882-6893
Omar Abdulsalam Hussein et al.

Cyber Blackmail Crime Against Women - A Case Study

[1]Omar Abdulsalam Hussein
Law Research Centre, Faculty of Law, UniversitiKebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia,
P97504@siswa.ukm.edu.my.
[2]SProf. Dr. Nazura Abdul Manap
Faculty of Law, UniversitiKebangsaan Malaysia, 43600 UKM Bangi, Selangor,Malaysia.
nazura@ukm.edu.my
[3]Prof.Dr.Muhammad Rizal Abdul Rahman
Faculty of Law, UniversitiKebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia.
noryn@ukm.edu.my./*Correspondence: P97504@siswa.ukm.edu.my,
ORCID ID :https://orcid.org/0000-0002-7106-9844

Abstract:
Cyber blackmail against women is a pernicious form of cybercrime that has become pervasive in modern society. It is a covert crime with significant social ramifications. Blackmail cases against women have made waves on social media.During the pandemic Covid-19, a survey by the Iraqi Ministry of Interior women found that 60% of women in Iraq have been victims of cyber-blackmail crimes, which is a lot. Here is the main problem when you ask whether or not Iraqi law is good enough to protect women from cyber threats.This demonstrates the significance of the subject of this study, as it impacts women and their families, as authentic social traditions and conventions govern oriental civilization. The paper examines pertinent national legislation and regulations and the contemporary challenges associated with cyber-blackmail against women. Additionally, the study will discuss the most critical components of a lawsuit and measures for preventing this crime.The research examines relevant national rules and regulations in Iraq and the current issues of cyber-blackmail crime against women. The descriptive and analytical technique is used to describe, analyze, and diagnose the problem in all dimensions. As a result, the article contributes to a greater understanding of cyber blackmail by providing a comprehensive discussion of a variety of issutopicsIraq and the reasons for the expansion of cyber blackmail and an analysis of the most critical aspects of litigation and community awareness regarding the crime of blackmail. The paper finishes with prevention strategies and advice for stakeholders on how to bto address this situation.
Keywords: Cyber blackmail, women, legislation, social media, victims.

Introduction:

Since the US invasion of Iraq in 2003, the phenomenon of the spread of cybercrime has swept the country, especially crimes targeting women, including crimes of blackmailing girls, slander, defamation and indecent assault against them through social networking sites, which caused significant problems that afflicted the cohesion of Iraqi families. Specialists believe that the reasons for the spread of these crimes are due to the weak application of the law in Iraq at present, in addition to the decline in the moral and value system in society, the absence of religious scruples, and the spread of poverty and unemployment experienced by some Iraqi families.

Lawyer and judicial expert Tariq Harb believes that cybercrime of all kinds, such as extortion and drug crimes, during the period of social separation since the outbreak of the Corona pandemic, has now constituted 35% compared to other criminal offenses.Some electronic crimes also target the promotion of significant crimes due to the absence of legal culture in this type of crime, as the representative of the Legal Committee in the Iraqi Parliament, Hussein Ali Al-Aqaba, says to Al Jazeera Net[1]. The purpose of this article was to provide an analysis of the phenomenon and the most significant aspects of litigation. The research was conducted using a large dataset comprised of several hundred cases filed with Iraqi courts, several of which will be discussed in this study. These contents were analyzed to denote and classify essential topics and issues.

Research Questions

What cyber blackmail threats?
What is the most important the lawsuit side?
What are the reasons for the expansion of cyber blackmail?
How are they to be avoided?

Cyber Blackmail Threats

Cyber blackmail is an online crime in which hackers seize control of your data, website, computer systems, or other sensitive information to extract payment. It frequently manifests itself as ransomware and distributed denial-of-service (DDoS) assaults, both of which have the potential to cripple your organization. Additionally, technology enables threats to be conveyed to many people using a phony identity or another person's identity, potentially magnifying dread or anxiety[2]. Blackmail takes many forms and has many definitions. For example, among other things, the use of threats to damage a person's reputation, put another person to shame, or reveal "any secret that affects another person" to coerce a victim to do or abstain from doing any act against his will. According to the U.S. Sentencing Guidelines, the term "blackmail" refers to obtaining a thing of value from another person through the unlawful use of (a) force, (b) fear of bodily injury, or (c) threat of bodily injury[3].

Money, property, advantage, or even a sexual relationship are examples of "things of worth." Threats of blackmail include making or implying threats to induce the victim's belief that their power, fortune, social standing, personal or work security, or self-esteem may be jeopardized. Blackmailers must employ threats to "grab" or "acquire" property, not simply disenfranchise or dispossess the victim. Blackmail is the unlawful acquisition of another person's property 'with his cooperation' through the use of threats. Professor Stephen Shafer, Director of the Harvard Law School's John M. Olin Center for Law, Economics, and Business, stressed that the threats must be credible enough for the victims to feel a significant probability of the threat being carried out if they do not comply. However, as demonstrated in several cases, victims who submit to blackmail threats are more likely to face recurrent demands from the perpetrators,

[1] Threat, blackmail and defamation.. Cybercrime is expanding in Iraq and women are its victims, Al Jazeera Net, https://www.aljazeera.net/news/women/2020/9/28/أبرزها-الخيانة-الزوجية-الجرائم. Last visit 15 April 2022.

[2]Uma, S. (2017). Outlawing cyber crimes against women in India. *Bharati Law Review*, *5*(4), 103-116.

[3]Uma, S. (2017). Outlawing cyber crimes against women in India. *Bharati Law Review*, *5*(4), 103-116.

resulting in a lengthy relationship of control and dependency[4].

Common definition of Cyber Blackmail

Despite the multiple definitions of the phenomenon of cyber blackmail, they all agree on the element of threat that the offender uses and ends up in an illegal act of violence against the person if he does not comply with the blackmailer's demands. Let's look at the definition of the crime of cyber blackmail. We find that it is a crime related to obtaining money, property, or services from an individual or institution by threatening, using an illegal means, such as hacking a computer and taking pictures or videos of a person, or he may be the one who provided them to the blackmailer himself. The blackmailer asks for Money in return, and if we analyze this definition, we conclude:[5]

"If a person is threatened and forced to pay money, service, or give up property, this is an assault. Explicit on the right to private property represented in money and property, as well as an attack on the individual's right to security and safety through the use of the threat element, which is supposed to be safe for the individual to his life and private property from assault."

"The penetration of mobile phones, obtaining private correspondence, and threatening the person violates the confidentiality of correspondence and the sanctity of the private life of individuals guaranteed by the constitution."

Lawsuit Side

Blackmail and cyber threats can take on a variety of shapes and settings, allowing for multiple explanations and intriguing arguments and perspectives. The following subsections discuss various aspects of threat intent and reality.

Intention as an element in Lawsuit

Intention cannot be accurately defined in a stricter and narrower sense since it encompasses a broader scope and cannot be constrained by a rigid composition of its meaning. The intention is the deliberate use of a person's mental powers to perform an act with the intent of completing or satisfying a goal. To intend is to have a set purpose of accomplishing the desired goal; thus, the term "intention" refers to the state of mind which anticipates and wishes the possible repercussions of his conduct. It should be observed that intention cannot exist without foresight, as a man must decide to his satisfaction and anticipate the object of his stated purpose. Again, a man cannot intend to do what he does not desire to do. Criminal responsibility exists only if the individual was in a guilty psychological state at the offense. The United States Model Penal Code defines intent in four distinct categories: purpose, knowledge, recklessness, and negligence (in descending order of guilt).

The term "intent" has a variety of interpretations, and the judicial repercussions vary according to the understanding accepted by the court. As she has stated in cases involving fundamental criteria for criminal law interpretation, "I presume intent [anything more than negligence] is the criminal intent needed by criminal legislation[6]." It is self-

[4]Vasiu, I., &Vasiu, L. (2020). Cyber Extortion and Threats: Analysis of the United States Case Law. *Masaryk University Journal of Law and Technology*, *14*(1), 3-28.

[5]SuadAlisawee, The Crime of Cyber Extortion (A Comparative Study), University of Al-Qadisiyah, November 2019.

[6]Vasiu, I., &Vasiu, L. (2020). Cyber Extortion and Threats: Analysis of the United States Case

evident that unforeseen consequences can occur without identifying the defendant's illegal intent precisely. Determining "intention" presents an array of intriguing arguments and criteria. For example, the court determined that it was not essential to establish that the defendant intended or could carry out the threat in one case. Regardless, the defendant argued that evidence that he intended or could carry out the threats was relevant because it "may affect the required criminal intent," and the court agreed[7].

Real Threats as an element in Lawsuit

Most laws provide that no law restricting freedom of expression may be passed. However, specific categories of speech are excluded from this protection, including incitement to commit an unlawful act, obscenity, defamation, child pornography, fraud, and actual threats, as well as speech that is not an integral part of criminal conduct or speech that poses a serious and imminent threat to the government's ability to prevent it. Numerous legal experts have thoroughly discussed these points. However, the Public Prosecution Office is not entitled to prosecute speech just for being violent or objectionable[8]. For instance, when someone recommends "vengeance," this does not always imply violating any law. To complicate matters further, much of the harm that threats can inflict may result from the endorsement of, for example, some political message that "threats, however, must be defended." Individuals are protected from "fear of violence" and "fear-related disturbances," as well as "the possibility of the threat of violence" by prohibiting genuine threats.

Reasons for the Spread of Cyber Blackmail

There are several reasons for the spread of Cyber Blackmail discussed in detail.

Weak Belief

One of the most significant elements influencing the tendency toward criminal behavior is a lack of commitment to Islamic law, particularly the failure to execute religious tasks. Religion contributes to maintaining social cohesion. It enables its adherents to adjust to changing life circumstances, and crises brought about by changes in many areas of most societies in general and Iraqi society in particular. Additionally, some changes occur in individuals' lives due to social, economic, and political outlooks[9].

Inappropriate Use of Technology

Inappropriate use of the Internet, a lack of sufficient knowledge of modern technologies, and ignorance about their proper usage are the primary reasons victims fall prey to blackmail. Additionally, there is the diversity of social media, which includes visual ways for users to see one another, record films, and save them in specific files for later use. These methods have facilitated the hacking of personal information, particularly in light of global advancements in electronics and conversations and correspondence facilitated by networks

Law. *Masaryk University Journal of Law and Technology*, *14*(1), 3-28.

[7]Kareem, H. A. M. A. (2021). The social risks of electronic extortion. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(4), 8263-8273.

[8]Uma, S. (2017). Outlawing cyber crimes against women in India. *Bharati Law Review*, *5*(4), 103-116.

[9]Abdulhameed, R. S. (2021). Crimes Of Threats and Cyber Extortion Through social media: A Comparative Study. *Review of International Geographical Education Online*, *11*(12), 1022-1033.

through downloading files, such as on Facebook, Twitter, and others[10].

Sexual Goal

This is one of the most dangerous forms of electronic blackmail, in which the blackmailer seeks sexual services from the victim in exchange for silence regarding the publication of her photographs and sexual content, and things begin with the blackmailer requesting pictures of sexual content, followed by request to establish a voluntary sexual relationship. Without the victim's consent on the ground, the blackmailer forces the victim to do all that is required of sexual matters, and this is, of course, considered one of the most immoral things in the world[11].

Material Goal

The blackmailer uses all of the victim's sexual content to obtain money in exchange for his silence regarding the publication of this content; the process begins with the victim's photographs for a certain amount; after a while, the negotiations evolve into video clips, and the required amount increases; the more dangerous the content, the greater the amount required to be provided to the blackmailer. This is because poverty, or a family's low level of living, can significantly impact the commission of a crime. When a family's income is insufficient to cover its fundamental necessities, it may be tempted to engage in unethical behavior such as theft, fraud, blackmail, and other criminal acts.

Exploitative Purpose

Threats and sexual blackmail of this nature are employed against authorities, journalists, and prominent members of society. The victim is blackmailed using the same methods as in other forms of blackmail, but the reward is different. Here, the blackmailer seeks to elicit interest in the victim's social position or coerce him to cease following. The victim's case is connected to other criminals in society, and this is the most common type of blackmail to which the victim is subjected because the social circle is more significant than that of the average citizen and thus more dangerous to the victim, despite his awareness and knowledge of how to deal with such matters[12]. Most individuals who use the Internet do not use security software and technologies to protect their devices against hackers and spies. This will fail to disclose the commission of a crime on time, undoubtedly impeding the ability to face this crime[13]. Failure to report cyber-blackmail crimes out of fear of embarrassment for the girl and her family is one of the factors contributing to the spread of these crimes.

Cyber Blackmail Cases

After knowing the features of the crime of electronic blackmail and the most critical aspects of litigation, and the reasons for the expansion of the crime of cyber blackmail, the study sees the importance of addressing some issues of cyber blackmail in Iraq to know the extent of the strength of the Iraqi law to protect women from the crime of blackmail

[10]Kareem, H. A. M. A. (2021). The social risks of electronic extortion. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(4), 8263-8273.

[11]Bhardwaj, A. (2017). Ransomware: A rising threat of new age digital extortion. In *Online banking security measures and data protection* (pp. 189-221). IGI Global.

[12] Colonel Dr. / Ahmed Nahi Attia Colonel Dr. Ziyad Muhareb Muhammad Colonel / Ahmed Hashem Rady Colonel / Jamal Walid, Mr. Yusef Abadi Muhammad, Editor-in-Chief Major General Dr. Saad Maan Al-Mousawi, 2019, Electronic Extortion Modern Crime, Ministry of Interior, Directorate of Relations and Information.

[13]Kareem, H. A. M. A. (2021). The social risks of electronic extortion. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(4), 8263-8273.

and what mistakes women make to fall into such crimes.

Cyber blackmail is increasing in light of the growing number of social media users and the acceleration in the number of various chat programs. The blackmail process often begins with establishing a friendship with the person, after which the blackmailer lures the victim and records conversations with the victim containing offensive and explicit remarks. Finally, he threatens and blackmails the victim with a request to transfer sums of money, or the confidential information will be leaked. In some cases, the blackmail may reach a level where the victim's honor, customs, and traditions are violated, taking advantage of the victim's helplessness and ignorance of the methods used to deal with such cases. In many instances, the perpetrators seek to obtain explicit self-made or indecent materials to blackmail their victims.

One of the difficulties in applying these classic texts to criminal activities performed using current technology tools. Because the Iraqi Penal Code was enacted in 1969, when cyber blackmail did not exist, the articles above differ from the criteria for the crime of cyber blackmail in that the materials are traditional rather than cyber. The concept of blackmail lags behind the pictures of the other offenses mentioned above. As a result, there is an urgent need to re-examine the legal system to address the issue of criminalizing cyber blackmail and enforcing the resulting penalties. Nonetheless, the study will investigate these materials to determine their suitability for combatting cyber blackmail at the moment through cyber blackmail lawsuits as follows:

A woman was blackmailed through social networking sites, where the blackmailer was running fake pages on social media, and he was claiming to know the future of people and what they will face by sending some naked pictures. Unfortunately, many believe in these myths, including some women, and due to the lack of awareness among most women, prints were sent by women to this fake page. After sending the photos, the blackmailer began saving the pictures and threatening to publish them or send them to her friends and family, taking advantage of the victim's weakness and inability to face such challenges unless a monthly payment was paid or more photos were sent, and the goal was to put the victim under his control.

It later became clear that the blackmailer sometimes targets women living on the outskirts of cities, taking advantage of their inability to go and file a complaint against him, especially in eastern societies. Specialized lawyers contacted the competent authorities to help the victim after her appeal. After communicating with the competent authorities in the Iraqi Ministry of Interior, a committee was formed to investigate the case. The blackmailer was arrested and referred to the court under Threat Article 430 of the Penal Code No. 111 of 1969. The trial of the offender began.[14]

The Karkh Investigation Court, headed by the Karkh Federal Appeals Court in Baghdad, ratified the confessions of an accused who claimed to be a "fighter of cyber-blackmail crimes" through a private page for him and after the victims appealed to him to save them. It turned out that he was blackmailing girls and threatening them through social media. The court confirmed the defendant's confession of blackmailing a minor in exchange for money. The competent

[14] It did not file a judicial complaint regarding this case, but rather a personal action to help the girl, and I phoned the competent authorities to combat extortion, and it was agreed to move as soon as possible and help her.

court has instituted all legal procedures against him by Article (456) of the Iraqi Penal Code. The Karkh Investigation Court, headed by the Baghdad Federal Court of Appeal in Karkh, ratified the confessions of members of a network that specialized in hacking social media sites by taking pictures, copying electronic conversations, bargaining with females victims, and threatening to publish. On all sites, if they do not pay, all with the intent of defamation, threats, and blackmail. By Article (430) of the Penal Code, legal measures were taken against the accused and referred to the competent court.

Blackmail is not limited to sending intimate photos or files. Sometimes, a person himself may make a mistake when he sells his devices to online stores. The danger here is that some shopkeepers have a criminal tendency to retrieve files, such as personal photos or documents, from electronic devices. After recovering the photos, the blackmailer starts communicating with the women on these devices and blackmailing them. As is usual with this crime, fear and terror are instilled in the victim, probably to fulfill his demands for money. In this case, the victim was with her husband when she sold her mobile device. A few days later, the victim was threatened and blackmailed for days, subjected to significant psychological trauma and the collapse of her marriage. After investigation and investigation by the competent authorities, he was arrested and transferred to the RusafaCourt of Appeal under Threat Article 430 of the Penal Code No. 111 of 1969[15].

The defendant, who pretended to be a minor boy on a chat site, asked an underaged girl to take off her shirt. Unbeknownst to the victim, the defendant recorded the act and then threatened to publish the recording on the Internet, causing the victim to fear her life. The accused concealed his identity, obtained nude photos and videos,and used malware and other computer tools to operate the victim's webcam without her consent remotely. The perpetrator threatened to publicly post the hacked pictures or videos on the victim's social media account unless the latter sent him more nude photos or videos[16].After a while, he was arrested and referred to investigation and then accused of violating women's privacy and blackmailing him under Articles 452 and 430 of the Iraqi Penal Code No. 111 of 1969. These are the punishments for threatening crimes in the Iraqi Penal Code, which also apply to cyber-blackmail criminals. However, is proving cyber-blackmail so easy that the Penal Code texts suffice for him?

Certainly not; most culprits are highly trained in technical areas, fully aware of them and how to cope with them, and catching them is never easy. Rather than that, the majority have learned how to hack an account by creating a fictitious Facebook page and uploading images or videos of the victims. Then blackmailer them. If only those rules were effective in deterring criminals, Iraq would not have ranked second in the Arab world for cyber-blackmail crimes, and it would not have spread in this manner[17]. Therefore, these laws alone could not protect the victims of blackmail in Iraq, especially with the development taking place now. In addition to that, the laws of the crime of threat mentioned above look at the corruption of

[15] Case No. 3800/C/2020 in the Iraqi Court of Appeal specializing in criminal offenses, and it was tried according to Article.

[16] See e.g., Criminal Complaint, United States (2017) Case No. 6:17-mj-1361 (M.D. Fla.), 4 April at 4.

[17] The questionnaire was published by the Community Police in Iraq under the title Electronic Extortion in Iraq... Women's Tales that End in Murder and Scandal. https://al-ain.com/article/cyber-blackmail-iraq-crimes. Last visit 16 April 2022.

blackmail as a crime of threat only. It is considered one of the serious flaws that the Iraqi legislator claims to take serious steps to address this legislative void. These traditional legislations also did not keep pace with the complex electronic crime technology, so the Iraqi legislator must enact and legislate a special law separate from the penal code, for information crime of all kinds, as in many Arab countries now, which realized early on the seriousness of these crimes, and quickly enacted and legislated laws Specialized in cybercrime to eliminate and combat it, and I see that a country the size of Iraq is no less than other countries, to take such an important step, so we appeal to the Iraqi legislator to enact such a law, to protect Iraqi society from the dangers of this crime that has exhausted it severely Recently.

Number of Cases of Cyber Blackmail in Iraq

Year of the case	Total Population	Internet Population	Number of Cases Reported
2006	29,034,096	4,800,000	303
2007	29,216,107	6,260,000	953
2008	29,405,568	7,820,000	2258
2009	29,520,776	8,230,000	6858
2010	29,604,550	8,800,000	10853
2011	29,689,122	9,160,000	13003[18]

Blackmail Risks and Consequences

Following are the consequences and risks associated with Blackmailing:

Social Dangers

The propagation of this crime is a breach of civil peace because it poses a risk and hazard to the individual and his family and thus to society. The number of young men and women hesitant to marry has increased due to the secrets that blackmailers may divulge to the organization. Injustice and tyranny have also become more prevalent due to the victims' remaining under the blackmailers' power.

Psychological Risks

These risks manifest themselves in the victim's psychological problems, anxiety, dread, and depression, which contribute to a troubled and unhappy personality and may contribute to a high rate of suicide. Bear the grave penalties that may arise from the offender's exorbitant content.

Threats to Security

This increases the degree of crime of all types: theft, murder, and others because the blackmailer typically demands large quantities of money to coerce individuals into stealing money they do not have, and robbery, of course, can result in murder and other crimes in some circumstances[19].

Community Awareness

Parents must assist their children and adolescents in using technology safely. They should maintain a balanced perspective and be aware of the Internet's numerous benefits. While parents may focus on the educational benefits of the countless beneficial skills acquired online, they must acknowledge and value the social benefits children might gain—playing and exploring personal interests can be significant motivators for children's Internet use. Understanding these issues may

[18] Sattar Aboud, "An Overview of Cybercrime in Iraq," *", The Research Bulletin of Jordan ACM- ISWSA (IJJ)* Volume II (January 1, 2012): 31–34.

[19] Cyber One Company, the most important causes of electronic blackmail, and how to get rid of the blackmailer, https://cyberone.co/the most important-reasons-of-electronic-extortion/. May 2021.

help parents cope with and support their children more effectively. Parents, caregivers, and guardians should be aware of the following to ensure that children and young people use the websites safely and appropriately[20]:

Recognize the dangers and opportunities their children and adolescents may face while using the Internet. They must recognize potential concerns for their children and consider that the risks may be harmless.

Involvement in their children's online activities, including the type of content they see, transmit, or generate, the services, platforms, and games they use, and the people they connect with. It is always beneficial for parents to experiment with their children's services.

Parents should discover educational and entertaining websites and activities that they can share with their children. A good website or game will have a dedicated safety page with links, transparent reporting systems, and guidance for children, adolescents, and parents and caregivers.

Maintain a consistent, candid, and open discussion with children and adolescents that is age-appropriate and evolves through time.

It is prudent to exercise caution when utilizing mobile devices, mainly when filming ladies, as the equipment may be lost or stolen by abusers. Users should be reminded not to leave their phone's memory card in while it is being serviced since certain employees at these locations may exploit the images and use the program to recover erased content. Additionally, films and publications imported from other countries and movies that promote criminal behavior should be strictly regulated.

In the event of blackmail, one should communicate with the appropriate authorities. It is necessary to be candid with the parents when informing them about the situation to confront the blackmailer and refrain from communicating with him under any threat to hold him legally accountable.

Through the use of information and communication technology, schools have the chance to revolutionize the educational process and assist students in realizing their potential and raising their level. However, children must understand how to stay safe when interacting with these new technologies, particularly the more collaborative ones such as social media platforms and services, which are critical components of productive and creative social learning. It is now easier for children and adolescents to create and distribute their material via social media sites, the majority of which also support live streaming[21].

By examining several studies on this subject, we identified several types of cyber theft likely to result in cyber blackmail.

Identity theft is one type of cyber theft. It is a type of cybercrime prevalent on Facebook. A hacker obtains information about a person's profile from the Internet and uses it for inappropriate or illegal purposes. Due to the vast number of Facebook users, it has become straightforward to access and steal individuals' identities and use them to create bogus profiles, creating an atmosphere of insecurity. According to a study conducted in Saudi Arabia, cyber blackmail is a significant

[20] International Telecommunication Union Development Sector, Guidelines for Parents and Educators on Protecting Children on the Internet, Place des Nations CH-1211 Geneva 20 Switzerland. 2020

[21] International Telecommunication Union Development Sector, Guidelines for Parents and Educators on Protecting Children on the Internet, Place des Nations CH-1211 Geneva 20 Switzerland. 2020

issue because it is associated with privacy violations.

Iraq's government has taken appropriate measures to combat cyber blackmail. It has established free hotlines (533 and 131) to follow up on blackmail cases and explain all the circumstances surrounding the topic to the appropriate authorities to prevent blackmailers and educate all members of society about these critical issues.

Preventive Measures

There are several tactics and techniques that individuals, particularly women, can use to protect themselves from the risks of social media, the most serious and dangerous of which is cyber blackmail.

Developing international rules that impose severe punishments on cybercrime culprits as governmental and global engagement is necessary, given the gravity of the situation.

Notify security authorities immediately if they are subject to cyber blackmail.

Using social media privacy settings to protect your info from hackers and vulnerable individuals.

Never divulge your password, update it frequently, and use complex passwords. Avoid storing images of other people on social media platforms and PCs.

Avoid posting private and personal information, such as news, images, or video clips, particularly those of family members.

Exercise caution and do not believe all advertisements; instead, verify their legitimacy using well-known search engines.

Continue to monitor children and attempt to save them and intervene at the proper time, mainly if they exhibit suspicious signs like anxiety or dread.

Recommendations

Raising the social awareness of vulnerable populations, particularly females, to protect them from the hazards of technological blackmail. This is accomplished by providing additional support, encouraging them to be candid, and facilitating family discourse by hosting seminars and conferences aimed at educating families on this subject.

Family members should use social media appropriately and refrain from uploading and sharing intimate images on Facebook, Instagram, WhatsApp, and other platforms due to their negative social and security implications.

Strengthening family ties and preventing family disintegration through continuous monitoring of children, especially during critical stages of their lives, and avoiding a chaotic drift behind globalization, which contributes to the destruction of the family entity and the loss of children, particularly girls. Activating the community police and distributing toll-free numbers throughout the state's institutions and satellite channelsis accomplished in collaboration with the Ministry of the Interior, Communications, and other appropriate government agencies.

Conducting seminars and workshops in schools in collaboration with school administration, a representative from the Ministry of the Interior, and professionals in electronic technology and communication to raise awareness about the hazards of electronic blackmail.

Do not keep any bank accounts, personal or family photos, or confidential information on any statement, whether on computers or mobile phones, as all these devices are connected, and blackmailers can hack them, making this a hazardous issue.

Adopt and enforce cybercrime legislation scientifically and legislatively, considering the

type of crime committed and its repercussions. This is accomplished through collaboration between the Ministries of Justice and the Interior.

Increasing the activation of international cooperation mechanisms by signing agreements with nations that prosecute this type of crime creates a protective network for the state on both the local and worldwide levels.

Notify the appropriate authorities if you are a victim of electronic blackmail via the numbers provided by the security authorities.

By bringing attention to the issue of cyber blackmail via official satellite channels and establishing confidence and collaboration between citizens and security services.

Conclusion

The increasing reliance on computers to access the Internet has exposed many Iraqis to extortion, especially women. Thus although legislators have taken some initial steps to address this problem, they seem insufficient when it comes to this type of electronic extortion. As a result, Iraqi lawmakers should consider revisions rather than relying on existing laws. This study conducted an in-depth analysis of the phenomenon of cyber blackmail. The article contributes to a better understanding of the topic by discussing the threat of cyber blackmail and the most crucial lawsuit side, such as intent and the real danger in the crime of cyber blackmail. In addition to analyzing some cases against women and knowing the extent to which the current Iraqi law deals with this crime, the reasons for its spread in Iraqi society, and how the Iraqi legal systems deal with it and issue judgments. The study also showed that such contacts, particularly in their extreme forms, can have dire consequences, including placing women in a constant state of fear and pressure, leading to significant psychological harm or general trauma, disrupting people's daily activities, and endangering people's daily activities. Public interest at risk.

The study explained that the risks and consequences of cyber-extortion against women, especially in its extreme forms, can have serious consequences, such as putting victims under the blackmailer's control. The study also highlighted the importance of awareness in Iraqi society of the crime of extortion to avoid women such this dangerous phenomenon. The article explained that the risks and consequences of cyber-blackmail against women, especially in its extreme forms, can have serious consequences, such as putting victims under the blackmailer's control. The study also highlighted the importance of awareness in Iraqi society of the crime of blackmail to avoid women such this dangerous phenomenon. Although this article only analyzed cases in Iraq, the findings could be of interest to a global audience. The results of this article can be used to develop educational materials for law enforcement training programs and law school clinics to develop fact analysis and counseling skills for clients.

References

1. Vasiu, I., &Vasiu, L. (2020). Cyber Extortion and Threats: Analysis of the United States Case Law. *Masaryk University Journal of Law and Technology*, *14*(1), 3-28.
2. Abdulhameed, R. S. (2021). Crimes Of Threats and Cyber Extortion Through social media: A Comparative Study. *Review of International Geographical Education Online*, *11*(12), 1022-1033.
3. Colonel Dr. / Ahmed Nahi Attia Colonel Dr. Ziyad Muhareb Muhammad Colonel / Ahmed Hashem Rady Colonel / Jamal Walid, Mr.

Yusef Abadi Muhammad, Editor-in-Chief General Dr. Saad Maan Al-Mousawi, 2019, Electronic Extortion Modern Crime, Ministry of Interior, Directorate of Relations and Information.

4. Uma, S. (2017). Outlawing cyber crimes against women in India. *Bharati Law Review*, *5*(4), 103-116.
5. SuadAlisawee, The Crime of Cyber Extortion (A Comparative Study), University of Al-Qadisiyah, November 2019.
6. Kareem, H. A. M. A. (2021). The social risks of electronic extortion. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(4), 8263-8273.
7. Kumar, S. (2022). A quest for sustainium (sustainability Premium): review of sustainable bonds. Academy of Accounting and Financial Studies Journal, Vol. 26, no.2, pp. 1-18
8. Case No. 1080/C/2021 in the Iraqi Court of Appeal specializing in criminal offenses, and it was tried according to Article 431.
9. Case No. 1588/C/2021 in the Iraqi Court of Appeal specializing in criminal offenses, and it was tried according to Article 431 and 432.
10. See e.g., Criminal Complaint, United States (2017) Case No. 6:17-mj-1361 (M.D. Fla.), 4 April at 4.
11. Bhardwaj, A. (2017). Ransomware: A rising threat of new age digital extortion. In *Online banking security measures and data protection* (pp. 189-221). IGI Global.
12. Cyber One Company, the most important causes of electronic blackmail, and how to get rid of the blackmailer, https://cyberone.co/the most important-reasons-of-electronic-extortion/. May 2021.
13. International Telecommunication Union Development Sector, Guidelines for Parents and Educators on Protecting Children on the Internet, Place des Nations CH-1211 Geneva 20 Switzerland. 2020.
14. The questionnaire was published by the Community Police in Iraq under the title Electronic Extortion in Iraq... Women's Tales that End in Murder and Scandal. https://al-ain.com/article/cyber-blackmail-iraq-crimes. Last visit 16 April 2022.
15. Threat, blackmail and defamation.. Cybercrime is expanding in Iraq and women are its victims, Al Jazeera Net, https://www.aljazeera.net/news/women/2020/9/28/أبرزها-الخيانة-الزوجية-الجرائم. Last visit 15 April 2022.