SAM
Rights & Liberties

ONLINE EXTORTION IN YEMEN ..

The Phenomenon and Solution

نوفمبر 2022

www.samrl.org

SAM
Rights & Liberties

Digital Rights Project

A non-profit human rights window affiliated with SAM Organization, with the support of Internews, aims to introduce digital rights and monitor digital violations against users of the digital space, as it works to advocate for the digital rights of Yemenis, with the aim of reaching a safe, fair and free digital space. The window allows reporting digital violations, documenting them and creating a database about them. She publishes studies and research on digital activism, digital rights and digital security, in addition to planning and managing local and international advocacy campaigns.

violations@samrl.org

ONLINE EXTORTION IN YEMEN ..

The Phenomenon and Solution

SAM
Rights & Liberties

Introduction

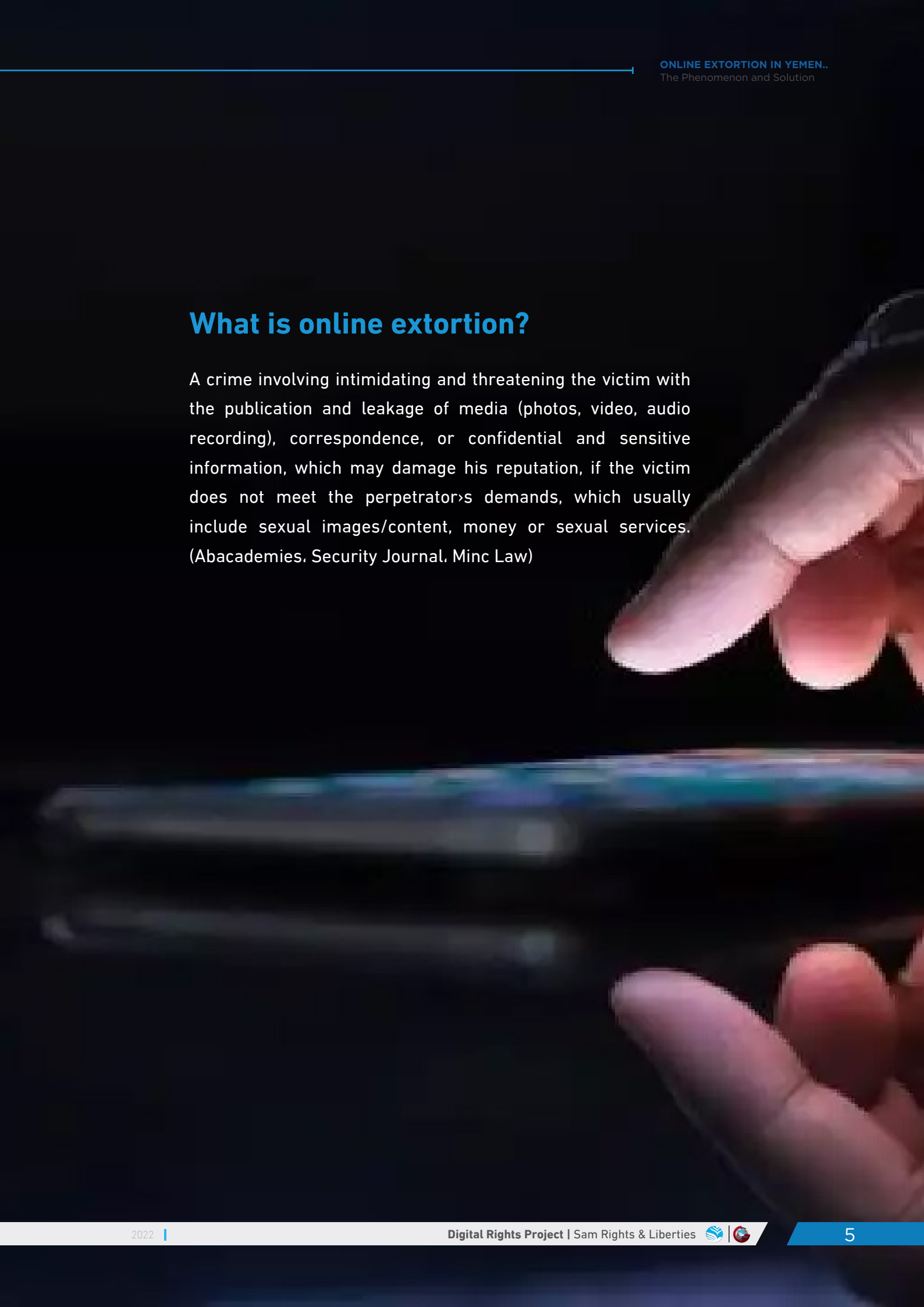
Social media platforms have witnessed a significant increase in the number of users in Yemen, with 3.50 million subscribers, equivalent to 11.4% of the total population, and unfortunately, a large percentage of these users lack digital awareness, which exposes them to the risks of misuse, such as exposure to online extortion, which has become a terrifying and dangerous phenomenon.

In addition to the lack of digital awareness among the user, a number of individual, social, and legal factors have combined to lead to the spread of the phenomenon of online extortion and compounded its repercussions. The methods and ways in which individuals fall into the trap of extortion vary, and what is terrifying is that making a mistake may seem simple, but it can trap the victim in an unacceptable maze.

It can be said that the government/institutional role in combating online extortion is absent and at best ineffective, which prompted digital security activists to fill the vacuum and play a remarkable and positive role in addressing this abhorrent phenomenon.

The consequences of online extortion and defamation do not stop at the victim›s feeling of anxiety, depression and psychological pressure, but go beyond that to resort to suicide, and may push the victim›s family to get rid of her by killing her, based on sick societal calculations and accusations that are completely unjustified, which we have unfortunately monitored and mentioned in this report.

We tried to provide a modest glimpse into the reality of online extortion in Yemen, and the tragedies and unfortunate stories of girls who in most cases had no guilt other than that they fell into the trap of unscrupulous people, with the help of a society that has long criminalized the victim and exonerated the perpetrator.



What is online extortion?

A crime involving intimidating and threatening the victim with the publication and leakage of media (photos, video, audio recording), correspondence, or confidential and sensitive information, which may damage his reputation, if the victim does not meet the perpetrator›s demands, which usually include sexual images/content, money or sexual services. (Abacademies، Security Journal، Minc Law)

Legal context. Texts and effectiveness

Yemen lacks a law on combating cybercrime, which puts law enforcement authorities in front of a challenge when dealing with cases of online extortion, and therefore the legislator is forced to adapt the provisions of the (general) Penal Code and drop it on this type of case, with its shortcomings and lack of keeping pace with developments, not to mention that the current legal texts do not approve deterrent penalties against the offender.

There are provisions in the Penal Code regarding extortion and the violation of the sanctity of private life, in a general form, as Article (254) stipulates the following:

Whoever threatens another by any means to commit a crime, a harmful act or an act committed against him or his spouse or a relative up to the fourth degree shall be punished by imprisonment for a term not exceeding one year or a fine if the threat is likely to cause panic among the person who signed it.

Article 256 adds: Anyone who violates the sanctity of private life by committing one of the following acts in cases other than those authorized by law or without the consent of the victim shall be punished by imprisonment for a term not exceeding one year or by a fine:

- Listen, record or transmit by means of any device of any kind conversations that took place in a private place or by telephone;
- Take or transmit with any device of any kind a picture of a person in a private place.

In all cases, the confiscation of devices and other items that may have been used in the crime shall be adjudicated, as well as the erasure or execution of the recordings obtained thereon.

Article 257 states: Whoever broadcasts, facilitates a broadcast, or uses, even if it is not public, a recording or document obtained by one of the methods

set forth in the preceding article, or without the consent of the person concerned, shall be punished by imprisonment for a period not exceeding two years or a fine. A public official who commits one of the acts set forth in this article shall be punished by imprisonment for a term not exceeding five years depending on the authority of his office.

In all cases, confiscation of devices and other items that may have been used in or obtained from the crime shall be adjudicated, as well as the erasure or execution of the recordings obtained from the crime.

Article 313 on extortion also stipulates the following: Whoever intentionally sends in the soul of a person the fear of harming him or any other person of interest to him and induces him to do so with bad intention to hand over to him or to any other person any money, legal document or anything signed by a signature or seal that can be converted into a legal document, shall be punished by imprisonment for a term not exceeding five years or a fine.

«Yemeni laws are seen as lagging behind and not keeping pace with many cases and crimes, including cyber extortion crimes, which emerged with the technological revolution that the world has witnessed. This has opened the door to calls and demands for the modernization and development of these legislations and laws, like other Arab countries. In view of the serious societal effects caused by the crime of electronic extortion, Diaa Muhairez, a former judge and professor at the Faculty of Law at the University of Aden, believes that «the Yemeni legislator should have singled out a legal text related to this crime, and increased the punishment.» South 24 February 2022.

The phenomenon of online extortion in Yemen

In an interview with the Digital Rights Project, Reham Al-Asbahi, digital safety officer at ODET, said that the phenomenon of online extortion in Yemen is increasing due to digital illiteracy, which is the most prominent cause of extortion, and it turns out that the victim›s ignorance of the simplest digital protection tools exposes her to the withdrawal of the largest amount of personal information, which is ultimately used by the blackmailer against her.

Mokhtar Abdel Moez, an activist in digital security and information protection, said that between 25 and 30 cases of extortion arrive daily to the team he set up with colleagues, which means (750 to 900 cases per month). Al Sharea Newspaper in September 2022.

Activist Ahmed Ghazi stated in another Facebook post (on November 2) that he receives at least ten cases of extortion per day, pointing out that there are dozens of organized gangs that work to blackmail girls, which despite revealing some of them and informing the security services, interaction is almost non-existent. Ghazi believes that the main problem lies in the mentality of a society that is not ready to characterize extortion as a crime, but rather always views the girl (who was blackmailed) as a criminal until proven innocent, and if proven, excuses exist, [to hold her responsible], he said.

In an investigation conducted by the Dekkah platform – which lasted for three months, and was published in December 2021 – more than 31 Yemeni girls from Aden and Ibb governorates were blackmailed. 50% of these girls were from Aden Governorate while the rest are distributed to the rest of the governorates, and while two of these blackmailers were from outside Yemen, 92% of them were from Yemen and through Yemeni numbers, and all these blackmailers communicated with the girls via WhatsApp. Among those girls, there were two girls from Ibb and Aden who tried to commit suicide, fearing a scandal, so that their affairs would not be exposed and their families would not know about the leaking of their photos or the blackmailer would carry out his threat and publish the photos to the public on social media.

Reasons for online extortion

Speaking about the reasons for the spread of this exploitation, Nabila Saeed, a women›s rights defender, told Anadolu Agency (April 2022) that there are many «overlapping» reasons why girls are vulnerable to online blackmail, noting that «the most obvious reason is the lack of digital literacy among young girls and the impulsive use of communication devices, which pulls them directly into the hands of blackmailers easily.» Other reasons include girls› insensitivity to sharing their personal photos or videos online, lack of control over the family, and poverty, Saeed said.

Technical expert Fahmy Al-Bahith says that the spread of «social media» in the hands of the general public without knowing the dangers of technologies in general in a society dominated by ignorance, illiteracy and poor educational outcomes, helped in the spread of the phenomenon of cybercrime and digital blackmail. He stresses that the response of some cases to blackmail requests, which usually start with small requests for fear of scandal in her social environment, and then soon develop into larger requests after the victim was unable to implement more requests.

Independent Arabia - November 2022

Activist Nour Sreib adds in an interview with the Dekkah platform (dated December 2021), «Unfortunately, most girls ignore the ABCs of protecting

their personal account, such as two-step verification and choosing a complex password, which makes using a simple hacking program and applying some codes on the Snapchat account and some applications easier to access the images stored in the Snap memory, and from it the hacker may access the email and be able to download the images stored on Google Drive if the images are in sync mode.» In a series of tweets on Twitter (November 2022), activist Sreib points out that the lack of capabilities in the field of digital security and the lack of digital criminal investigation like in other countries, in addition to the lack of demand for the extradition of criminals who are outside the country, all of this has led to an increase in extortion cases, as the criminal feels safe inside and outside the country.

In addition, social customs and the culture of shame play a major role in reviving the «electronic extortion» directed against women in Yemen, as they condemn them more than the criminals themselves, so many victims receive punishment from their families and blame from society for crimes in which they may not have a hand, and they are not spared from any harm, even if they are innocent, they are convicted anyway simply because they are women. It happens that the concept of «honor» pushes men in some areas of Yemen to kill their female relatives if they are exposed to a sex scandal, even if it comes to just leaking a picture of one of them on social media, and this excessive sensitivity in society›s view of women is what contributes to the expansion of the phenomenon of «electronic blackmail» in Yemen, according to a report issued by the Post in October 2022.

In turn, lawyer Ishraq Al-Maqtari acknowledged the increase in the spread of this phenomenon in Yemeni circles, pointing to the existence of a gap or lack of reference and clear and categorical discussion in Yemeni laws of cybercrime, and explains that most of the legislation was drafted in the nineties and there was no development on it, and most girls usually refuse to report being blackmailed, for fear of scandal, negative society›s view and other reasons. Al Arabiya Net - April 2022

How does the victim fall into the trap of blackmail?

Electronic extortion has taken on a wider dimension in light of the spread of phones, as images of women in spontaneous sessions dancing to music have been leaked, and these videos often cause blackmail campaigns against women. But the most common way represented in blackmailers talking with girls on social media and instant messaging programs, and delude them of love. The girl sends a picture of herself without a hijab, and then the series of blackmail begins to obtain other photos or push the girl to commit immoral acts. Because the girl does not feel safe and fears that her family will respond to murder, she is forced to carry out the blackmailer›s wishes and hide the blackmail and pressure she is subjected to. Al Jazeera Net - November 2022

There are networks that are very active, whose goal is to carry out extortion operations in Yemen, through the use of somewhat sophisticated programs, which can open a camera, and programs to change the sounds that delude the victim that the person he is talking to is a girl, and he is filmed in a disorderly situation, to be blackmailed by delivering the video to his family and relatives.» Al-Mushahid - November 2022

Fadi al-Aswadi, a digital security specialist, points to other ways and says that victims› data is leaked to blackmailers, including women losing their personal phones in public, sometimes reaching the hands of blackmailers, voyeur of personal photos of women from weddings through female soldiers for this act, as well as direct hacks of the phones and computers of Yemeni internet users, who do not have sufficient digital awareness to avoid the tricks of blackmail networks. Post Website - October 2022

Activist Nour Sreib stated in a series of tweets on Twitter (dated November 2022) that she came across cases of extortion in which there was dishonesty from friends, neighbors, acquaintances and co-workers, and others because of trust in some mobile repair centers and shops.

Repercussions of Online Extortion

The consequences of blackmail do not stop at the victim›s suffering from obsessive-compulsive disorder, depression, defamation, exposure to domestic violence, and other psychological and societal effects, but also to what is more serious, as there are victims who committed suicide, and others who were killed, by their families. In this context, activist Mukhtar Abdel Moez said in an interview with the Digital Rights Project that during this November, four suicides, due to extortion, were recorded in the governorates of Taiz and Hodeidah, as follows: two suicides, a suicide attempt, and a murder case, in which society was deluded that the victim committed suicide, according to his words.

On the second of November, the humanitarian activist, Sarah Alwan, shot herself, in an attempt to commit suicide, after she was blackmailed and threatened to publish her photos, which lasted for 8 months, amid the failure of the security services to her, despite revealing the identity of the blackmailer, and providing all evidence against the blackmailer, according to activists, but the security did not interact with the case, according to activists. As for how the blackmailer obtained Alwan›s photos, activist Ramez al-Maqtari said that one of the blackmailer›s relatives stole the victim›s flash drive, copied the photos, and then handed them over to the person who began to blackmail Alwan.

Less than two weeks after the incident of activist Sarah Alwan, a girl in one of the districts of Taiz governorate committed suicide by hanging after being subjected to an electronic extortion operation. Al-Shari newspaper reported on November 14 that the girl was subjected to an electronic blackmail operation by a young man named «A.G.», after a friend lost her phone memory in the village.

For his part, activist Ahmed Ghazi revealed the killing of a girl from Hodeidah Governorate, on November 17, by a gang, after being subjected to blackmail, indicating that the blackmailers wanted to practice vice with her or expose her and publish her pictures and pictures of her family, which reached them through her colleague, but she did not acquiesce to them, and ended up being killed at their hands, and pointed out that the victim›s family confirmed that the girl did not commit suicide, but was killed by blackmailers who tried to delude everyone that she committed suicide, pointing out the initial examination of the body showed signs of beatings and torture, which confirms the account of her relatives. According to him.

These incidents are just a sample of thousands of similar stories and terrible tragedies suffered by victims of electronic extortion, in a society that throws the weight of accusation and the burden of sin on its shoulders, even if all the evidence and evidence prove its innocence.

Official institutions and the absent role

The government›s role in implementing the control and control measures that are supposed to be adopted to prosecute cybercrime in Yemen is absent, due to the disintegration of the state and the multiplicity of ruling authorities in the country due to the conflict crisis. On the security front, we have found that complaints of «digital extortion» are not dealt with effectively, which applies to the areas of influence of the Yemeni government, and the areas controlled by the Houthis as well, according to a report by the website Post (dated October 2022). Mubarak al-Basha, the author of the report, added that they contacted two security sources, one in the investigations department of the Criminal Investigation Unit in Taiz governorate, which is run by the Yemeni government, and the other in the General Department for Family Protection at the Ministry of Interior of the Houthi government in Sana›a, to find out how the security authorities deal with complaints of «electronic extortion» crimes that they receive from citizens. It was found that both authorities adopt rudimentary and inconclusive measures in dealing with these problems, and even lack modern means of control specialized in curbing this type of crime.

However, activist Abdel Moez considered Taiz a good model for cooperation in this aspect, responding to reports and providing facilities to victims, as cases of exploitation of girls have recently decreased, after they were high in the past periods, he said. Regarding the interaction of the security services in the capital, Aden, with cases of extortion, he says: «In Aden, our reports are not well responded to, or with the victims,» although we have collected evidence, revealed the identity of the person and provided evidence, but they are not caught, and he explains, «The security authorities do not interact with these cases unless they are very popular on social media.» He pointed out that in the current period, the team›s reports on extortion cases in the city of Sana›a have received relative cooperation from the security services, where a number of blackmailers were arrested, while in Ibb governorate, Abdul Moez says, «Despite the large number of extortion cases in it, the security services do not arrest blackmailers and do not deal with reports submitted to them well. Al-Shari Newspaper - September 2022.

Lieutenant Colonel Osama Al-Sharabi, a spokesman for the police in Taiz Governorate, told Al-Jazeera Net, «For us we are a police service, we deal with any report that reaches us according to legal procedures, and after the seizure and completion of procedures, we refer the case file to the prosecution, but there is a tendency and orientation towards ending most cases and resolving them amicably.» Al Jazeera Net - November 2022

According to the head of the Criminal Investigation Department in the southern Yemeni city of Taiz, Major Muhammad Ba›alawi, the Mobile Phone Crimes Division in the Criminal Investigation Department tries to track the blackmailer by all available means despite the difficulties related to the response of the telecommunications companies in Sana›a, as they often reject requests to reveal the identity or locations of the owners of the chips used by the blackmailers, but we use the division›s technical team to track the blackmailers at times and track money transfers at other times. Dekkah Platform (December 2021)

The role of civil society organizations and activists

During the seminar (Digital Privacy) conducted by the Digital Rights Project last month, the head of SAM Organization Tawfiq Al-Humaidi pointed out that in the absence of a state or legislative institutions, and therefore the absence of an official role in addressing cybercrime, the available margin is what civil institutions, media outlets, and specialists in this aspect are doing today.

Civil society institutions play their role in raising awareness of the dangers of extortion and cybercrime in general, and provide advice and guidance to Internet users in Yemen, and there is coordination between some local institutions, in this aspect, in order to build capacity and form a lobby that pressures decision-makers to improve current legislation and establish new laws that keep pace with developments in the digital level. In addition, civil society organizations call for the formation of national emergency teams to respond to cybercrime and provide emergency support to victims and those affected. As for external networking, a number of local institutions participate in international conferences, such as the «Bread and Net Forum», to support and promote digital rights.

At the individual level, a voluntary initiative was established by digital security activists, including Mokhtar Abdel Moez and Fahmy al-bahith, who made tangible efforts to address electronic extortion and provide assistance to victims, starting with receiving and examining complaints, closing pages and accounts that publish victims› photos, to ousting the blackmailer, and handing over the case file to the security and judicial agencies.

Al-Shari Newspaper - September 2022 traced the march of this initiative, which began in March 2020, by Mokhtar and his companions, and includes a team of about 300 to 400 people, including specialists in social media, psychiatrists, lawyers, technicians and technicians, in addition to cooperative officers and security personnel. Despite the threats and harassment that Mokhtar and his team were subjected to by gangs and some people who blackmailed women, which amounted to the possibility of «killing and liquidation» through attempts to hack their accounts. However, the team continued to assist victims, according to a report published by Al-Shari Newspaper in September 2022.

Abdel Moez says the number of victims he and his team have contacted since the inauguration is very high. Abdel Moez estimated the number of victims that the team was able to help at more than ten thousand out of 15,000 cases that requested help. He said the team «was able to identify more than 2,000 people.» The percentage of victims that gangs managed to seduce through romantic relationships is 65 percent of the cases that reached Abdel Moez›s team. The rate of penetration of victims› accounts is 35 percent. However, he points out that account hacking cases have decreased recently due to the effectiveness of the awareness campaign on ways to secure social media accounts. previous source.

Age Groups of Victims

Adolescent girls (12-17 old) → **Girls** (18-30 years) → **Women** (30 and 40 years).

Al-Shari Newspaper in September 2022.

If legal proof is made against one of the accounts that practice extortion, then the victim can use a law enforcement team to communicate directly with Facebook to stop the account, according to digital security expert and digital rights activist Mokhtar Abdel Moez, who says, «I work with the help of a team of lawyers voluntarily to save victims in the event that the images spread on the Internet by submitting law enforcement requests to Facebook, requests are responded quickly and content is usually restricted within an hour.» Dekkah platform December 2021.

For his part, «Digital security expert Fahmy Al-bahith, one of those approved to submit reports to Facebook, says, «If I encounter violent content or I am informed of a fake account that practices any kind of violation, I will send an email to the specialized team at Facebook to report with an explanation of the reason. But the real problem, according to Eng. Nour Khaled, affiliated with YODET, one of the organizations accredited to submit reports, lies in the cultural barrier between a conservative country like Yemen and the Facebook team reviewing the reports. «We usually have difficulty convincing the team of the specificity of our culture towards the spread of images of women, and we do not find interaction or restriction measures from the team because they consider the image to be non-infringing content,» Noor said. Previous source

Solutions

Cybersecurity expert Mukhtar Abdel Moez advises girls to activate two-factor authentication for all programs and applications, and to put a difficult password and fingerprint, and prefer to use phones that do not have external memory so that if the mobile phone is lost, hackers cannot access the data. If they use external memory, it is better to encrypt it, not to save images «cloud», not to activate synchronization between e-mail, applications and photos, in addition to not opening suspicious and anonymous links, and avoid being dragged into closed rooms, video chats and sending photos, no matter how great the trust in the person. Daraj Media - December 2021

«As for Engineer Muhammad Bayazid, he recommends users to refuse to accept anonymous friendships, adopt difficult passwords, avoid chat and dating sites and suspicious applications on the digital space, deal cautiously with users of virtual worlds, avoid sending pictures and private data on communication sites, reject chat requests, and beware of visiting pornographic sites, and calls on the Yemeni family to educate its children about the dangers of indiscriminate use of digital means, urging them to adopt parental control measures on their use of the Internet, to ensure safety.» Website Post - October 2022

In addition, girls should be aware of the danger of selling devices (laptops, phones), since deleted files can be recovered, and they should be careful when performing maintenance of devices, by emptying them at least, of any personal content, so that a family member takes over the task of handing them over to a trusted engineer who is known for his integrity and honesty, while staying close to him, during the repair process.

Social activist Hadeel al-Mowafaq noted the need to «make police stations, prosecutions and courts safe places for women to report crimes against them, establish special units for women, and increase the number of women working in these facilities.» Independent Arabia - November 2022

On the importance of digital awareness, Mubarak Salmeen, a professor of sociology at the Faculty of Arts at the University of Aden, said that «society,

especially parents, must be aware that girls are the victims and the criminal is the blackmailer.» In an interview with SOUTH 24 (dated February 2022), Salmeen stressed «the importance of promoting the media to raise these files and warn of their dangers, in addition to developing programs to educate women about the danger of electronic blackmail and how to avoid falling into its trap.

The need arises for the importance of «... Issuing strict legal legislation, especially for cybercrime, so that it includes fair penalties for its perpetrators, strict control over phone sales and repair centers to prevent extortion and its causes, facilitating the procedures for reporting and dealing with these crimes (reports) seriously, and moving quickly to arrest the perpetrators as soon as reliable reports are received, in addition to educating the community about the dangers of silence on these crimes, and urging them to report them to facilitate their early control and avoid their catastrophic consequences for everyone. Manasati 30 - December 2020

During the seminar (Digital Privacy), the President of the Defense Foundation for Rights and Freedoms, lawyer Huda Al-Sarari, called for the issuance of the «Cybercrime Law», with the rehabilitation of investigators and judges and training them on how to deal with cybercrimes, accompanied by awareness that stopping the danger and addressing violations is within the limits of the law. Activist Fahmy, a researcher, adds in an intervention that laws can be used as a double-edged sword, and therefore when there are laws, they must be subject to long and in-depth discussions with stakeholders before their approval, so that there are no terms that accept interpretation and interpretation according to the mood of the judge and decision-makers. Dr. Walid al-Saggaf, a lecturer at Soderturn University in Stockholm, believes that establishing alliances and communication with other organizations and companies and trying to raise awareness of what has happened in Yemen and where blackmail is taking place, may help raise the possibility for technology companies to respond to complaints submitted in this context.

Conclusion

All the reasons and solutions mentioned in the report can be summed up and reduced to one word: (awareness), as the more aware the user is, the less he is exposed to risks, and the more aware the society, the more able he is to address the problem and remedy it, and vice versa. Noting that there are cases where the victims are people with a high level of awareness and maturity, as absolute safety in the digital space is impossible.

Changing the awareness of individuals is the first step to changing their reality, and based on this postulate, we bet on the media, civil society institutions, activists and influencers to assume this responsibility, and to address the phenomenon of electronic blackmail, which requires networking and coordination, at the local and international levels, in a way that doubles the effectiveness and efficiency of the efforts made.


SAM
Rights & Liberties

ONLINE EXTORTION IN YEMEN ..

The Phenomenon and Solution

November 2022

violations@samrl.org
www.dg.samrl.org

Digital.Rights.Yemen
@SamDigitalRight

SAM
Rights & Liberties

www.samrl.org
info@samrl.org