International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217414

Tracing of the Blackmailers in Sextortion Case and Tactics to Defend It – An Experimental Cybercrime Case Study

Sarthak Rathod[1], Madhav Gaur[2], Krishna Parihar[3], Akhlesh Kumar[4], Dr. S. K. Jain[5]

[1]Forensic Professional (FPACT PLUS), Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

[2,3]Forensic Professional (FACT), Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

[4]Assistant Director & Scientist – 'C', Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

[5]Director-cum-Chief Forensic Scientist, Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

ABSTRACT

Article Info

Volume 7, Issue 4

Page Number: 135-142

Publication Issue :

July-August-2021

Article History

Accepted : 02 July 2021

Published : 08 July 2021

Sextortion is a new form of cybercrime that is spreading very fast in India. Sextortion is such a type of incident where victims are very ashamed of sharing and talking. And that is why it becomes a very easy and suitable target for blackmailers. Innocent social media users are being trapped in Sextortion. Victims not only lose their money but also pride and respect in society especially family members and friends. The research paper has explored to understand the modus operandi of the blackmailers. The present study has attempted to trace blackmailers in a sextortion incident. The research paper has described the process of tracing the blackmailers online. The study analyzed the incident from a cybercrime detection and identification perspective. The research paper is also attempting to spread awareness by describing tactics to defend against cybercrimes such as sextortion.

Keywords : Sextortion, Cyber Crime, Cyber Forensics, Online Blackmailing, Phishing, Organized Crime, Intimate Photo/Video, Nude Video Call

I. INTRODUCTION

The world is has become digital entirely. In today's time, everyone has access to the Internet, and it should be the minimum human right that everyone holds. Nevertheless, growing internet use has resulted in crimes such as cyberbullying, phishing attacks, money laundering, ransom attacks, illicit pornography, and sextortion, among other things. Surprisingly, Sextortion is of the topmost leading cybercrimes on the internet today (Pradhan, 2021). Sextortion is made up of two words, one is being 'Sex' and another being 'Extortion'. Sextortion means providing blackmailers sexual pictures, sexual favours, or money in return for not disclosing the victim's personal and sensitive information. Sexual extortion is such a heinous and inhumane crime that thrives on victims' shame in the eyes of his family and society. Sextortion is similar to online blackmail in that the blackmailer either demands that the victim participates in sexual acts, such as posing for naked photos or masturbating in front of a camera, or demands that the victim pay a significant sum of money (Mahawar & Verma, 2021). The belief that only women are the suitable targets for sextortion is fading away slowly. Because in recent trends of sextortion witnessed that young males are being targeted by the blackmailers who are also a bunch of men only. These types of incidents have been reported globally. But, India has witnessed more cases like this.

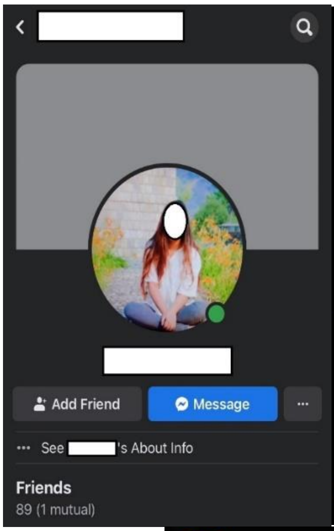
The most famous method of sextortion uses social media platforms such as Facebook and Instagram & messaging mobile apps such as WhatsApp and Telegram. Firstly, Blackmailers make fake Facebook or Instagram profiles where they use a display picture of a young girl. Then, they search the random people on the social media platform and tries to identify the potential victims. Generally, blackmailers' suitable target is a young male who would be well connected with his family and socially well-known. They identify this by simply looking at the user's social media profile personal details and images posted by him only. Blackmailers attempt to understand the cyberpsychology of the person. They even study and look for profiles of the close family members of the potential victims so that they can blackmail victims to share their personal and sensitive information with their family members and friends later on. After this primary selection process of a suitable target If they think that he could be lured easily then they will send a friend request from the fake profile. This is the first mistake that many victims made that they accept the friend request from unknown profiles. Blackmailer will start messaging immediately and after some time they will ask the victim to have a nude video call or sex on the video call. These potential victims who are generally young males, get lured easily and accept the offer. Blackmailers ask victims to give their messaging mobile app details i.e. WhatsApp so that they can have a video call. The moment victims give their WhatsApp details, Blackmailers will start the chat and asks the victims to be ready for a nude video call or sex on the video call. Then, Blackmailers and Victims have a video call where Blackmailers show a pre-recorded Pornographic video where generally the girl is undressing clothes or masturbating. Blackmailers then ask victims to participate and do the same activities on the video call. Victims are unaware that Blackmailers are recording the entire video call with a screen recording facility/software in the mobile phone. The moment victim participates in the video call is the same moment victim has been trapped already. Suddenly, Blackmailers stop the video call and sends the video clip of their videocall in WhatsApp along with the screenshots of the profiles of the family members and friends of the victim. Blackmailers threaten the victims to pay a sum of significant money or else they will share the video clip with their family members & friends and even they will upload it on the social media platforms such as Facebook, Instagram, and YouTube. The victim does not understand how to tackle the situation and to save his dignity and pride he agrees to pay the money. If victims do not agree to pay the money then Blackmailers send video clips to their family members & friends on social media platforms. Blackmailers generally give bank details, UPI ids, or sometimes share phone numbers registered with online payment mobile apps such as Paytm, Google Pay, Phone Pay, and BHIM (Bharat Interface for Money). These payment sources are generally operated on a commission basis. The account holder gets some nominal commission and the remaining amount would be transferred to Blackmailers.

This type of offense is part of organized crimes which is specifically known as ‘Racketeering’. Sextortion is a serious offense where victims lose a handsome amount of money & their pride and dignity in society. In some cases, victims may take extreme steps such as suicide. A 26-year-old aspirant working in the federal government committed suicide after becoming a victim in a sextortion case (Bengaluru News, 2021). Such cases of sextortion have been reported by PAN India and it has become a major challenge to tackle with. Cyber Cells of all the State and Central Government is working in the direction of detection of gangs who run this kind of rackets to victimize people. Many law enforcement agencies have succeeded also and arrested Blackmailers from Rajasthan, Haryana, and Uttar Pradesh (Naveen, 2021). To aware the general public about sextortion Maharashtra Police held a webinar on cybercrime awareness so that innocent people do not fall in hand so these gangs (Narayan, 2021). The government has launched many campaigns and awareness programs to spread the knowledge on this emerging crime i.e. sextortion so that crime and victimization can be prevented.

In the present study, one of the authors received a fake friend request on Facebook and started messing in the same modus operandi like used in sextortion. Therefore, the authors decided to analyze the incident by playing along with blackmailers. Authors have explored the ways to trace the location of a blackmailer in a live sextortion case. Blackmailers followed the almost same modus operandi in the incident. The authors also attempted to explain the tactics to defend similar kinds of sextortion cases.

II. Case Study and Analysis

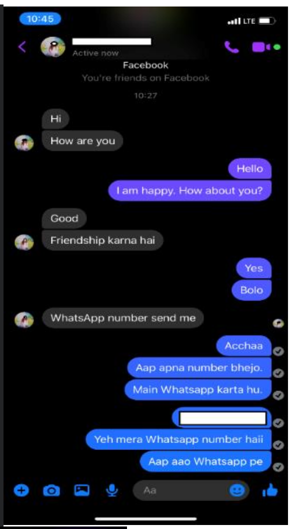
Facebook is one of the most famous social media platforms. Mr. X. is a Facebook user since 2008 and he has more than 2000 friends in his profile. Almost all his family members and friends are also active Facebook users. He works in a prestigious central government organization. Mr. X. is a young male and married. He is very well known and respected in his life and Facebook. This profile of Mr. X. makes him one of the most suitable targets and probable victims for the Blackmailers. He received a friend request on Facebook from an unknown person. Display picture of the profile was of a girl’s picture. The name of the profile was similar to the name of Mr. X.’s hometown. Being well educated and aware of the sextortion cases, he knew that profile is fake it is being used by some Blackmailers. He immediately received a message from Blackmailers. After asking ‘Hello, how are you?’ They sent a message asking that ‘do you wish to become friends?’ Mr. X doubted this conversation but replied with ‘Yes. Blackmailers asked his WhatsApp number and this was the moment, that he suspected it to be a sextortion attempt. He immediately contacted co-authors and explained the issue. The authors decide to play along with the Blackmailers and attempt to trace his location and defend his blackmail. The authors recorded everything for evidence and proceeded further with exchanging WhatsApp numbers with the Blackmailers. Screenshots of the above-mentioned trails are shown below. Faces and contact numbers are masked to protect the privacy of the persons.


[redacted]

[redacted]

··· See [redacted]'s About Info

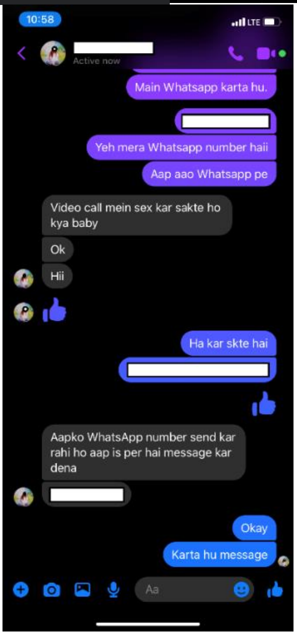
Friends
89 (1 mutual)


10:45

[redacted]
Active now

Facebook
You're friends on Facebook
10:27

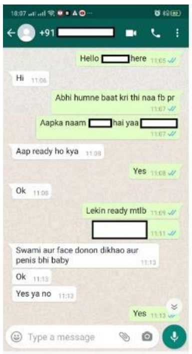
Hi
How are you
Hello
I am happy. How about you?
Good
Friendship karna hai
Yes
Bolo
WhatsApp number send me
Acchaa
Aap apna number bhejo.
Main Whatsapp karta hu.
[redacted]
Yeh mera Whatsapp number haii
Aap aao Whatsapp pe


10:58

[redacted]
Active now

Main Whatsapp karta hu.
[redacted]
Yeh mera Whatsapp number haii
Aap aao Whatsapp pe
Video call mein sex kar sakte ho kya baby
Ok
Hii
Ha kar skte hai
[redacted]
Aapko WhatsApp number send kar rahi ho aap is per hai message kar dena
[redacted]
Okay
Karta hu message

Mr. X. started the conversation with Blackmailers with the normal introduction but Blackmailers directly asked that whether Mr. X. is ready for a video call or not. They also instructed him to show face and male sex organ in the video. Mr. X. played along and answered to participate (Image – 1). Blackmailers started a video in a girl who was undressing, Mr. X. understood that it is a pre-recorded porn video clip and it is being played on a computer screen and Blackmailers are showing that in the video call (Image). Mr. X. did not switch on his face camera. So, Blackmailers ended the video call and instructed in the WhatsApp messages to get into a bathroom and show his face and male sex organs (Image – 4).

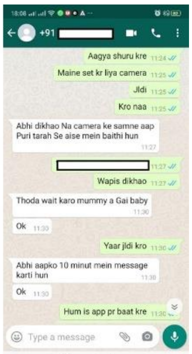

18:07

+91 [redacted]

Hello [redacted] here 11:05
Hi 11:06
Abhi humne baat kri thi naa fb pr 11:07
Aapka naam [redacted] hai yaa [redacted] 11:07
Aap ready ho kya 11:08
Yes 11:08
Ok 11:08
Lekin ready mtlb 11:09
[redacted] 11:11
Swami aur face donon dikhao aur penis bhi baby 11:13
Ok 11:13
Yes ya no 11:13
Yes 11:13

Image - 1

Image - 2

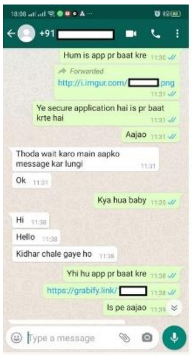

18:06

+91 [redacted]

Aagya shuru kre 11:24
Maine set kr liya camera 11:25
Jldi 11:25
Kro naa 11:25
Abhi dikhao Na camera ke samne aap Puri tarah Se aise mein baithi hun 11:27
[redacted] 11:27
Wapis dikhao 11:27
Thoda wait karo mummy a Gai baby 11:30
Ok 11:30
Yaar jldi kro 11:30
Abhi aapko 10 minut mein message karti hun 11:30
Ok 11:30
Hum is app pr baat kre 11:30

Image - 3

Mr. X. Immaterially created a link to reconnaissance and have a preliminary survey to gain information. He used an open-source website - 'Grabify'. Grabify is an IP logger website that allows its user to create a link to track the IP address of any user who clicks on it. It also provides other information such as Country, Browser, Operating System, Device name, and Internet Service Provider. Mr. X. shared the link and asked Blackmailers to click on the link to have a video call (Image – 4). Blackmailers did not click on the link and they insisted to have a video call on WhatsApp only. Before Blackmailers starts the video, Mr. X. also decided to do the same thing that they are doing. He opened a pre-recorded porn video clip on a computer screen where a boy is showing his face and male sex organ in the bathroom. And, when Blackmailers started video call he showed this clip (Image - 5). After few seconds, Blackmailers disconnected the video call and shared a video clip in the WhatsApp messages. They have recorded this video call and shared it (Image – 6).


18:08

+91 [redacted]

Hum is app pr baat kre 11:30
Forwarded
http://i.imgur.com/[redacted].png 11:31
Ye secure application hai is pr baat krte hai 11:31
Aajao 11:31
Thoda wait karo main aapko message kar lungi 11:31
Ok 11:31
Kya hua baby 11:35
Hi 11:38
Hello 11:38
Kidhar chale gaye ho 11:38
Yhi hu app pr baat kre 11:38
https://grabify.link/[redacted] 11:38
Is pe aajao 11:39

Image - 4

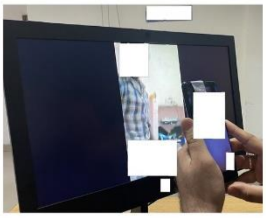
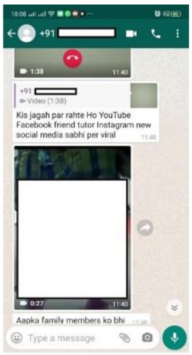


Image - 5

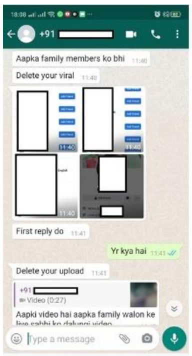

18:06

+91 [redacted]

1:38 11:40
+91 [redacted]
Video (1:38)
Kis jagah par rahte Ho YouTube Facebook friend tutor Instagram new social media sabhi per viral 11:40
0:27 11:40
Aapka family members ko bhi 11:40

Image - 6

Along with that as already mentioned above that they also study suitable target's social media profile friends and family members. So, they shared screenshots of profiles of friends and family members of Mr. X. and threatened to send this recorded video call to them and also make it viral on social media platforms (image – 7). Then, Blackmailers asked Mr. X. that whether he wants them to delete the video or not. He answered to delete the video clip. Blackmailers directly asked to give money to delete the video clip (Image - 8). When Mr. X. asked how much money? Then they replied Twenty-One Thousand Rupees (INR 21,000/-). He replied that amount is big and he cannot pay so they replied that whatever money he can give is fine (Image – 9).


+91 [redacted]

Aapka family members ko bhi 11:40

Delete your viral 11:40

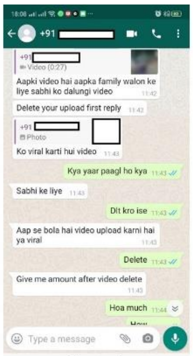
First reply do 11:41

Yr kya hai 11:41

Delete your upload 11:41

+91 [redacted]
Video (0:27)
Aapki video hai aapka family walon ke

Image - 7


+91 [redacted]

+91 [redacted]
Video (0:27)
Aapki video hai aapka family walon ke liye sabhi ko dalungi video 11:42

Delete your upload first reply 11:42

+91 [redacted]
Photo
Ko viral karti hui video 11:43

Kya yaar paagl ho kya 11:43

Sabhi ke liye 11:43

Dlt kro ise 11:43

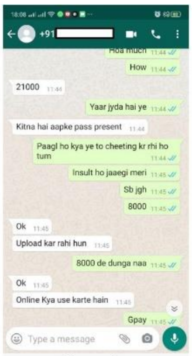
Aap se bola hai video upload karni hai ya viral 11:43

Delete 11:43

Give me amount after video delete 11:43

Hoa much 11:44

Image - 8


+91 [redacted]

Hoa much 11:44

How 11:44

21000 11:44

Yaar jyda hai ye 11:44

Kitna hai aapke pass present 11:44

Paagl ho kya ye to cheeting kr rhi ho tum 11:44

Insult ho jaaegi meri 11:45

Sb jgh 11:45

8000 11:45

Ok 11:45

Upload kar rahi hun 11:45

8000 de dunga naa 11:45

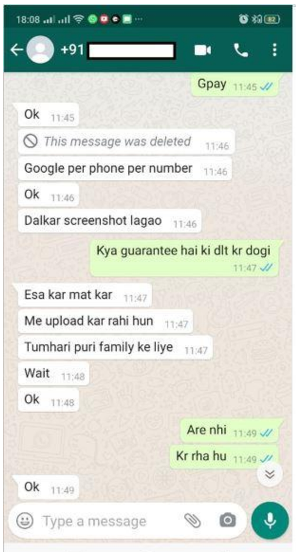
Ok 11:45

Online Kya use karte hain 11:45

Gpay 11:45

Image - 9

Blackmailers gave a phone number and instructed to deposit money through an online payment mobile application named Google Pay. They also asked to share the screenshot of the successful payment transfer. And if Mr. X. is unable to pay the money then they will share the video clip with his family members (Image – 11). Mr. X. decided to fool them and trapped them to click on the Grabify link. So, with a plan of a screenshot of fake money transfer. So, he shared a screenshot of a successful money transfer of Eight Thousand Rupees (INR 8,000/-). Along with that He shared the Grabify link and instructed them to check the successful payment in the link (Image – 14).


+91 [redacted]

Gpay 11:45

Ok 11:45

This message was deleted 11:46

Google per phone per number 11:46

Ok 11:46

Dalkar screenshot lagao 11:46

Kya guarantee hai ki dlt kr dogi 11:47

Esa kar mat kar 11:47

Me upload kar rahi hun 11:47

Tumhari puri family ke liye 11:47

Wait 11:48

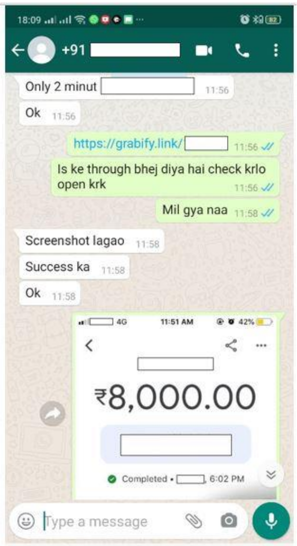
Ok 11:48

Are nhi 11:49

Kr rha hu 11:49

Ok 11:49

Image - 10


+91 [redacted]

Only 2 minut [redacted] 11:56

Ok 11:56

https://grabify.link/[redacted] 11:56

Is ke through bhej diya hai check krlo open krk 11:56

Mil gya naa 11:58

Screenshot lagao 11:58

Success ka 11:58

Ok 11:58

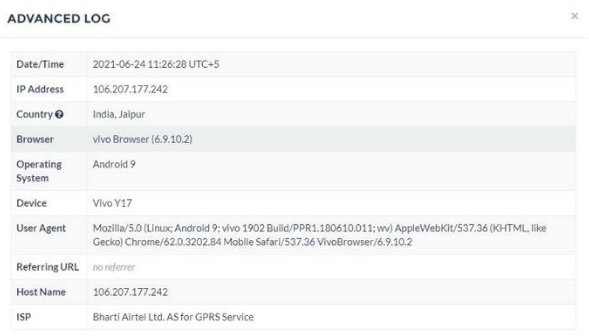
11:51 AM

₹8,000.00

Completed • [redacted] 6:02 PM

Image - 11

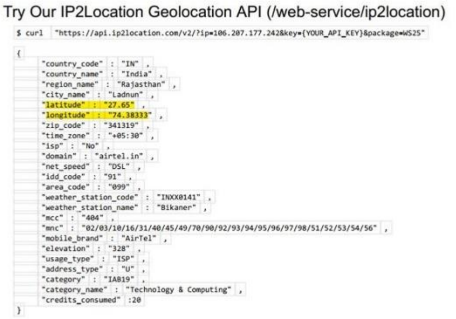
This time fortunate for authors and unfortunate for Blackmailers, they did click on the link. Mr. X. immediately got the Blackmailer's IP Address, Country, Browser, Operating System, Device name, and Internet Service Provider information (Image - 12). After getting their IP Address, Mr. X. used another website named 'IP2location'. This website helps in identifying geographical location by IP address. IP2location provided the geographical coordinates (longitude and latitude) of the Blackmailers by their IP address got from Grabify. It also provided the information of the city and state of the IP address users in India (Image - 13). And, in the final stage, the Authors put the geographical coordinates in Google Maps and reached the nearest location to the Blackmailers (Image - 14).



ADVANCED LOG

Date/Time	2021-06-24 11:26:28 UTC+5
IP Address	106.207.177.242
Country	India, Jaipur
Browser	vivo Browser (6.9.10.2)
Operating System	Android 9
Device	Vivo Y17
User Agent	Mozilla/5.0 (Linux; Android 9; vivo 1902 Build/PPR1.180610.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.84 Mobile Safari/537.36 VivoBrowser/6.9.10.2
Referring URL	*no referrer*
Host Name	106.207.177.242
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image - 12



Try Our IP2Location Geolocation API (/web-service/ip2location)

```
$ curl  "https://api.ip2location.com/v2/?ip=106.207.177.242&key={YOUR_API_KEY}&package=WS25"

{
    "country_code" : "IN" ,
    "country_name" : "India" ,
    "region_name" : "Rajasthan" ,
    "city_name" : "Ladnun" ,
    "latitude" : "27.65" ,
    "longitude" : "74.38333" ,
    "zip_code" : "341319" ,
    "time_zone" : "+05:30" ,
    "isp" : "No" ,
    "domain" : "airtel.in" ,
    "net_speed" : "DSL" ,
    "idd_code" : "91" ,
    "area_code" : "099" ,
    "weather_station_code" : "INXX0141" ,
    "weather_station_name" : "Bikaner" ,
    "mcc" : "404" ,
    "mnc" : "02/03/10/16/31/40/45/49/70/90/92/93/94/95/96/97/98/51/52/53/54/56" ,
    "mobile_brand" : "AirTel" ,
    "elevation" : "328" ,
    "usage_type" : "ISP" ,
    "address_type" : "U" ,
    "category" : "IAB19" ,
    "category_name" : "Technology & Computing" ,
    "credits_consumed" :20
}
```

Image - 13

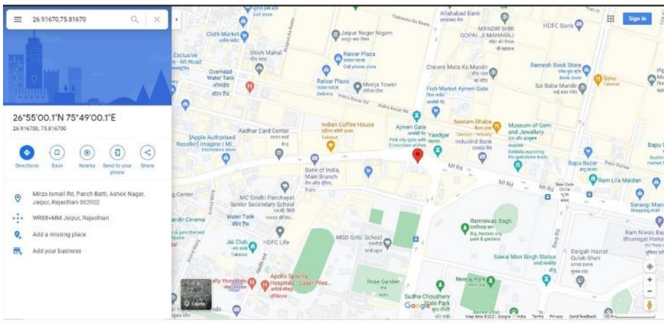
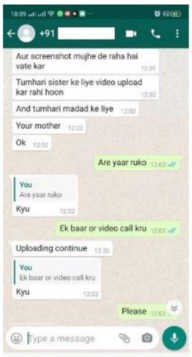


Image - 14

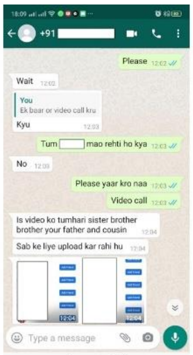
While authors were tracing Blackmailers' location, they continued to share screenshots of Mr. X.'s family members and threatened to share the video clip with them (Image – 15). Authors started confronting Blackmailers by asking whether they live in the Ladnun Village of Jaipur City in Rajasthan (Image – 16). After spending time and energy, Blackmailers did not get money and since they were already on the fake profile they went ahead and they shared the video clip with Mr. X.'s wife and close family members (Image – 17).



+91 [redacted]

Aur screenshot mujhe de raha hai vate kar 12:01
Tumhari sister ke liye video upload kar rahi hoon 12:02
And tumhari madad ke liye 12:02
Your mother 12:02
Ok 12:02
Are yaar ruko 12:02
You
Are yaar ruko
Kyu 12:02
Ek baar or video call kru 12:02
Uploading continue 12:02
You
Ek baar or video call kru
Kyu 12:02
Please 12:02

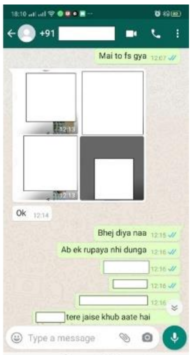
Image - 15



+91 [redacted]

Please 12:02
Wait 12:02
You
Ek baar or video call kru
Kyu 12:03
Tum [redacted] mao rehti ho kya 12:03
No 12:03
Please yaar kro naa 12:03
Video call 12:03
Is video ko tumhari sister brother brother your father and cousin 12:04
Sab ke liye upload kar rahi hu 12:04

Image - 16

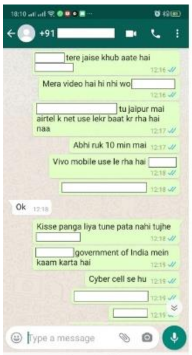


+91 [redacted]

Mai to fs gya 12:07
Ok 12:14
Bhej diya naa 12:15
Ab ek rupaya nhi dunga 12:16
[redacted] 12:16
[redacted] 12:16
[redacted] 12:16
[redacted] tere jaise khub aate hai

Image - 17

Authors confronted more and informed Blackmailers that authors are aware of this kind of scam and there is no point in threatening Mr. X. and demanding money (Images – 18). But, the story does not end here, Blackmailers were still demanding money or else threatening to post the video clip on a social media platforms 'YouTube' and they even shared screenshots as if they are posting the video clip on YouTube (Image – 19). When nothing worked out for them, they further tried to evoke emotions by saying that Mother, Father, and Sister of Mr. X. would be watching this video and it would be a shame for him. Mr. X. informed that Blackmailer that he is aware that they have shown a pre-recorded porn video clip and he has also done the same thing. So, in a nutshell, the recording of the videocall is nothing but another porn video clip (Image – 20). Blackmailers started deleting all the messages and videoclips that they have shared with Mr. X. and his family members on Facebook. They deactivated the fake profile also. Therefore, Mr. X. blocked Blackmailer's WhatsApp number before he deletes all the messages, screenshots, and videos from the chat. Since those were the very important pieces of evidence.



18:10

+91 [redacted]

[redacted] tere jaise khub aate hai [redacted] 12:16

Mera video hai hi nhi wo [redacted] 12:16

[redacted] tu jaipur mai airtel k net use lekr baat kr rha hai naa 12:17

Abhi ruk 10 min mai 12:17

Vivo mobile use le rha hai [redacted] 12:18

[redacted] 12:18

Ok 12:18

Kisse panga liya tune pata nahi tujhe [redacted] 12:18

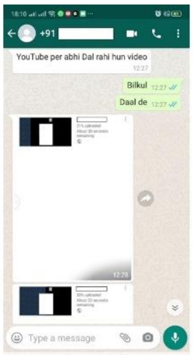
[redacted] government of India mein kaam karta hai 12:19

Cyber cell se hu 12:19

[redacted] 12:19

[redacted] 12:19

Image - 18



18:10

+91 [redacted]

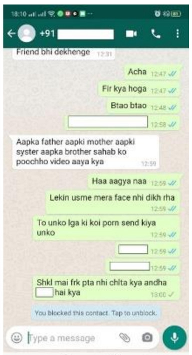
YouTube per abhi Dal rahi hun video 12:27

Bilkul 12:27

Daal de 12:27

12:28

Image - 19



18:10

+91 [redacted]

Friend bhi dekhenge 12:31

Acha 12:47

Fir kya hoga 12:47

Btao btao 12:48

[redacted] 12:58

Aapka father aapki mother aapki syster aapka brother sahab ko poochho video aaya kya 12:59

Haa aagya naa 12:59

Lekin usme mera face nhi dikh rha 12:59

To unko lga ki koi porn send kiya unko 12:59

[redacted] 12:59

[redacted] 12:59

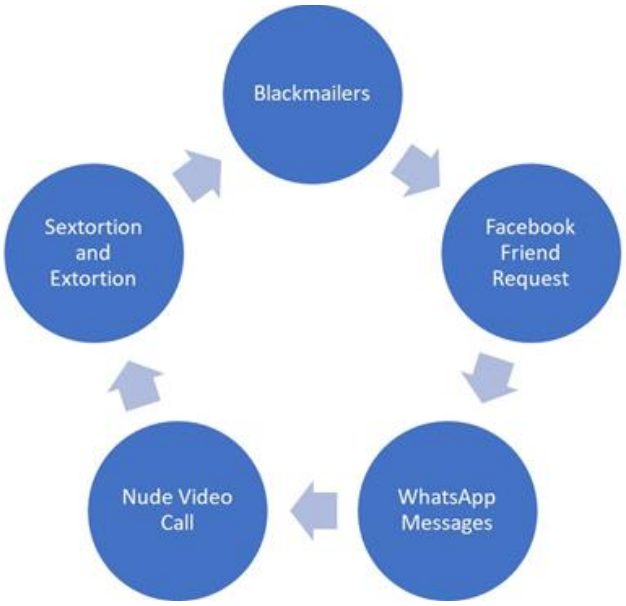
Shkl mai frk pta nhi chlta kya andha [redacted] hai kya 13:00

You blocked this contact. Tap to unblock.

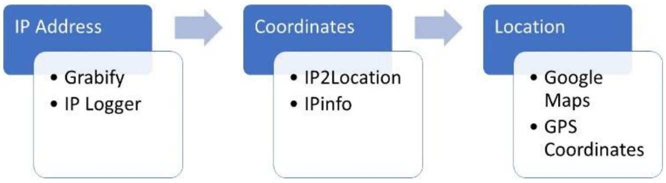
Image - 20

III. Conclusion and Tactics to defend Sextortion

Cybercrimes are growing with the growing number of internet users. And hence, new forms of cybercrimes are also growing. Sextortion has become the most hit cybercrimes in recent times in India. After the analysis of the above-mentioned case, The research paper is presenting the modus operandi of the blackmailers in sextortion cases. This can be understood by the graphical presentation shown below.



This cycle of sextortion and extortion can be broken by spreading awareness about social media platforms and cybercrimes. Internet users are using these platforms without the awareness of their advantages and disadvantages. The government has set up the cyber cell and cyber police stations across the nation to deal with the issues. But crime prevention is better than detection. Social media users should report these types of fake profiles to the social media company. Victims should complain about their victimization to the concerned law enforcement agency. One of the simple methods of tracing the location is used in the present study. It can help law enforcement agencies to trace the blackmailers. The graphical presentation is shown below for easy understating (Hendrickson, 2019).



There are many social media platforms, especially Instagram where cyber pornography is offered. There many profiles which seems to be a girl's profile, where user can pay money and in return, they can have a nude video call. But actually, this is also a scam because these profiles are generally fake profiles used by blackmailers. They use the same modus operandi of sextortion. Social media users should know their do's and don't. following tactics can save them from crime and victimization of such crimes (Cyber Suraksha, 2021).

1. Do not accept a friend request from an unknown person.
2. Unknown numbers should not be accepted as video calls.
3. Never pose naked, and never post intimate photos over online video calls or social networking sites.
4. Refrain from clicking on intimate/semi-nude photos/videos on your phone, which could create embarrassment if they are leaked.
5. Immediately report sextortion to the nearest police station or dial 100, or on cybercrime.gov.in.

To report any such profiles, use the "Report User" feature on social networking platforms.

IV. REFERENCES

[1]. Bengaluru News. (2021, June 24). Bengaluru IAS aspirant suicide: Two accused released on bail go off police radar. Retrieved July 01, 2021, from www.timesnownews.com: https://www.timesnownews.com/bengaluru/article/duo-held-in-sextortion-case-violates-bail-conditions-in-bengaluru/775349

[2]. Cyber Suraksha. (2021, February 20). Nude Video Call Blackmail: Sextortion & Extortion. Retrieved July 2, 2021, from YouTube: https://www.youtube.com/watch?v=L4K9QQDJtck

[3]. Google Maps. (n.d.). Retrieved June 28, 2021, from https://www.google.com/maps/

[4]. Grabify IP Logger. (n.d.). Retrieved June 28, 2021, from Grabify: https://grabify.link/

[5]. Hendrickson, J. (2019, April 18). How to Track Someone's IP (and Location) With a Link. Retrieved July 7, 2021, from www.howtogeek.com: https://www.howtogeek.com/410897/how-to-track-someones-ip-and-location-with-a-link/

[6]. IP2Location. (n.d.). Retrieved June 28, 2021, from https://www.ip2location.com/

[7]. Mahawar, S., & Verma, V. (2021, June 5). How to take legal action against sextortion. (D. R. Sehgal, Editor) Retrieved June 26, 2021, from www.blog.ipleaders.in: https://blog.ipleaders.in/take-legal-action-sextortion/

[8]. Narayan, V. (2021, June 5). Maharashtra cyber chief holds webinar to create cyber awareness .. Retrieved July 1, 2021, from www.timesofindia.indiatimes.com: https://timesofindia.indiatimes.com/city/mumbai/maharashtra-cyber-chief-holds-webinar-to-create-cyber-awareness/articleshow/83262476.cms

[9]. Naveen, P. (2021, May 31). Multi-state 'sextortion' gang that hit MLA busted. Retrieved June 26, 2021, from www.timesofindia.indiatimes.com: https://timesofindia.indiatimes.com/india/multi-state-sextortion-gang-that-hit-mla-busted/articleshow/83101859.cms

[10]. Pradhan, S. (2021, January 20). Sextortion. Retrieved June 25, 2021, from www.timesofindia.indiatimes.com: https://timesofindia.indiatimes.com/readersblog/cyberthoughts/sextortion-29215

Cite this article as :

Sarthak Rathod, Madhav Gaur, Krishna Parihar, Akhlesh Kumar, Dr. S. K. Jain, "Tracing of the Blackmailers in Sextortion Case and Tactics to Defend It - An Experimental Cybercrime Case Study", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 4, pp. 135-142, July-August 2021. Available at doi : https://doi.org/10.32628/CSEIT217414

Journal URL : https://ijsrcseit.com/CSEIT217414