



CYBERCRIMES AND VICTIMIZATION OF WOMEN- A STUDY

G.Lakshmipriya, Research Scholar, Dept. of Law, SPMVV, Tirupati

ABSTRACT

Neither the Information Technology Act, 2000 nor any other legislation in India directly addresses cybercrime. The Indian Penal Code of 1860 and other legislation provide detailed definitions of crimes and their accompanying punishments. As a result, cyber crime may be thought of as a combination of criminal activity with technologies means. Cybercrime may be defined as "any offence or crime that includes the use of a computer". When committing a crime online, the offender is often able to remain anonymous and avoids direct physical contact with the victim, thus the term "cybercrime". A computer or its data may be intended victim of a cybercrime or just the means by which another crime is committed. The umbrella word "cybercrime" encompasses all of these different wrongdoings. Despite the impossibility of creating a crime-free society, which exists only in fiction, efforts should be maintained to uphold laws that keep criminal activity to a minimal. To combat the inevitable rise of cybercrime in our increasingly digital society, law makers will need to implement stricter penalties for those who use fraudulent identities online. As with many things, the potential for good and evil in the use of technology is always there. Several laws have been passed to protect women against cybercrime. Therefore, it is the responsibility of government officials and law makers to ensure that technological progress is made in a positive direction and is used for lawful and ethical economic development rather than illegal activities.

Key words: cyber crimes, women as victim, morphing , phishing

INTRODUCTION

BACKGROUND

The Internet is rapidly becoming and an integral aspect of contemporary life for people everywhere. The expansion of Internet-based activities, however, has not been accompanied by a corresponding decline in online crime. Crimes that are caused due to the presence of the internet are internet crimes called rightly as 'cyber caused crimes'. Now these crimes are of various types, in these sense, that their nature is different. There is cyber bullying, phishing, malware and spyware infections, ransomware etc. More recently people have resorted to online harassment, theft of data and money. As time goes on and the internet continues to expand, cybercrime evolves into one of them most sophisticated and pervasive forms of criminal activity. Therefore, some individuals are able to conduct crime and victimise others via the misuse of computers and the Internet. People who use the internet often and without hesitation put themselves at danger by

overestimating the safety of their online activities. The victims believe that the chance of being a victim is lower for them than for victims of more common types of crime in the actual world. In addition, "information on crime trends, their commission, and victims' reactions are vital for designing preventative strategies and user awareness-raising campaigns." There is a need for having greater control over the criminal activities caused online due to its irregular control and heavy practices. This study takes a close look at what leads to become victims of cybercrime by conducting a systematic literature review with an eye on gleaming insights from the "regular activity hypothesis".

Literature Review

The "unlawful" or "unauthorised" action of "destroying, stealing, or using, modifying, or copying information, programmes, services, equipment or communication network" is what we call cybercrime. Cybercrime is defined by the Council of Europe as "any criminal offence perpetrated against or with the use of a computer network." A computer or other device involving computation is required¹. It is important to remember that cybercrime is a global issue, to which no nation is completely immune. "Cybercrime", sometimes known as "computer crime", refers to an illegal activity in which a computer or internet is involved. In this context, "technology" refers to any electronic device such as a computer, smartphone, or tablet used in the execution of criminal act. Consequently, "this sort of crime has proven extraordinarily expensive to the economy, with yearly losses estimated at 575 billion globally. However, because of the unique circumstances surrounding cybercrime, different risk factors for both offending and victimisation. In other words, the Internet's accessibility across time zones and national boundaries and its pervasiveness in everyday life provide many opportunities for both criminality and victimization. To provide one example, those who engage in more internet activities, that includes online shopping and use of social media, are more vulnerable to becoming victims of internet fraud. Thus, the internet exposure to cybercrime victimizations such as cyberstalking, cyber harassment, hacking, or malware infection.

Cyber crimes and their types

During the epidemic and lockdown, people were compelled to utilise the internet for all aspects of their lives, from work to play. With the rise of the laptop, the smartphone, and the internet, working women could now conduct their careers from the comfort of their own homes. Women students have little choice but to reply on the internet during this time because a growing number of women were actively participating in online communities and utilising various online services for professional and personal reasons. Since the whole nation was on lockdown, the perpetrators of the crime were unable to physically harm the victim and instead resorted to verbal and psychological abuse. Some of the most common types of inter crimes that women face are as follows

CYBERSTALKING

Cyber stalking include following or trying to follow a target online or over the phone despite the targets clear disinterest: leaving harassing or threatening comments on the targets profile: and repeatedly contacting the target vis e-mail or phone calls.

SEXTORTION

During the epidemic, sextortion was the common cybercrime perpetrated by women. In an effort to extort money or sexual favours from their victims, the crooks turned to blackmail to get them to provide intimate photos or photos of themselves that had been digitally altered. As a copying mechanism for the pandemic' anger the offenders threatened women in order to coerce them into engaging in sexual video conferencing or writing. Also, they were desperate, so they used altered photos of victims to blackmail them into giving them money.

¹ Submitted to Coventry University

CYBER ATTACKS

As the pandemic affected the world throughout, more and more people started getting their news online thanks to cyber attacks. Over the last several years, we have seen a rise in the prevalence of fake news and information. When the ladies visited malicious URLs, hackers gained access to their personal information, triggered their phone, microphones and cameras and recorded private moments. Criminals then use this information and these photos for sexing and other purposes.

CYBER BULLYING

The victim is subjected to cyber bullying, which can take many forms, such as the dissemination of false, misleading, and abusive statements about the victim on social networking sites, along with demand for payment to have them removed, the posting of derogatory comments on the victim's posts, the exchange of morphed private pictures of the victim without her consent, and the transmission of rape and death threat²s. Digital or communication technologies, such as a computer, mobile phone or laptop, may be used to engage in a kind of harassment and bullying.

PHISHING

To make money during the shutdown, thieves engage in a practice known as "phishing", in which they send out fake emails that, when viewed, lead the receipt to a website designed to steal sensitive information such as bank account details, contact details, and passwords. It seems that these messages are genuine. Suspicious transactions are then made using the victim's bank account and other confidential information by the offenders.

PORNOGRAPHERS

During the course of the outbreak, pornographers morphed the images of women who had been the victims of internet sexual assault and distributed them for sale.

CYBERSEX TRAFFICKING

Cybersex trafficking is different from traditional sex trafficking in that the victim never meets her attacker in person. When a dealer broadcasts, films or pictures a victim engaging in sexual or personal acts from a central location and then sells this content to sexual abusers and customers through the internet, this is known as cybersex trafficking. The perpetrators have committed acts of sexual violence against women by pressuring, intimidating, and otherwise exploiting them into engaging in cybersex trafficking.

WOMEN-PRIMARY VICTIMS OF CYBER CRIME

While males and adults were victims of a variety of cybercrime schemes, women and children were the easiest targets because to their heightened vulnerability during the epidemic. Many women, especially stay at home moms and social media users, were targets of these crimes throughout the epidemic.

According to statistics compiled by the 2021 National Commission for Women, cybercrime against women drops during a shutdown. During April and May of 2021, when India was hit hard by the second batch of COVID-19 and practically the whole nations was subjected to harsh lockdown restrictions, the number of cyber crimes committed against women spiked dramatically. The frequency of cyber-attacks gradually decreased when the second pandemic wave ended and lockdown limitations were lifted in June. This situation persisted until July, when the curfew was finally removed. Prior to the epidemic and subsequent shutdown, female victims of cybercrime were uncommon.

² Submitted To Eastern Illinois University

CONCLUSION

Any one, wherever in the world, may become a victim of cybercrime since it is mostly an online crime. The most common types of cybercrime include “cyber bullying online fraud, cyber deviance, the crypto market, cyberstalking, sexting, online child sexual abuse and cyber hatred³. A pro-cyber bullying mentality, psychopathic behaviours, social inequality, increased cell phone and Internet use, strong emotions, greed, a lack of awareness, weak law enforcement and international cooperation and the availability of personal information” have all been identified as contributing factors to the rise of cybercrime. Whereas, the most effective responses to cybercrime will include warnings about potential victimization, risk assessments of employees, sanctions and educational initiatives. These results on cybercrime’s root causes, categories and fixes will advance the field of cybercrime studies. What will be the next step in the effort to create a method for reporting cybercrime to law enforcement, however, is something that the present research cannot address due to its reliance on empirical evidence.

REFERENCES

1. Bergmann, M.C., Dreibigacker, A., von Skarczinski, B., & Wollinger, G.R. (2018)- “Cyber-Dependant Crime Victimization: The Same Risk for Everyone?”
2. Catherine D. Marcum And Geogr E. Higgins Cybercrime In, Krohn, Md., Hendrix, N., Penly Hall, G., & A.J. (Eds.). Handbook On Crime And Deviance. Handbooks Of Sociology And Sociology And Social Research.
3. Illievski, A. (2016) “ An Explanation Of The Cybercrime Victimization: Self Control And Lifestyle/ Routine Activity Theory” Innovative Issues And Approaches In Social Sciences, Vol.9, No.1. Pp.30-47
4. Kranenbarg, M.W., Holt, T.J. & Van Gelder J.L. (2019). Offending And Victimization In The Digital Age: Comparing Correlates Of Cybercrime And Traditional Offending Only, Victimization Only And The Victimization-Offending Overlap, Deviant Behaviour, 40:1, 40-55
5. Mesko, G. (2018)- “On Some Aspects Of Cybercrime And Cyber Victimization”. European Journal Of Crime, Criminal Law And Criminal Justice, 26(3)189-199
6. Shabnam, N., Faruk, M.O. And Kamruzzaman, M. (2016)- “Underlying Causes Of Cyber-Criminality And Victimization: An Empirical Study On Students. Social Sciences”. Vol.5, No.1, Pp.1-6.

³ Link.springer.com