INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Aug 2023
ISSN: 2582-6433

DECODING THE CHALLENGES OF DIGITAL VICTIMIZATION

AUTHORED BY - JOEL JOHN THOMAS,
ABHIJITH TOJO & THERES EMMANUEL
Students, 3rd Year B. A LLB
Kristu Jayanti college of Law, Bangalore, Karnataka
Email: joeljohnthomas83@gmail.com
abhijithtojo@gmail.com & kavitheres@gmail.com

Abstract

21st Century has witnessed a tremendous increase in the field of science and technology. Great emphasis has been made on the advancement and the role that cyber space has in the modern world. Cyberspace is one of the stark realities which determines the importance that it plays in the digital world. Cyber space has opened avenues of opportunities which has provided huge benefits to mankind. These opportunities have been utilised and exploited through various technological methods which has led to the diverse growth of digital crimes and intercepted the personal privacy of the individuals. This research paper mainly focuses on e-crimes and the group of people in which hackers intrude on their sensitive data and blackmails them through these vital data's. This paper mainly finds the reasons of victimization which is been revolving around various digital offences. The extent of victimization among the innocent people is increasing at a spontaneous rapid pace rather than decreasing in its trend even though various laws are placed in accordance with the modern digital society. Likewise, this research paper also investigates the support and the need to have new laws for the protection of victims, to tackle the emerging cybercrimes in the digital world and also to have new technological oriented self-awareness programs so that cybercrime can be prevented from further unauthorized sources. This study advocates the principle to have privacy safeguards against commercialization and exploitation of the victim's data. Traditional methods shall be replaced with new modern security measures in order to rectify the loopholes of our system in the cyber space. This paper stresses the need of the hour in order to protect the victims from any further challenges or problems through the invocation of special procedures and to ensure that law enforcement is properly executed.

ISSN: 2582-6433

Keywords: Cyberspace, Victims, Digital world, Cybercrime, Privacy.

1.1 Introduction

Science and technology act has a dominating factor in the present world scenarios which has led to vertiginous changes in the short span of time. These commendable changes have led to numerous inventions and innovations which gradually elevated the standard and lifestyle of human being. These factors have made the life much easier and simpler but has led to the pleather of opportunities where crimes can take place. Crimes have shifted from traditional, conventional to modern, Digital, and electronic offences in the cyber space which has given favourable inclination to offenders. These offences over a period have initiated and made a radical rise of shift in the relational paradigm of personal, cultural, and social interactions in the society which has changed the present world order. The present proliferation of information, to digital and communication technologies has led to importance of study of victimological perspectives in the cyber-World. It is very essential to pay attention to the mode of design of digital architectures which have paid the path for a notable increase for criminal offences initiated and conducted by defrauders and criminal offenders which facilitates for the huge rise in the field of digital victimisation. This has affected the people day to day life order and has made them more prone to adapt a risker lifestyle in the society. This research paper does give a detailed and clear importance in understanding the various forms of challenges and threats that exist in the cyber space. The study resorts to various instruments and tools in designing preventive strategies and constructive measures to tackle the set of changes brought by the digital era. It advocates the need of protection, safety and security of potential victims who are listed in the risk category. This study does promote the need to focus on one own surroundings that can influence the behavioural patterns. thoughts, actions, and desires of the victims in the digital world. These are plenty of loopholes present in the legal aspects of cyber laws in our country. The moment has raised to cement these gaps and tendency of victimisation by promoting, protecting, and nourishing new methods of defensive modes operand against the external illicit interventions in our country.

1.2 Literature review

Sara Giro Correa (2019) mentions about the need to have a proper enforcement and victimization policy that should be put in proper place because it would hamper the process of facilitation and delivery of emergency measures which needs to be taken when a victim is under digital misuse and fraud. It clearly advocates the need of vulnerability understanding of a victim in a specific

ISSN: 2582-6433

situation so that there can be a proper mechanism of adequate victim response to the digital crimes which are taking place in the cyber world.

Catherine Bluya -- (2016) discuss about the growing use of cyberspace among the youth of society which acts as an important instrument for socialization and for building new opportunities in cyberworld. At the same time, it acts as a mechanism of both positive and negative aspects, which is being used for various illegal activities. There is an urgent need of action regarding educating the society with the safe use of cyber space.

C. D Marcum (2021) clearly indicates in his research paper that there are so many hazardous and ripple effects of cyber victimisation which means that cyber victimisation from one sector can affect the other people from various sectors. It is one of the most common patterns which is seen among the group of victims in India. They are cyber of effects which can undermine the survival and the way existence of the individuals in the cyber nation.

Thomas.J. Holt (2017) This research paper analysis that the traditional crime is gradually decreasing and there is a shift towards modern advanced use of cyberspace. The crime rate in our country depicts the fact there is a tremendous increase in the cybercrime rates. There is a need to focus on a separated study between offenders and victims in order to understand the circumstance which lead to the digital crime.

Marleen Weulen Kranenbarg (2017) clearly suggests that the present series of cybercrime it is seen that victims are themselves to be offenders. Here, the cyber offenders utilize a high risk of victimization, victimization – offending this mainly happens due to the law self-control and routine activities that victims do while once they are generally engaged in the social networking sites. They themselves fall prey to these high – risk traps. The degree of victimization increases significantly.

Taher Muhammad (2020) Mentions the causes of cyber-crime victimization in order to understand the severity of cybercrime offences. Among the several kinds of users in the cyber space, adolescents are the most targeted victims of cybercrime. Main cause of victimization includes law self-control, social inequalities, and more usage of cybermedia. Preventive measures like sanctions and educational awareness, warning and many other strategies should be initiated to prevent the threat of victimization.

ISSN: 2582-6433

James Hawden (2001) This paper mentions about the important to implement and educate the society regarding the impacts of digital victimization. There is an urgent need to introduce and enact victim policies in our cyber law system in order to address the contemporary knowledge gap in this digital era.

Rachel killean (2022) which clearly talks about the technology assisted sexual violence which takes place with the complexities that arise from the cyber victimization. Sexual violence is not reproduced in physical from but augmented in virtual settings, this article argues the amplified the traditional understanding of victim and offender behaviour concerning sexual crimes. It highlights the challenges around the ideal victim and responsibility of blame and victim offender. Bystanders continuously which emerge not only within discourses of sexual violence using digital evidence at trial.

Debarali Halder (2021) clearly indicates in his research paper that there are some many hazardous and ripple effects of cyber victimisation which means that cyber victimization from one sector can affect the other people from various sectors. It is one of the most common patterns which is seen among the group of victims in India. They are cycles of effects which can undermine the survival and every existence of the individual in the cyber world.

1.3 Research Questions

- What are the promoting reasons for the tremendous increase of digital crimes in cyber space?
- Is there a need to introduce new preventive measures to decodes the challenges of digital victimisation?
- Whether the present cyber laws sufficient to tackle the challenges of digital victimisation in the present scenario in our country?

1.4 Objective

This research paper aims at decoding the challenges of digital victimisation by examine the various trends of cybercrime present in our society. The promotes the level of responsibility and analyse the bar of awareness about the various criminogenic factors that nourishes and facilities the illicit behaviour that is common among the offenders. It advocates the need to have better knowledge and sense of awareness about the existing laws, rights, and the governing principles

ISSN: 2582-6433

regarding e-crimes. The focus relies on the execution and implementation of new approaches and strategies from the traditional background to a new modern outlook towards the betterment of the individuals in the cyber space and to strengthen the national security of the country.

1.5 Methodology

Present study is mainly based in secondary data collected from various sources about available information on the given topic also, the secondary data has been collected from different sources which includes official data, official figures, and official statistics from the authorised validated sites. The Literature review content for this topic is mainly taken from different journals, books, articles, newspapers etc. This paper gives a clear picture on the present challenges that the victims are facing from cybercrimes in the digital world and due to certain circumstances, they get into the vicious cycle of victimization. Methods and proper strategies are implemented to decode these challenges, so that there will be a better cyber society which is free from the hatched plans and webs created by the online frauds.

1.6 Study Result

Reason for the Increase in Digital crime

It has been observed in the study that there is a lack of awareness among the group of people which is mainly the youngsters, women and children who get facilitated with the marvels of innovation. There is an emergence of cyber culture in which they give less attention to the basic age of maturity which should have been prominent important to access the social networking sites. Newest trends show there are camouflages identities of the individuals which are leading to severe legal issues and unethical approaches which are imposing direct challenge to the nation and to the cyber space which includes various other forms of cyber-attacks etc. Limited opportunity for socialization has led to a special kind of delinquency among the behavioural pattern of the victims which led us to the frozen state of mind and makes them more inclines to the cyber space. We could see a t6endency among the youngsters in which there is a dissociation between the real self and emergence of creation of a digital self. One of the most main problems which is observed in this study is that sharing one's own personal ID and password and sensitive information to virtual friends in which they have never seen and allowing them to use it for personal purpose. When it comes to the children and minors there is a lack of strict vigilance by the guardians providing g the accessibility of electronic devices to the children. This research clearly shows that there is a lack of digital knowledge regarding the safety precautions tools and measures that must be proved

ISSN: 2582-6433

while accessing into the digital space. Due to the mad race of life, people do not read the rules and regulations, policy guidelines to get into these cyber communities. Hence due to the lack of reading this can lead to hacking, economic and sexual crimes. Verbal and child abuses.

Table 1: Awareness of cyber culture among Indian internet users

Awareness of cyber culture among Indian internet users	**Yes**	**No**
1. Knowledge of minimum age to join cyber communities like Facebook, Orkut, Myspace etc	56.2%	43.8%
2. Allow others to use one's own email id / profile id /passwords etc	46.6%	53.4%
3. Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites etc	69.9%	30.1%
4. Mail back to unknown senders of spam / pornographic / erotic /phishing mails	37.0%	63.0%
5. Share personal information / emotions with virtual friends / chat room partners etc whom you do not know in real life	74.0%	26.0%
6. Believe in controlling free speech while communicating in the cyber space	37.0%	63.0%
7. Read policy guidelines of social networking sites, ISPs etc	28.8%	71.1%
8. Use pseudo names	45.2%	54.8%

Arising need to tackle the challenges of Digital

This research paper has found in its observations that there is a trend of continuous sequence of Digital crimes which is taking place in the digital world which are like hacking, stalking, Impersonation, phishing, defamation, bullying moreover different forms of victimisation by virtual friends. In normal instance it has been seen that people are not aware in taking preventive measures and precautions to safeguard their personal sensitive data and rights which led a favourable path to the offenders to conduct digital crimes. People from various age groups fall prey to these crimes and becomes victims and thus the process of victimisation gradually and momentously starts its repercussions step by step. Thus, from all these understanding we can conclude that there is a high need to prevent these forms of digital victimisation. Due to the lack of awareness of the victims about phishing attacks, large amount of money is debited from their personal bank accounts and the money is channelized for illegal purpose including online fraud, cheating, gambling, dark web etc. Impersonation and passionate tricking individuals have led to

ISSN: 2582-6433

defrauding by making cloned profiles of invalid information in order to cheat others. This is done through the mode of recourse of interaction and socialization in social chat rooms and public networking forms. This is possible because of the very irregular nature of appearing in the cyber space and using it for professional purposes which can lead unconsented activities. Data and information miming from social network sites has led to cyber profanity where there is prodding by creating proxy profiles. People once they are immersed in their daily activities people often are subjected to defamation statements against them. Cyber space culture has seen new variants like receiving bullying messages, flaming words, and morphing pictures of victims. It has been seen in the due course of study that after the exhibition of personal information by the victims to the virtual friends they turn out to be online harassers and questions the existence of survival of the victims. It was clearly from the study that the victims are failing in reporting to respective competent legal authorities either due to the lack of courage, fear, and confidence due to the lack of awareness and otherness of reporting such incidents where and how.

The table which is given below delineates the aspect of reporting behaviour and tendency of the victims to the law enforcement agency.

Table 2: Awareness of rights and reporting behaviour

Awareness of rights and reporting behaviour	**Yes**	**No**
Aware that hacking, creation of pornography/distributing the same, distribution obscene materials etc are criminal offences	80.8%	19.2%
Aware of his / her legal right to protect privacy in the cyber space	78.1%	21.9%
Aware that cyber bullying, cyber stalking, sending annoying, defaming messages etc can be penalized	19.2%	80.8%
Has reported incidences of cyber victimization to police / lawyers / courts	9.6%	90.4%

This table clearly depicts that if proper measures are not taken then there will be huge increase of digital victimization among the victims.

Sufficiency of cyber laws in the present scenario

This research paper in its study must come to understanding that there are many loopholes existing in the cyber laws which is present in the country. Cyber laws are not adequate and loosely framed

ISSN: 2582-6433

innovations where issues cannot be dealt in a proper manner in the present legal system. Information and technology Act 2000 act has abominating factor in the cyber field but due to latest innovation in the cyber spaces there is a need to introduce ,implement and execute a proper framed law which addresses all the current issues and tackle all the challenges of digital victimization such as hacking, violation of one's own personal privacy , identity of theft , cyber terrorism, breach of confidential information , transmitting of publications of sexually explicit materials cheating by impersonation and various other cyber related offences. It was clear in the study that there is no proper dissemination of information and lack of education provided by the governmental and state machineries to the educational institutions like schools and colleges etc. Where the main cruse of problem begins. Judicial and Legal Authorities are acting in a lethargic manner to give strict and stringent punishments to the offenders and harassers. When it comes to cyber communications the fundamental right given to the citizens of the country which right to privacy and freedom of speech and expression, right to navigation and of security rights are being violated in the cyber space which is a serious threat that the victims facing in order to voice and echoes their own opinions of the harassment and the intensity of the crime that they have faced. There are no awareness campaigns conducted in our society about the illegalities leading to the victimization in the cyber world are comparatively less than other countries. There is a tendency which is prominent among our fellow human beings to corner the voice and the stand taken by the victims. Due to this attitude, they are stuck in the world of victimisation and it is very difficult to come out from it. There are no proper cybercrime police stations in major parts of our country to take proper remedial measures and there is a fear of hegemonism by police authorities which present them from reporting the various experience of victimization in the cyber world.

Awareness of rights and reporting behaviour	**Yes**	**No**
Aware that hacking, creation of pornography/distributing the same, distribution obscene materials etc are criminal offences	80.8%	19.2%
Aware of his / her legal right to protect privacy in the cyber space	78.1%	21.9%
Aware that cyber bullying, cyber stalking, sending annoying, defaming messages etc can be penalized	19.2%	80.8%
Has reported incidences of cyber victimization to police / lawyers / courts	9.6%	90.4%

ISSN: 2582-6433

1.7 Findings

This research paper has exclusively found out in its abbreviations and findings that there should be a mandatory need of understanding the importance of reading the terms and conditions and policy guideline before entering contract in social networking sites so that online defrauders cannot mime our sensitive data and information. Victims should be precautious in taking necessary steps while they share their profile, passwords, and other personal information to the strangers as well as to their closest friends and relatives so that they will be prevented from further cyber victimization in the future. While having mutual interactions and connections with unknown virtual friends they should be vigilant while they chat, talk, socialize, and mingle with them so that spams, fraudulent activities, misrepresentation, and email spoofing etc can be detected and prevented at an early stage and avoid responding to these messages. Victims should not immediately take asylum with virtual friends when they face any problems because virtual friends tend to utilize and manipulate their identities and the emotional balance of the victims. There should be a fostering of a culture of ethics and education in the minds of victims as well as children and they should be brought up with the basic principles that they should strictly follow while interacting and communicating in the cyber world with full knowledge and awareness of the cyber ethics. It was found in the study that there is a rampant increase of cybercrime in India like cyber defamation, usage of bulling words, sending threat messages, digital harassment, Fake accounts etc. In order to prevent these cybercrimes more the government and the civil society should implement stringent laws so that to prevent further damage experience by individuals in the cyber world. Majority of victims are unable to understand the true nature of hacking and stalking which is taking place in the cyber world and there is a blockade of process of taking proper preventive measures to protect-themselves from the offences of victimization. There is a tendency which is seen in the present scenario where the culture of privacy is not nourished or encouraged but rather it is comprised at a large scale where it becomes a breeding ground for the digital offenders to victimize the victims from the various cybercrime committed in the digital world. Different instruments and measures should be implemented to create a greater consciousness about victimisation among the internet users. Government should have discussions with technocrats and technological resource persons to frame, implement and execute concrete policies so that the extent of digital victimization can be reduced. Digital offenders and victims should be given situation- oriented treatment programs so that they can be reformed and renewed and their contributions would be beneficial for the development of the society.

ISSN: 2582-6433

Table 4: Twenty-Five Techniques of Prevention of Situational crime from Cornish and Clarke (2003)

INCREASE THE EFFORT	INCREASE THE RISKS	REDUCE THE REWARDS	REDUCE PROVOCATIONS	REMOVE EXCUSES
Target harden	Extend guardianship	Conceal targets	Reduce frustrations and stress	Set rules
Control access to facilities	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce arousal and temptation	Alert conscience
Deflect offenders	Use place managers	Disrupt markets	Neutralise peer pressure	Assist compliance
Control tools/weapons	Use place managers	Deny benefits	Discourage imitations	Control drugs and alcohol

Table 5: Twenty types of situational prevention measures for cyber-criminality from Miró Llinares (2012)

REDUCING ENVIRONMENT OF INCIDENCE	INCREASING PERCIEVED EFFORT	INCREASING PERCEIVED RISK	REDUCING PERCEIVED REWARDS	ELIMINATING EXCUSES
Do not introduce targets Separation of hard drives with and without access to system; Systems of parental control; Content filters; ActiveX security controls; No access to chat rooms (grooming)	Control access to system Firewall; Update operating systems; Passwords for system access; Passwords for access to web; Update passwords;	Extend guardianship Forum moderators; Echelon, Enfopol, Carnivore and Dark Web systems	Hide targets Use systems of encryption; Hide personal data on social networks; Do not use bank passwords; Perfect e-commerce systems	Set rules International legal harmonisation; "Netiquette"

ISSN: 2582-6433

	Profiles on social network			
Identify risk zones Informational campaigns about risks; Advise network of spam infections; White and blacklists of web and spam; Identify bots	Detect and impede the attack Antivirus; Antispyware; Antispam; systems of control for electronic banking	Reduce anonymity Identify IPs; Registration on web forums; User identification systems; Biometric identification and authentication	Remove targets Removable hard drives; Alternative payment systems (PayPal); Change web addresses, domains and other	Set rules Web licence notifications: copyright and 'copyleft'; Privacy notifications on Social networks
Decontamination/residue clean-up Erase and destroy latent viruses; Bot disinfection	Deflect offenders' Close networks; Request removal of illicit content; Flagging mechanisms on social networks; Denial of access to specific IPs.	Strengthen formal surveillance Control networks through proxy; Specialized teams for cybercrime persecution	Remove benefits Persecution of buyers of illicit content; persecution of money laundering	Strengthen moral conscience Raise consciousness about intellectual property; Morally enforce legitimate businesses
Separation of targets Internet2; Creation of local security sub-networks	Control tools/weapons Obligatory vigilance through IPPPS;	Assist natural surveillance Improve IP identification systems;	Disrupt markets Offer economic systems of file sharing	Assist compliance new business models (Apple); Legal hacker competitions;

ISSN: 2582-6433

	Control data through RSS	Reconstruct architecture with defensive ends	(Spotify and others); Control direct file download sites	Strengthen open software

This table clearly depicts how situational crimes can be prevented.

These should be proper training and research for digital victimization so that there will be proper solutions put in place to solve the problems which arises out if digital victimization. Increased consciousness should be instituted in the minds of online users about their internet lifestyles by paying more attention to GPS location systems. Guardians should take proper care regarding minores when it comes to exposure of the digital world. There should be increased perceived effort and risk by the police forces and special hotline numbers should be put in place so that digital victims can approach and report to the police at the earliest and the police can arrest the online offenders. In Individuals should possess the basic criminological and technological knowledge so that they can respond in a proper manner in times of need. Responsibility does not lie with government authorities but it has with public, private, and business organizations to adopt methods to eliminate excuses put to adapt polices to present cybercrime victimization in the digital world.

1.8 Conclusion

In a century where satisfaction level of human being is at highest par with the social engineering platforms present in the cyber space. Cyber space provides a lot of opportunities and many disadvantages but the staking fact is that many people fall prey to these designs and hatched webs created by the online defrauders. Victims which arise and come out from there webs are very high in the trends and they are not at all decreasing which is one of the dangerous factors in the developing society. Due to the large presence of victims the process of victimization is increasing at faster pace. Digital victimization is therefore considered a bane than a boom and should be stemmed from further proliferating. It is found in the research study that the group of people themselves flout the rules and regulations and policy guidance due to their negligence and ignorance and they suffer a lot of repercussion in the cyber space. In this digital era where the speed and fast combativity in communication n has led to the cluster of social engineering skills and techniques there has been a tremendous overwhelming development where identity of human

ISSN: 2582-6433

being is comprised in face of artificial intelligence. Digital victimization should be abolished only if stern steps are taken by appropriate authorities to curb the crimes which takes place, Swami Vivekananda says "It is our self-matters" We has human beings should have a sense of responsibility, vigilant mind, dutiful spirit to oversee actions arise from the process of victimization to damage us.

Reference

Tafer Mohammed (2020) Journals of victimisation vol 5, pp 119 -123

Thomas. J. Holt (2019) Journal of criminal offenders and victimization, Vol 3, pp 118 - 121

Catherine Balya (2016) Journal of Cyber space and cybercrimes digital space, Vol 4, Pp 113-115

www.thehindunewspaper.com

www.Indianstatisticaldata.com

www.sarahcohenjournals.com