CYBER VICTIMIZATION: ATTENTION FOR PREVENTION

Jatin Kalon[*]

I. INTRODUCTION

Cyber victimization requires urgent attention, especially when the Internet has become the need of the hour.[1] Governments, both at national and international levels are promoting digitalization as a new way of governance. Internet, which initially started with the desktop computer only, now has omnipresence. 'Mobile Phones', which once were known as the means of communication, are converted into 'smartphones' and are now used both as a fashion symbol and a way to do commerce. So many smartphones' based applications are available by which it is very convenient to do transactions.All this shows as to how cyberspace has created such a powerful and omnipresent virtual world without which we cannot live in the present times. And, therefore it is neither easy to prevent cyber-crimesnor easy to even detect them and more so, when identified, it is very difficult to prosecute the criminal and punish him. And, therefore, cyber victims are the most vulnerable of all; sometimes they are even not aware of as to who is the criminal. In this article, the author has *firstly*, tried to explain the term 'cyber victimization',*secondly*, the author has examined reasons as to why there is a need to give attention to the cyber victims and *thirdly*, as to what are the possible ways to prevent cyber victimization.

II. CYBER VICTIMIZATION

Cyber-victimization is a process of victimizing any human being by using information and communication technologies such, as the internet, computers, smartphones, etc. And, a cyber victim can be anyone, including, from an individual to the big-big organizations and many times, even the governments. In the traditional crimes, the offender and victims are required to interact physically, but in the cyber victimization 'there is no physical convergence in space and time of offenders and victims'.[2] Generally, people who spend more time on online transactions are more prone to cyber victimization of online fraud.We have often heard the sentence, 'Sorry! I had not sent that message. My mail was hacked'. We have also heard a number of the times that some political party's website has been hacked. Hacking is the most prominent cyber-crime. There isample evidence which clearly establishes the fact that individual organizations and governments are the most vulnerable cyber victims.[3] Similarare cyber sexual offences, cyber bully, etc. In cyber sexual offenses, it is often seen that the victims are harassed by cybercriminals by sending them morphed images, messages, etc. Constant threats are also made to cyber victims, which creates mental and physical stress. Many times, this has led to psychological disturbances of the cyber victims. And, because Cyber-crimes are increasing every day, therefore there is a strong need to do research on cyber-victimization and how to prevent it.

[*] Research Scholar at Faculty of Law, University of Delhi, Delhi.

[1] Jacqueline D. Lipton,"Combating Cyber-Victimization"26(2) *Berkeley Technology Law Journal*1103-1155 (2011).

[2] M. W.Kranenbarg, T. J.Holt, *et.al.*, "Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and TraditionalOffending-Only, VictimizationOnly and the Victimization-Offending Overlap"40(1) *Deviant Behavior* 40-55 (2019).

[3] United Nations Office on Drugs and Crime, "Cybercrime" (2013), *available at*: https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf (last visited on July 05, 2019).

III. TYPES OF CYBER VICTIMS

All internet users are vulnerable to the cyber-attacks. It is found that most of the crimes in cyberspace are the online version of the traditional forms of crimes.[4]Internet users are harassed by unsolicited digital communications or interactions that threaten to defame. This platform is being used by the perpetrator to victimize or bully through abusive or humiliating comments or pictures, and personal identification.[5] Individual social media and digital footprints are used to harass, intimidate and cyberstalk.[6] It has been seen that the victims also suffer identity theft and are subjected to malware and viruses.[7] There are primarily three types of abusive online conducts, Cyber-bullying, Cyber-harassment, and Cyber-stalking[8] and in all these three categories, the victims face mental harassment, which at times, compels them to end their lives. Cyber-bullying often happens in the case of juveniles, where one person tries to dominate over the other students and this is very commonon social sites. Similarly, in Cyber-harassment, the harassment is done on social media sites, by either using vulgar languages or by sharing some verypersonal information on social media. And, in Cyber-stalking, the conduct of the accusedis directly aimed at the cyber victim, as the person starts following the other person everywhere, intrudes into personal social media accounts and tries to access almost every cyber account.

'Online sexuality' like 'pornography, sex shops, sex work, sex education, sex contacts, and sexual subcultures' which engaged large volume of Western people irrespective of age, gender and sex.[9] While Doring[10] argues internet sexuality should not be considered as ‘‘virtual pseudo-sexuality” in comparison to ‘‘real sex” as 'online dating' services' is a successful mechanism to meet the sexual partner in the real world. Cyber sexuality has both positive and negative consequences. In a positive way, it gives sexual satisfaction without facing sexually transmitted diseases but the negative side is that it has an adverse impact on the sexual attitude and identities. All these offences are severe in nature and cause extreme cyber-victimization.

IV. CYBER VICTIMS: IMPACT OF CYBERCRIMES ON BUSINESSES AND INSTITUTIONS

Every crime plays a negative role in the lives of the victims and cyber-crimes also have a negative impact on all the businesses and institutions and particularly on the finance sector. The cyber-criminals steal the confidential data and other critical information by using various types of malware, or by simply hacking the server or the websiteof the businesses and organisations. They can even spread viruses.[11] The above threats forced companies especially online/ e-commerce companies to spend huge amounts on digital security.

[4] A. Baxter, “Improving responses to cyber victimisation in South Australia” (2014), *available at*:http://www.victimsa.org/files/cybercrime-report-2014.pdf (last visited on July 09, 2019).

[5] *Supra* note 1.

[6] L. Roberts, “Cyber Victimisationin Australia: Extent, impact on individuals and responses” 6*Tasmanian Institute of Law Enforcement Studies*1–12 (2008).

[7] Supra note 2.

[8] Supra note 3.

[9] N.M. Doring, “The Internet’s impact on sexuality: A critical review of 15 years of research” 25(5) *Computers in Human Behavior* 1089-1101 (2009).

[10] *Ibid*.

[11] P.R.J. Trim and Y.I. Lee, “Issues that managers need to consider when undertaking research relating to the cyber environment”, in P. R. J. Trim and H. Y. Youm (eds.), *Korea-UK initiatives in cyber security research: Government, University and Industry collaboration* 66–79 (Republic of Korea: British Embassy Seoul, 2015).

Sometimes, the budget of digital security is extremely huge as compared to the rest of the expenses. There are various individual organisations which provide special digital security services to the governments and the other organisations, such as, Norton Anti-Virus, and others.

A. IMPACT OF CYBER-CRIMES ON THE HEALTH OF CYBER VICTIMS

Health is wealth, but when the wealth is lost in a cyber-crime then the health automatically derails. The impact of cyber-attack on the individual victims can be seen directly on their health and sometimes,the victims even suffer depression, fear and anxiety, mental trauma and in extreme cases, even suicide.[12]Cyber-attacks directly affect the savings, financial assets and credit ratings and sometimes employment too.[13]The financial cost to an organisation and businesses to prevent cyber victimization is sometimes very high. Various cyber-crimes include hacking, defrauding, extortion and stealing of financial and intellectual assets of the firms/entities/individuals. There are various types of cyber-crimes can be happened with the Firms, such as, they can be hacked, defrauded, extorted and have their financial and intellectual assets stolen. Not only this, their brand and name value can also be compromised in cases of severe cyber-attacks. According to Google, hackers steal almost 250,000 web logins each week[14] and the average cost of cybercrime for an organization has increased from US$1.4 million to US$13.0 million.[15]Not only the individuals but the governments havealso been targeted for taking political and financial advantages. Maximum information of government is available online which invitesa sophisticated and severe systematic attack on the critical information and infrastructures.

V. CAUSES OF CYBER VICTIMISATION

The first step of the Cyber-criminals is to identify their soft targets in the cyberspace. For instance, they constantly use public announcements, as a means to identify their soft targets. Children and aged persons are more prone to cyber-crime than anyone else. Like a year back in India, there was a public announcement that every bank account holder should connect their Aadhar card details with the bank accounts. Now, these cyber-criminals started making calls to the persons on behalf of the bank and started pressurizing them to share their phone number, and Aadhar details so that their bank account can be linked with the bank accounts. And, by this process, people voluntarily started sharing their confidential details with the cybercriminals and ended up losing their money. This is not the only instance, there isa plethora of such pending complaints and further, many cases even go unreported. It is, therefore, necessary to examine the causes of Cyber-victimization. There are various other types of cyber victims also. It is seen in many cases, that women harassment clips are made available on social media, which causes tremendous stress to cyber-victims. Similarly, in many cases, it has also been found that cyber financial frauds are caused in which, the most vulnerable part of the society, children and aged persons are the victims. In fact, the world is facing another threat of cyber terrorism where the victims are going to be all the citizens of the county.

[12] R. Dredge, J. Gleeson, *et.al.*, "Cyberbullying in social networking sites: An adolescent victim's perspective" 36 *Computers in Human Behavior*13–20(2014).

[13] *Supra* note 6.

[14] See https://money.cnn.com/2017/11/09/technology/google-hackers-research/index.html (last visited on July 05, 2019).

[15] See https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (last visited on July 05, 2019).

Victims of cyber-attacks, often, are rich and wealthy people and organizations, banks, casinos, financial firms, etc. And, it is very difficult to first, identify the criminals in cyberspace, and even more difficult to arrest them. This is one of the major reasons forincreasing cyber-crimes because the criminals are aware of the fact that it is not easy to identify the, and the herculean task is to arrest them. The followings are the main causes of cyber victimization.

A. Saving Oneself in the Cyber-world

While working in cyberspace, many of cyber users are not aware of the safeguards attached with it, such as, how to secure oneself from the cyber hacking, when they are logged in through their desktop, laptop, smartphones, etc. In fact, in a number of cases, it is found that the cyber victims found noting 'ID' and 'Passwords' of their applications, phones, etc. in a notebook accessible to all or in the mobile phones, which if stolen, can lead to loss of complete data. Therefore, ignorance or unawareness of internet users has made them more vulnerable to cyber-attack. It is very easy for the Hackers to steal or access internet users' codes or retina images or advanced voice recorders of those internet users, and it is further very easy for them to fool biometric systems easily and bypass firewalls, which can be utilized to get past many security systems.[16]

B. Data is Available in a Compatible Format

One of the major cyber-crimes is stealing one's data. In today's world, data is everything. Everybody needs data and due to excessive demands of data, there is an increase in number of data theft cases. The smartphones and computers have a unique quality to store maximum data in minimum storage. This unique feature helps the cybercriminals to steal data and information from the machine's storage easily and victimize the users and many times, this results into demand for ransom, defame or killing the victims. There are various reported cases, where stolen data was used for ransom and in many cases, victims give up by ending their lives.

C. Computer Programming is Complex

Computers and smart devices operate through millions of codes and the human capabilities are very limited and therefore, the possibility of negligence increases. Even a single negligent step is enough for cybercriminals to victimize the victim by accessing or controlling their computer or any other smart system.

D. Negligible Reporting of Cyber Crimes

In many cases, people, very late get to know that they are cyber-victims. All the internet users are not aware ofthe fact that police complaintscan be filed about cyber victimization. In fact, every police station has a cyber cell to report cybercrime cases. Yet, very few cases are reported at the police station. Even, sometimes the police officers themselves are not aware of the provisions of IT Act 2000. Therefore, many of the instances of cyber-victimization remain unreported.

[16] See https://krazytech.com/technical-papers/cyber-crime (last visited on July 09, 2019).

Cybercrime is nothing but human destructive activities in the cyberspace, which lead to severe destructive results.

VI. The Ways of Tackling Cyber-victimization

We are aware of the fact that cybercriminals are sharp in their activities, but only by taking certain precautions, one can no doubt save oneself from the cyber-attacks. One should be aware of the fact that every person is vulnerable, when he connects his electronic machines to the internet. Below, certain steps have been discussed to tackle Cyber-victimization.

A. Using Random Passwords

Most of the cybercriminals before hacking computers get personal information of the victims so that by using that information, they can easily hack their e-mail and other accounts. It is, therefore, necessary to know that, internet users must not use personal information in their IDs and Passwords, such as, one must not use birthday date, year, son's or daughter's name, date of birth, etc. as either e-mail IDs or passwords. One should always use random numbers and alphabets, caps lock feature, numbers, and symbols for making passwords.

B. Using Firewalls and Security Software

There are various ways of protectingthe computer system from cyber-attacks. One of them is to use firewalls and the other is to use various types of customized security software available. The government sites are managed and controlled by the government's specialized agencies. While in the case of big businesses, they either have to set up their separate departments to continuously check updates and firewalls of the websites or they take specialized services from other big companies for securing and protecting their sites and data from hacking. E-Commerce companies such as, Flipkart, Amazon, Infibeam, etc.use secure platforms for online transactions and keep updating their sites for better performance and protection. In short, everyone including governments is focused on taking measures to keep the computer system, data, and server, safe. And, they spend huge amounts on cybersecurity to protect them.

C. Combating Cyber Harassment from SocialMedia

Cyber-victims are most vulnerable to crimes such as, cyber-harassment, because any news on social media spreads like wildfireand comments and reviews start coming in within minutes. It is therefore essential to know as to how to combat it. On social media sites such as, Facebook, there are provisions for reporting the contents, which can be used to inform the social media provider about the harassment the victim is facing[17]. In this way, not only strict action is taken against the cyber-criminal, but it also helps the cyber-victim not to fall prey to mental stress and trauma.

VII. Empowering Cyber-victims

[17] Tom van Laer, "The Means to Justify the End: Combating Cyber Harassment in Social Media" 123(1) *Journal of Business Ethics*85-98 (Aug., 2014).

It is therefore essential to empower the internet users who become cyber-victims so that they not only save themselves from the cyber-attacks but, they also help in authorities to catch hold the cybercriminals. It is only by empowering cyber-victims with the requisite knowledge that cyber-victimization can be avoided. There are various e-initiatives taken by the Banks and Income Tax Department by issuing time to time notices in the newspapers regarding fake calls demanding Bank Account Number or Permanent Account Number (PAN) issued by the Income Tax Department or Aadhar Number. In fact, the customers are informed by the banks and Income Tax Department, directly *via* e-mails and also on their registered mobile phone numbers. By dissemination of timely information like this, the cyber-victims can be empowered. The solution to cyber-victimization is to take timely-precautions and all the possible preventive measures to save oneself from cyber-crimes such as, online fraud and not to panic at any time and immediately report any such suspicious event. By taking the above preliminary steps, cyber-victimization can be prevented.

VIII. Conclusion

Cyber Crimes have become a big challenge which has engulfed almost everybody. Every function of the government is executed on the internet. All the banks, public transport system, businesses, stock exchanges, etc. are completely dependenton internet for their smooth running and therefore, there is a constant threat, of securing the network from the cybercriminals, because any cyber-attack will make the situation precarious. In fact, the security of the State is also internet-based, and therefore, the threat is alarming and deserves urgent attention.