THE DIGITAL AGE: CYBERCRIME VICTIMIZATION AMONG ADOLESCENTS

[1]JINCY T.C, [2]A.ENOCH

[1]Research Scholar, [2]Assistant Professor
Department of Research (M.Phil. and PhD) in Social Work
Madras School of Social Work
Chennai- 600 008

***Abstract*: People's lives are being transformed by the digital age, which is faster, more creative, and, as a result, in a critical state. This conceptual study examines cybercrime and safety issues during adolescence. Adolescence is a period of enthusiasm and its consequence is the unabashed acceptance of new technology without avoiding its threats. Through secondary data, this study analysed the cyber threats and safety among adolescents in the aspects of promotion, prevention, treatment, and rehabilitation. This study aimed to educate adolescents and society about the importance of using social media responsibly in order to avoid cybercrime. It creates a new generation with the prudence to operate advanced innovations for the progress of the world.**

***Keywords*: Cybercrime victimization, cyber threats, prevention, treatment, rehabilitation**

Introduction

The new generation invests more time in social networking sites with smartphones and computers to play games, chat, create TikTok videos, and make friends. The new technology prompts cyber users to increase their usage, which indirectly leads to an increase in cybercrime too. Information and communication technology have become an unavoidable part of our daily lives. Contacting friends, sharing updates, playing games, shopping, and so on are all possible thanks to advanced communication media. Without bothering about the cyber threats, adolescents, as an experimental group, are always testing the digital medium. Increased use of cyberspace at a young age leads to the rapid proliferation of cybercrime. (Ministry of Home Affairs, Government of India, 2018).

Most adolescents argue that there is no harm in chatting with strangers and accepting any friend request. They have friends of different genders and are not bothered by sharing vital and personal information (Hamsa, S.2018). This paper discusses cybercrime, victimization, and digital media in adolescence.

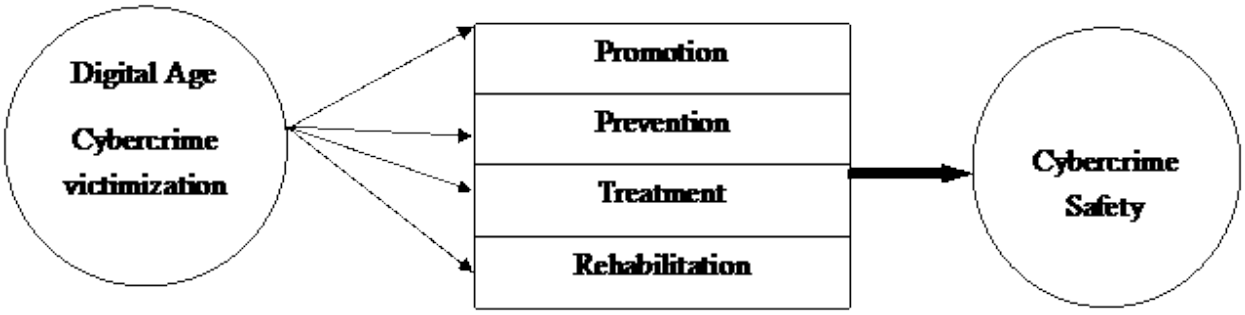
Statement of the Problem

The expansion of the internet into an integral part of everyday life has brought a large amount of potential risk for its users. Various types of cybercrime have become established in the online space, which sometimes leads to facilitating damaging behaviors. Cybercrime, as a term, is a broad concept that encompasses all manners of criminal activities carried out online. Online interaction does not permit the social presence and richness of face-to-face interaction, but it is transferred into computer-mediated communication (CMC). Even though it is not equivalent to face-to-face interaction, online social networking sites have become an increasingly vibrant source of social identification and support (Kaakinen, M. et al., 2018). In the year 2017, 1785 cases have been reported (Rs 71.48 crores) related to credit/debit and Internet banking fraud (Ministry of Home Affairs, Government of India, 2018). A study on the power and the pain of adolescents' digital communication: cyber victimisation and the perils of lurking revealed that adolescents are heavily engaged in social media and text messaging. Adolescents are constantly fascinated by changing digital platforms and are using more than one social networking platform. Cyber aggression and cyber victimisation occur mostly through social networking sites like Facebook messaging and mobile phones (Underwood, M. K., and Ehrenreich, S. E., 2017). The Indian Computer Emergency Response Team (CERT-In) reported a total number of 44,679, 49,455, 50,362 and 53,081 cybersecurity incidents during the years 2014, 2015, 2016 and 2017 respectively. The National Crime Bureau (NCRB) registered a total of 9,622, 11,592 and 12,317 cybercrime cases during the years 2014, 2015 and 2016 respectively (The Hindu BusinessLine, February 09, 2018).

Methodology

The conceptual paper presents the original concept through synthesised information from previous research articles. This paper focuses on cybercrime and cybercrime victimisation in the aspects of promotion, prevention, treatment, and rehabilitation.

Conceptual Model



Literature Review

The literature review, which was a collection of published materials related to cybercrime and cybercrime victimisation among adolescents, contributed to the advancement of knowledge in the field of cyberspace. review discussed the digital usage of adolescents and its threats.

Cyber Crime

Social media creates social space for users to create a public profile and to interact with one another through online platforms. Cybercrime can be defined as unlawful acts where the computer is used either as a tool or a target or both. Cybercrime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and includes everything from electronic cracking to denial of service attacks. It covers crimes like phishing, credit card fraud, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, spam, and so on (Gupta.S. et al., 2017). According to the statistics of the National Crime Records Bureau (NCRB), cybercrime in India almost doubled in 2017. Cybercrimes are offences committed against individuals, institutions, and groups through computers, the internet, and mobile technology. Cybercrime mostly targets stealing personal information such as phone numbers, photographs, bank details, etc.

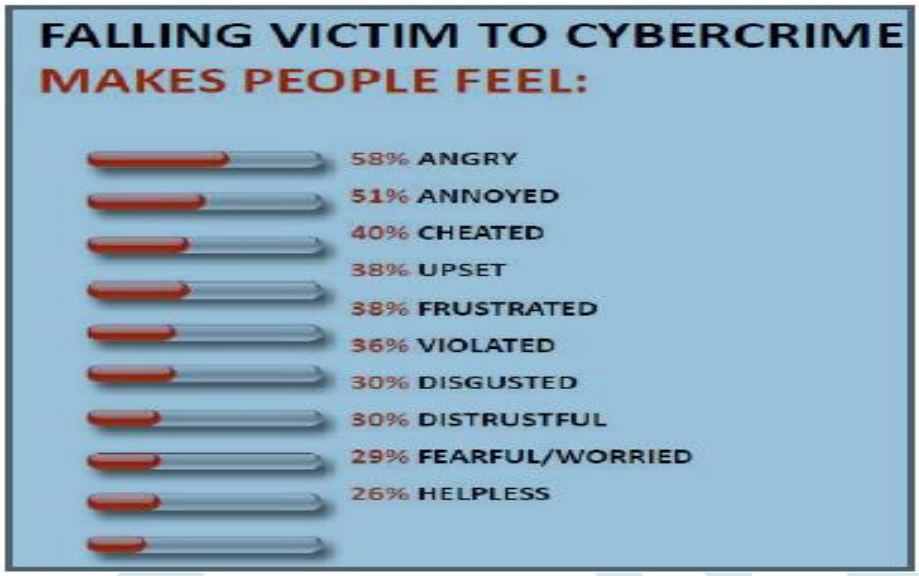
Cybercriminals use social networking sites, emails, pirated software, websites, etc. to harass victims. The personal information helps the criminals to create a fake profile and hijack other accounts. Email Spoofing, Malicious file applications, Social Engineering, Cyber Bullying, Identity Theft, Job Frauds, Banking Frauds, and E-Mail Fraud are the most common cybercrimes prevalent in these days of technology. Email account hacking by using malware is a very common cyber attack for sending fake messages. Cyberbullying is one form of common harassment or bullying faced by adolescents through the use of electronic or communication devices. Due to the augmented use of social media, cyberbullying has become a major issue among teenagers (Alim, S. 2016, 68). Offenders mostly target adolescents, as the age of immense biological, personal, and social changes creates an emotional bond through social media platforms with the aim of sexual abuse or exploitation (Ministry of Home Affairs, Government of India, 2018).

Cybercrime Victimization and Adolescents

Cyber-victimization refers to the process of victimising others through the use of information and communication technologies (Roberts, L. D. 2009, 575). According to a study on the development of criminal styles in adolescents and young adults, the majority of adolescents follow a solo offender trajectory (Goldweber et al., 2011, 332). A multi-nation study discovered that while online crime victimisation is uncommon, slander and the threat of violence were the most common forms of victimization. Male gender, younger age, immigrant background, urban residence, not living with parents, unemployment, and a less active online social life were all significant predictors of cybercrime victimisation (Nasi et al., 2015, 203). Weulen Kranenbarg et al. (2019, 40) discussed cybercrime offending and victimisation in the study on offending and victimisation in the digital age: When comparing correlates of cybercrime and traditional offending-only, victimization-only, and the victimization-only overlap, malware victimisation is most common among victims of cybercrime. Hacking by guessing a password is often committed by victim offenders. Cybercrime correlates with low self-control, IT skills, online and offline routine activities, and digital context. Low self-control is a significant predictor of being a cybercrime victim-offender.

A study on cybercrime victimization: an examination of individual and situational level factors (Ngo, Fawn T., and Raymond Paternoster, 2011) indicated that self-control was significantly related to cybercrime victimization. This study also found that age, race, employment status, and computer deviance were significantly related to cybercrime victimization, while sex and marital status had no effect on the possibility of becoming a victim in cyberspace. This article explores the effects of individual and situational factors on seven forms of cybercrime: the computer virus, unwanted exposure to pornographic materials, sex solicitation, and online harassment by a stranger, online harassment by a known person, phishing, and online defamation.

Psychological Impact of Victimization



Source: Norton Cybercrime Report, 2011

Cybercrime and Sensitization

According to the lifestyles and routine activities perspective, low levels of self-control and exposure motivate offenders to be online predators with aggressive behaviour and activities in cyberspace. Inculcating self-control among adolescents is the first and foremost constructive method to promote digital media in safe hands. (Ngo, Fawn T., and Raymond Paternoster, 2011). Parental control and supervision tend to have a protective effect on adolescents' high-risk internet behaviour and cyber aggression (Alvarez, G. et al., 2019, 1159). The behavioural and environmental approaches will help to create a positive attitude towards digital media and its appropriate use. Even though the enormous number of cybercrimes is reported in official documents, the awareness of cybercrime and its safety is quite low among students and adolescents (Ismailova, Rita, and Gulshat Muhametjanova, 2016, 32). E-security consciousness, training, and education for digital consumers have been of great assistance to the installation of security software and systems to avoid malware apps (Martin, Nigel, and John Rice, 2011, 803). At the early stage of sensitization, it is mandatory to facilitate the users to create positive thinking and digital skills to keep away from cybercrime victimisation (Sukhai, N.B. 2014, 128). Cyber-attacks are one of the top five risks in the world, and it is harder to identify, harder to stop, and it is causing a long-term negative impact on victims. To secure this cyber threat, we need to know about this crime and how it works against adolescents and others (Gunjan, Vinit Kumar, Amit Kumar, and Sharda Avdhanam, 2013). Schools have a great role in imparting knowledge of cyberspace and developing digital skills, critical thinking, decision-making as well as ethical, legal, and safe use of digital media (Filipa Pereira, 2015). Hardware and software gadgets are widely used to make stronger information systems against attacks (Ogutcu, G et al, 2016). Cybercrime, one of the most vital security issues in the coming years, needs precautions and safety measures to protect the next generation (Schilling et al., 2016).

Cybercrime and Prevention

In order to prevent cybercrime among adolescents, it was suggested that they discontinue use of media interfaces based on video-sharing sites, online games, social networks, and chat rooms (da Silva Pereira et al. 2015, 211). Cybercrime prevention requires more than just enforcing the law; it also requires a comprehensive policy approach and strategic intelligence (Buono, Laviero, 2014, 1). Fighting against cybercrime needs a holistic approach instead of just addressing it alone (Ajala, Emmanuel Babatunde, 2007). Holt, Thomas J., and Adam M. Bossler (2015) discussed five categories of situational crime prevention related to both offenders and victims. The five categories are: making it more difficult to commit crime, increasing the danger of detection, lowering the incentives that may arise from offending, reducing provocations to offend, and removing excuses for offending. Computer users and those who provide access to cyber space should take reasonable security actions to prevent the commission of cybercrime (Brenner et al., 2004).

The Ministry of Home Affairs, Government of India (2018) recommended some preventive and safety methods to protect adolescents from cyber crime.

- Do not accept a friend request from unknown people on social platforms. This is one of the best preventive methods to protect you from becoming a cyber victim.
- Subscribers must exercise caution when sharing personal information such as their date of birth, address, and phone number on social media or other online platforms.
- Restrict others from accessing our profile and never install unwanted software and apps, such as dating.
- Use two-factor authentication for login.
- Changing the PIN periodically

- Using public Wi-Fi to conduct online transactions is discouraged.
- Other preventive methods (Shoukat et al., 2018)
- Never upload sensitive data to social media platforms.
- Create a complex password and change it regularly.
- Ignore Pop-Ups
- Create the habit of no response to badly presented data and videos.

Early identification and early stage prevention would help to put a stop to cybercrime and avoid cybercrime victimization. Limited knowledge of cyber threats and enthusiasm in the field of digital communication lead the young to become easy victims of cyberbullying. Preventive methods help to control the usage and to avoid sending rude messages or spreading embarrassing rumors.

Cybercrime and treatment

Social media addiction and cybercrime addiction have become an inescapable crisis in the digital era. Like physical treatment, we should have to treat the victims and offenders to change their behaviour and overcome the impact of these events. According to Crime Addiction Anonymous out of Vancouver, Canada, "crime can be an illness as tenacious as dependency on alcohol or drugs." There are various views regarding the cause of the criminal nature of an individual. Some argue that committing a crime is due to the thrill and fun experienced by the perpetrator. Psychologists argue that criminal motivation can also be based on psychological desires and psychological needs like power, reassurance, or seeking retaliation for past harm. Behavioral therapy and self-discipline are the most effective methods of treatment to develop changes in behaviour and to prevent future criminal activity (Nykodym, 2008).

Early treatment would aid in avoiding the transformation of a simple problem into a complex one. Complicated operations need severe treatment in the digital world. Quick and requisite treatment in digital communication is blocking (Subrahmanyam, et al., 2006). If adolescents use the benefit to block the fake users in social media apps, it will help to overwhelm cybercrime (Cyber Safety for Adolescents-vikaspedia, 2020). Advanced cyberspace witnessed a great addition to online gaming, which adversely impacts the psychosocial behaviour of adolescents. Even though India owes a lot to the experimental growth of information technology (Nappinai, 2010), the number of cyber crimes reported is increasing day by day. The Digital Police Portal is a SMART policing initiative of the Ministry of Home Affairs that helps to report cybercrime. According to the Information Technology Act 2000 of India, producing, publishing and transmitting sexually explicit material or child sexual abuse material (CSAM) is a punishable offence (Ministry of Home Affairs, Government of India, 2018). The National Cybercrime Reporting Portal is an initiative of India to facilitate victims to report cybercrime complaints online.

Cybercrime and Rehabilitation

Crime victimisation not only affects the adolescents' academic performance but also their physical, emotional, and psychological well-being to a great extent. (Ministry of Home Affairs, Government of India, 2018). A survey with US college students found that frequent Facebook interaction is associated with greater distress directly and indirectly and lowers self-esteem (Chen & Lee, 2013). Promotions of outdoor activities and physical games instead of online games have been very beneficial to overall physical, mental, and social development. The habit of playing outdoor games helps to generate a new healthy environment, develop muscle strength, mount confidence, make new and real friends and develop overall personality (Ministry of Home Affairs-Digital Police). According to a study on cybercrime victimisation and subjective well-being: an examination of the buffering effect hypothesis among adolescents and young adults, victimisation to offensive crime had a stronger negative association with subjective well-being than victimisation to cyber fraud (Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A., 2018). Through rehabilitation activities, adolescents could recover from psychological problems like stress, depression, anxiety, and fear. It will help to promote positive thinking and the mature use of digital media. It may generate a creative comeback in the digital communication media.

According to Routine Activity Theory, a suitable target group and the absence of a capable guardian have been motivational factors for an offender to commit a crime (Chang, 2012). Parental protection has a great role in the rehabilitation and prevention process of cybercrime. Cyber Insurance coverage is used to protect users from digital-based risks and help to meet investigation expenses. It is beneficial in the event of a large-scale security incident (Shoukat et al., 2018).

Conclusion

Rapid technological growth changed adolescents' ways of thinking, acting, and styling. The digital revolution as a "double-edged sword" (Chang 2012), builds on constructive and crisis situations. Preventive measures help adolescents avoid cybercrime victimization. The advanced digital world needs an "alert action" in the field of communication. Parents, schools, and government authorities have an immense role in safeguarding adolescents from cyber threats.

Reference

Ajala, Emmanuel Babatunde. 2007. "Cybercafes, cybercrime detection and prevention." *Library Hi Tech News*.

Alotaibi, Faisal, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. "A review of using gaming technology for cyber-security awareness." *Int. J. Inf. Secur. Res.(IJISR)* 6, no. 2: 660-666.

Álvarez-García, David, José Carlos Núñez, Paloma González-Castro, Celestino Rodríguez, and Rebeca Cerezo. 2019. "The effect of parental control on cyber-victimisation in adolescence: the mediating role of impulsivity and high-risk behaviours." *Frontiers in psychology* 10: 1159.

Alim, S. 2016. Cyberbullying in the world of teenagers and social media: A literature review. International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 6(2), 68-95.

Árpád, Incze. 2013. "A greater involvement of education in fight against cybercrime." *Procedia-Social and Behavioral Sciences* 83: 371-377.

Brenner, Susan W., and Leo L. Clarke. 2004. "Distributed security: Preventing cybercrime." *J. Marshall J. Computer & Info. L.* 23: 659.

Buono, Laviero. 2014. "Fighting cybercrime through prevention, outreach and awareness raising." In *ERA Forum*, vol. 15, no. 1, pp. 1-8. Springer Berlin Heidelberg.

Chang, Yao-Chung. 2012. *Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait*. Edward Elgar Publishing.

Chen, Wenhong, and Kye-Hyoung Lee. 2013. "Sharing, liking, commenting, and distressed? The pathway between Facebook interaction and psychological distress." *Cyberpsychology, behavior, and social networking* 16, no. 10: 728-734.

Cyber safety for Adolescents- Vikaspedia.(n.d.). Litercy/information-security/a-handbook-for-adolescents-students-on-cyber-safety. https://vikaspedia.in/education/Digital%20

Goldweber, Asha, Julia Dmitrieva, Elizabeth Cauffman, Alex R. Piquero, and Laurence Steinberg. 2011. "The development of criminal style in adolescence and young adulthood: Separating the lemmings from the loners." *Journal of youth and adolescence* 40, no. 3: 332-346.

Gunjan, Vinit Kumar, Amit Kumar, and Sharda Avdhanam. 2013. "A survey of cyber crime in India." In 2013 15th International Conference on Advanced Computing Technologies (ICACT), pp. 1-6. IEEE.

Gupta, Shalini, Anamika Singh, Sheela Kumari, and Neelma Kunwar. 2017. "Impact of Cyber Crime on Adolescents through Social Networking Sites." International Journal of Law, 104–6.

Thakur, Anchal, and Tejpreet Kaur Kang. 2018. "Gender and locale differences in cyber crime awareness among adolescents." *Indian Journal of Health & Wellbeing* 9 (2018).

Vol, Pune. 2018. "Annual Research Journal of SCMS, Pune Vol. 6, March 2018" 6 (March): 97–123.

Holt, Thomas J., and Adam M. Bossler. 2015. Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

https://cybercrime.gov.in/Webform/Crime_OnlineSafetyTips.aspx 2/

https://cybercrime.gov.in/Webform/crmcondi.aspx 1/

https://digital police.gov.in

https://www.up.ac.za/media/shared/62/COPC/copc_principles02.zp55893.pdf retrieved on February 16, 2020

Ismailova, Rita, and Gulshat Muhametjanova. 2016. "Cyber crime risk awareness in Kyrgyz Republic." *Information Security Journal: A Global Perspective* 25, no. 1-3 : 32-38.

Jaishankar, K. "SASCV 2011: Special Conference Issue of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV)." *International Journal of Criminal Justice Sciences* 6, no. 1/2 : 12.

Kaakinen, Markus, Teo Keipi, Pekka Räsänen, and Atte Oksanen. 2018. "Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults." *Cyberpsychology, Behavior, and Social Networking* 21, no. 2: 129-137.

Konradt, Christian, Andreas Schilling, and Brigitte Werners. 2016. "Phishing: An economic analysis of cybercrime perpetrators." *Computers & Security* 58 : 39-46.

Martin, Nigel, and John Rice. 2011. "Cybercrime: Understanding and addressing the concerns of stakeholders." *Computers & Security* 30, no. 8: 803-814.

Ministry of Home Affairs Government of India. 2018. A Handbook for adolescents/ students on cyber safety.

Nappinai, N. S. 2010. "Cyber Crime Law in India: Has Law Kept Pace with Engineering Trends-An Empirical Study." *J. Int'l Com. L. & Tech.* 5: 22.

Näsi, Matti, Atte Oksanen, Teo Keipi, and Pekka Räsänen. 2015. "Cybercrime victimization among young people: a multi-nation study." *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16, no. 2: 203-210.

Ngo, Fawn T., and Raymond Paternoster. 2011. "Cybercrime Victimization: An examination of Individual and Situational level factors." *International Journal of Cyber Criminology* 5, no. 1.

Nishtha Vishwakarma. (n.d.). https://www.medianama.com/author/nishtha-vishwakarma/)

Nykodym, Nick, Sonny Ariss, and Katarina Kurtz. 2008. "Computer addiction and cyber crime." *Journal of Leadership, Accountability and Ethics*: 78.

Öğütçü, Gizem, Özlem Müge Testik, and Oumout Chouseinoglou. 2016. "Analysis of personal information security behavior and awareness." *Computers & Security* 56: 83-93.

da Silva Pereira, Filipa, Marlene Alexandra Veloso de Matos, and Álvaro Miguel do Céu Gramaxo Oliveira. 2015. "Cyber-crimes against adolescents: Bridges between a psychological and a design approach." In *Handbook of research on digital crime, cyberspace security, and information assurance*, pp. 211-230. IGI Global.

Roberts, Lynne D. 2009. "Cyber-victimization." In *Handbook of research on technoethics*, pp. 575-592. IGI Global.

Shoukat, Saba, and Adil Bashir. 2018. "Cyber Crime-Techniques, Prevention and Cyber Insurance." *International Journal of Computing and Network Technology* 6, no. 01 : 23-26.

Statista,2019. Choice Reviews Online, https://www.statista.com/topics/5054/cybercrime inindia/

Subrahmanyam, Kaveri, David Smahel, and Patricia Greenfield. 2006. "Connecting developmental constructions to the Internet: Identity presentation and sexual exploration in online teen chat rooms." *Developmental psychology* 42, no. 3: 395.

Sukhai, N. B. 2004, October. Hacking and cybercrime. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 128-132).

The Hindu BusinessLine, February 09, 2018. Over 53,000 cybersecurity incidents observed in 2017, Info-tech, New Delhi. https://www.thehindubusinessline.com/info-tech.

Underwood, Marion K., and Samuel E. Ehrenreich. 2017. "The power and the pain of adolescents' digital communication: Cyber victimization and the perils of lurking." *American Psychologist* 72, no. 2: 144.

Weulen Kranenbarg, Marleen, Thomas J. Holt, and Jean-Louis Van Gelder. 2019. "Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap." *Deviant Behavior* 40, no. 1: 40-55.