International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 12 Issue 2, Mar.-Apr, 2024, Impact Factor: 8.376

Impact of cybercrime on Youth

Purvi Sancheti

Bharati Vidyapeeth Deemed To Be University, New Law College Pune

ABSTRACT

Cybercrime has become an increasing issue in today's digital age, particularly among the youth demographic. With the widespread use of technology and the internet, young people are increasingly exposed to various types of cybercrimes such as hacking, identity theft, online harassment, and cyberbullying. These criminal activities can have wide-ranging impacts on the lives of young individuals, including psychological distress, compromised personal information, and even legal consequences. This study intends to investigate how cybercrime affects young people and to increase public awareness of the need for practical solutions to this expanding issue.The abstract serves asa summary of the research on cybercrime, providing a comprehensive overview of its content and main arguments. This research aims to capture the reader's interest while also providing essential information about the research scope and purpose. In the context of cybercrime, the abstract would highlight the rising prevalence of digital offenses, the challenges they pose to law enforcement agencies and individuals, and the critical role of technology in this criminal landscape. Additionally, the abstract could touch upon the importance of understanding cybercrime from a multidisciplinary perspective, encompassing legal, technological, and societal dimensions. By presenting an abstract at the beginning of the research, readers can quickly assess its relevance to their interests, enabling them to decide whether to continue reading and explore this complex and rapidly evolving field further.

INTRODUCTION

Cybercrime refers to criminal activities conducted through the use of digital technology. With the increasing reliance on the internet and digital devices, cybercrime has become a significant threat to individuals, organizations, and governments worldwide. This research aims to provide an overview of cybercrime, its impact on society, and the challenges it presents for law enforcement agencies. By understanding the nature and scope of cybercrime, strategies can be developed to prevent and combat these criminal activities effectively.

The rapid advancements in technology and the increasing reliance on the internet and computer systems have contributed to the rise of cybercrime. The young generation is mostly evolving in the gaming world, and the internet world and losing interest in the real world. One of the most common reasons for cybercrime is economic problems. The Crimes are happening because people are choosing the wrong way to produce the economy through fraud, cheating, and threatening the young generation**. As a whole, during the years 2015-2022, a staggering 14.5k young victims affected by cybercrime were reported by the FBI. And that gave a total figure of 2.9 million in terms of financial losses for such crimes**.[1]**2022 saw an increase in cybercrime against children. According to the FBI Internet Crime Center reports (2015-2022), there were nearly 20% more child victims of cybercrime in 2022 than the year prior. To put this into perspective, 7 children per day faced online exploitation in 2022**.[2] Cybercrime is affecting individual life as well as their families. So by the growing concern,the UNICEF commissioned the **Child Online Protection in India Report**[3]to better understand online risks faced by children, identify gaps in legislation, ensure the removal of harmful materials, support investigation, and law enforcement, and identify services for victims of online exploitation and abuse.

Cyberbullying is something which is the main crime that is not just affecting youngsters, or females but also affects the LGBTQ community as well, who takea stand for themselves on social media platforms but always face these bullies. Along

[1]https://www.digitalinformationworld.com/2023/05/cybercrime-against-children-is-on-rise.html#:~:text=As%20a%20whole%2C%20during%20the%20years%202015-2022%2C%20a,in%20terms%20of%20financial%20losses%20for%20such%20crimes
[2]https://surfshark.com/research/chart/cybercrime-against-children
[3]https://www.icmec.org/child-online-protection-in-india/

with encountering societal bullying, this community also faced the tough reality of being victims of cyberbullying in their everyday lives.

DEFINITION &CATEGORY OF CYBERCRIME

In arrange to get the effect of cybercrime on youth, it is imperative to have a clear definition and understanding of what cybercrime involves. Cybercrime alludes to criminal exercises that are conducted through the utilization of computers or the web (Brenner, Susan W.)[4] These violations can take different shapes and target people, organizations, or indeed governments.There are various types and categories of cybercrime, that are affecting many people and mainly the youth of the country.

1. **Individual**: This category covers a wide range of online crimes committed against an individual, such as identity theft, child pornography, and cyberstalking.

2. **Property**: As more corporate operations shift online, one of the most lucrative and prevalent forms of cybercrime is the theft of data and intellectual property. This can include sophisticated spear phishing attacks that use impersonation to request cash, phishing scams that steal credit card numbers and personal information, and ransomware attacks that aim to steal an organization's files and demand payment in exchange for returning them.

3. **Government**: Targeting the trade secrets and vital infrastructure of another nation, this type of cybercrime frequently involves state-sponsored attackers and cyber terrorists. Propaganda and false information are among the attacks.

Now, as we know cybercrime is all related tocomputers, the internet, and networks. The online system attracts people to engage in this kind of crime. Two types of categories tell us about computer crime, which are:

1**. Computer as a target or computer as a tool**: This mostly addresses theft and fraud, with the use of malware, hacking, and phishing serving as the best examples of how computers can be targets.

2. **Computer as a weapon**: Denial-of-service (DoS) attacks are essentially launched using this.

TYPES OF CYBERCRIME AND THEIR IMPACT

Cybercrime covers a wide range of criminal activities involving various digital platforms and technologies. Many types of cybercrime need to be addressed, from email and social media scams to phishing scams and ransomware attacks. Although there are someoverlaps. A few common sorts of cybercrime incorporate hacking, personality robbery, phishing, cyberbullying, and online extortion.

1. **Hacking** includes unauthorized get to computer frameworks or systems with the deliberate of taking or controlling information.

2. **Personality robbery** happens when somebody unlawfully gets another person's individual data to commit false exercises.

3. **Cyberbullying** is repeated behavior, aimed at scaring, angering, or shaming those who are targeted. Examples include: spreading lies about or posting embarrassing photos or videos of someone on social media, and sending hurtful, abusive, or threatening messages, images, or videos via messaging platforms.[5]

4. **Online extortion** includes a wide extend of illicit exercises, such as credit card extortion, online tricks, and false online barters.

5. **Email Scams:** Fraud schemes that take many forms. Fake emails mislead recipients, while social engineering techniques trick people into revealing information such as credit card numbers or handing over money to the attacker.

[4]https://ecommons.udayton.edu/cgi/viewcontent.cgi?article=1023&context=law_fac_pub
[5]https://www.unicef.org/end-violence/how-to-stop-cyberbullying

6**. Phishing Scams**:this involves deceptive communications to trick victims into downloading harmful software visiting links to websites, or disclosing sensitive personal information. Phishing scams can take the form of emails posing as correspondence from well-known companies, banks, governments, or social media platforms.

7.**Social media fraud:** Social media fraud is the use of websites and apps such as Facebook, Instagram, TikTok, and Twitter to trick and con people. False internet stores, impersonation scams, social engineering attacks, and catfishing are a few examples. Fraudsters on social media frequently take advantage of people's trust, ignorance, and propensity to overshare personal information online.

8.**Banking fraud:** Financial Theft fraudulent actions directed towards financial institutions, their stakeholders, or clients. The most common outcomes of banking thefts are identity theft or large financial losses, and the attackers' methods frequently include social engineering and advanced computer techniques. Credit card fraud, ATM skimming, and online banking fraud are a few examples.

9. **Malware and Ransomware**: Malware is a highly common software attack designed to introduce viruses, trojans, or spyware into computer systems to manipulate and destroy them. Ransomware is a kind of malware attack where the victims' vital data is encrypted and a ransom demand is made in exchange for the decryption key needed to unlock the data.
These are some common types of cybercrime. By understanding these distinctive sorts of cybercrime, we will better comprehend the potential dangers and impacts they may have on the youth.

IMPACT ON YOUTH

Cybernetic being the most common and highly practiced mode of Communication all over the world whether urban or rural, whether young or old.Online social networking through emails,instant messaging, and video conferencing are all the ways where we find Cybernetthe most prominent mode.Although being variably used it showcases the pros and cons. Every age group is excessively indulged in using social media.Teenagers are now occupied with being online all thetimeand assuming it isa friendly sphere as it is fictitious as the confident platform to be themselves but they are sometimes trapped in it. Teenagers are getting distracted and bewildered by the way they interact through social media. Their dialect is way more gabble and compressed.Today's youth is busy with social networking as they consider it as a friendly network to be in touch and connected through far and near ones.Cybercrime also has had a significant impact on individuals and society as a whole. One major consequence of cybercrime is the loss of financial resources. According to, the global cost of cybercrime was estimated to be $1.5 trillion in 2018, and this number is expected to rise in the coming years. The financial implications of cybercrime extend beyond the immediate victims, as businesses and governments also suffer significant financial losses due to data breaches and theft. Furthermore, cybercrime has a profound effect on personal privacy and security. Individuals are increasingly concerned about the vulnerability of their personal information and the potential misuse of their data. This has led to a loss of trust in online platforms and a reluctance to engage in e-commerce and other online activities. In addition, cybercrime can have serious societal consequences, such as the spread of disinformation and the manipulation of public opinion. For instance, the interference of foreign actors in elections through cyber means has become a major concern in recent years. Therefore, it is clear that cybercrime has far-reaching effects on both individuals and society as a whole.

NEGATIVE EFFECT OF CYBERCRIME ON YOUTH

Cybercrime has detrimental effects on youth, affecting their emotional, psychological, and social well-being. One of the negative impacts is the increase in cyberbullying, where individuals are harassed, intimidated, and targeted online. According to a study conducted by the National Institutes of Health, cyberbullying has been linked to increased levels of depression and anxiety among victims (Pravin Dullur, J. Joseph, Antonio Mendoza Diaz, P. Lin, R. Jairam, Rhian Davies, A. Masi, B. Shulruf, V. Eapen)[6]. Additionally, the exposure to explicit and violent content through cybercrime contributes toruthlessand aggressive behavior.

It has been found that youth who are frequently exposed to violent online content are more likely to engage in aggressive behaviors themselves. The negative effects also extend to the personal and social lives of young individuals, as cybercrime can lead to isolation, strained relationships, and a decrease in self-esteem. The perpetual fear of being victimized online

[6]https://www.nih.gov/news-events/news-releases/depression-high-among-youth-victims-school-cyber-bullying-nih-researchers-report#:~:text=Unlike%20traditional%20forms%20of%20bullying%2C%20youth%20who%20are,by%20researchers%20at%20the%20National%20Institutes%20of%20Health.

creates a sense of insecurity and vulnerability, causing youth to withdraw from social interactions both online and offline. It is imperative to address these negative effects by implementing effective preventive measures and promoting digital literacy among young individuals.

FUTURE TRENDS IN CYBER CRIMES

"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm." **-Anna Maria Chavez**[7]

By this quote, Anna Maria Chavez says that cyberbullies can do such harm because of cybercrime, as there is no identity reveal of the accused, and by using the internet and various connections, it is easy to harm the victims online, but by the laws which are for online scams, fraud and much more crime, the accused will be more alert as the laws are very strong and cybercrime is something which was and which is an ongoing trend and that will be going to be in future with rapid speed. With the widespread use of technology, cybercrime has seen a significant increase among young individuals. Studies have shown that youth engagement in cybercrimes, such as hacking, identity theft, and online scams, has risen in recent years. Researchers attribute this trend to various factors, including easy access to technology, lack of digital literacy, and the anonymity provided by the internet. Moreover, it points out that the lack of consequences and lenient punishments for cybercrimes committed by minors often encourages their participation in such criminal activities. As this trend continues to escalate, it is crucial to understand and address the underlying factors driving youth involvement in cybercrimes.

STRATEGIES TO PREVENT AND COMBAT CYBERCRIMEAMONG YOUTH

One effective strategy to prevent and combat cybercrime among youth is through education and awareness programs. Educating young individuals about the dangers and consequences of engaging in cybercriminal activities can help deter them from participating in such behavior. These programs can include workshops, seminars, and presentations that provide information on the various forms of cybercrime, the legal repercussions, and the potential harm it can cause to themselves and others. Additionally, teaching young people about online safety, including the importance of strong passwords, avoiding sharing personal information online, and recognizing phishing attempts, can help them protect themselves from becoming victims of cybercrime. By increasing awareness and providing knowledge on cybersecurity, we can empower youth to make responsible choices and contribute to the prevention of cybercrime.By increasing awareness and providing knowledge on cybersecurity, we can empower youth to make responsible choices and contribute to the prevention of cybercrime. (Elshenraki, Hossam Nabil)[8].

Prevention and countermeasures play a critical role in mitigating the risks and impacts of cybercrime. Organizations and individuals must proactively implement measures to safeguard their systems and data from potential threats. One effective approach is to develop comprehensive cybersecurity policies and procedures that outline best practices for maintaining the security and integrity of information systems. These policies should address areas such as access control, encryption, regular system updates, and employee training on safe online practices. Additionally, the use of robust antivirus and firewall software is essential for detecting and preventing malware attacks. Furthermore, organizations should establish incident response plans to effectively handle and contain cyber incidents when they occur. By adopting a multi-layered approach to cybersecurity, organizations and individuals can significantly reduce the likelihood of falling victim to cybercrime.

LEGISLATION RELATED TO CYBERCRIME IN INDIA

The major substantive criminal law is the Indian Penal Code a total code that bargains with all the offenses counting cyber wrongdoings. Hence, this routine criminal law is adequate to bargain with all sorts of wrongdoings counting cyber wrongdoings. India ordered the Data Innovation Act, 2000 fundamentally to direct e-commerce. The relevant sections related to Cybercrime are:

- **Section 354D of the IPC** This section addresses both offline and online stalking.An offender faces a maximum sentence of three years in jail for first offenses and five years for second offenses.[9]

[7]https://gatlabs.com/education/blog/how-to-stop-cyberbullying-at-your-school-in-5-steps/#:~:text=%E2%80%9CCyberbullies%20can%20hide%20behind%20a,experienced%20some%20form%20of%20cyberbullying.
[8]"Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities" IGI Global, 2020-12-11 by Elshenraki, Hossam Nabil
[9] Section 354D was introduced into the Indian Penal CodeIns. by Act 13 of 2013, s. 7 (w.e.f. 3-2-2013).

- **Section 419 of the IPC:** This section addresses fraud, including password theft for impersonation and data collection for personal gain, as well as email phishing.A person who deceives another person by persona manipulation faces imprisonment of any kind for up to three years, a fine, or both.[10]
- **Section 465:**The punishment for forgery, email spoofing, preparation of false documents, etc., are dealt with in Section 465 of the IPC. It states that anyone who commits forgery should be punished with imprisonment extending to two years, a fine, or both.[11]
- **Section 468 of the IPC**: Whoever commits forgery, intending that the[12] [document or electronic record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.
- **Section 509 of the IPC:**A person faces up to three years of simple imprisonment and a fine if they purposefully attempt to offend a woman's modesty by using derogatory language, gestures, or acts, or by invading her private.[13]

Sections related to Cybercrime under the Information Technology Act are:-

- **Section 66 (A–F)** this section deals with penalties for computer-related offenses, such as sending offensive messages, stealing resources from another person's computer, identity theft, impersonation, cheating, invasion of privacy, and cyberterrorism. A fine of up to five lakhs rupees, three years in prison, or both could be the possible penalties.[14]
- **Section 67 (A-B) of the Information Technology Act:** pertains to the penalties imposed on the dissemination of pornographic content, including sexually explicit acts, in electronic format. A fine of up to five lakh rupees and three years in prison are the penalties for first-time offenders. The maximum sentence for someone found guilty a second time is five years in prison.[15]

CASE LAWS

1. **Avnish Bajaj v. State (NCT) of Delhi**
   Facts: Avnish Bajaj, the CEO of Bazee.com was arrested under Section 67 of the IT Act for the broadcasting of cyber pornography. Someone else had sold copies of a CD containing pornographic material through the bazee.com website.

   Decision: The Court noted that Mr. Bajaj was nowhere involved in the broadcasting of pornographic material. Also, the pornographic material could not be viewed on the Bazee.com website. But Bazee.com receives a commission from the sales and earns revenue for advertisements carried on via its web pages.

   The Court further observed that the evidence collected indicates that the offence of cyber pornography cannot be attributed to Bazee.com but to some other person. The Court granted bail to Mr. Bajaj subject to the furnishing of 2 sureties Rs. 1 lakh each. However, the burden lies on the accused that he was merely the service provider and does not provide content.[16]

2. **SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra**
   Facts: In this case, Defendant Jogesh Kwatra was an employee of the plaintiff's company. He started sending derogatory, defamatory, vulgar, abusive, and filthy emails to his employers and to different subsidiaries of the said company all over the world to defame the company and its Managing Director Mr. R K Malhotra. In the investigations, it was found that the email originated from a Cyber Cafe in New Delhi. The Cybercafé attendant identified the defendant during the inquiry. On 11 May 2011, Defendant was terminated of the services by the plaintiff.

[10] Section 419 of Indian Penal Code gives punishment for cheating by personation.
[11]https://www.freelaw.in/legalarticles/Punishments-for-Cyber-Crime-Under-Indian-Constitution#:~:text=Section%2066%20(A%2DF)%3A%20This,of%20up%20to%205%20lakhs
[12]Subs. by Act 21 of 2000, s. 91 and the First Sch., for "document forget" (w.e.f. 17-10-2000)
[13] Subs. by Act 13 of 2013, s. 10, for "shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both" (w.e.f. 3-2-2013
[14]https://www.freelaw.in/legalarticles/Punishments-for-Cyber-Crime-Under-Indian-Constitution#:~:text=Section%2066%20(A%2DF)%3A%20This,of%20up%20to%205%20lakhs
[15]Section 67(A-B) of the Information Technology Act, 2000
[16](2008) 150 DLT 769

Decision: The plaintiffs are not entitled to relief of perpetual injunction as prayed because the court did not qualify as certified evidence under section 65B of the Indian Evidence Act. Due to the absence of direct evidence that it was the defendant who was sending these emails, the court was not in a position to accept even the strongest evidence. The court also restrained the defendant from publishing, or transmitting any information in Cyberspace which is derogatory or abusive of the plaintiffs.[17]

ANALYSIS & CONCLUSION

As technology continues to advance and society becomes increasingly dependent on digital platforms, the threat of cybercrime is expected to grow as well. Therefore, it is imperative for individuals, businesses, and governments to remain vigilant and proactive in combating cybercrime through various measures such as robust cybersecurity systems, public awareness campaigns, and international cooperation. Only by collectively addressing this complex and ever-evolving issue can we hope to mitigate the damaging effects of cybercrime and protect our digital lives.

In conclusion, cybercrime has become a significant issue for youth, affecting their well-being, personal development, and future prospects. The prevalence of cyberbullying, online harassment, and identity theft has inflicted immense emotional and psychological damage on young individuals. Furthermore, engagement in cybercriminal activities can lead to legal consequences and hinder educational and employment opportunities for youth. It is crucial for parents, educators, and policymakers to collaborate in implementing comprehensive preventive measures, such as education on digital citizenship, promoting responsible internet use, and fostering safe online environments for young individuals.

[17]CM APPL. No. 33474 of 2016