

	Journal Homepage: - www.journalijar.com INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR) Article DOI: 10.21474/IJAR01/ 21317 DOI URL: http://dx.doi.org/10.21474/IJAR01/ 21317	
---	--	---

RESEARCH ARTICLE

The National Conference on Innovative Trends in Modern Business Environment (ITMBE 2025) , DPG
Institute of Technology and Management (DPGIM) Gurugram

SOCIAL MEDIA: THE UNSEEN RISKS OF CYBERCRIMES

Manjeet Singh¹, Dr. Annapurna Metta² and Dr. Prof. Satyendra Patnaik³

1. Research Scholar Amity Business School, Amity University Chhattisgarh and Manager Software Engineering, Clear Trail Technologies Pvt Ltd. SDF No. K-12, NSEZ, Noida, UP 201305

<https://orcid.org/0009-0000-2157-1388>.

2. Assistant Professor, Amity Business School, Amity University Chhattisgarh <https://orcid.org/0009-0009-2015-6815>.

3. Professor & Dean, JSS University Noida: Noida, Uttar Pradesh, INDIA <https://orcid.org/0000-0002-1296-3387>.

Manuscript Info

Abstract

Key words:-

Cybercrime, Cyber bullying, social media, Harassment

Cybercrime has been on the increase in recent years. In particular, the rise in popularity of social media has made online harassment and cyber bullying more important and pervasive. People are increasingly relying on social media for things like networking and access to entertainment. There is a lot of uncertainty regarding the effects on users and how they might safeguard themselves in this uncharted terrain. Some types of crime have become more common among social media's user bases. Several details about victims make them more appealing to their abusers. In certain cases, criminal acts will have overlapping effects. It makes us wonder whether social media sites should be responsible for their users safety. Similarly, how can people stop themselves from being cyberbullied or victims of online harassment? The information acquired is freely available to the public and has been sourced from official institutions and dependable groups.

"© 2025 by the Author(s). Published by IJAR under CC BY 4.0. Unrestricted use allowed with credit to the author."

Introduction:-

The widespread use of social media has made it impossible to imagine modern life without it. The term "social media networking" refers to an online community where members may interact and exchange various forms of media such as text, music, video, photos, graphs, and animations. The contents may be regarded in terms of volume, diversity, velocity, truthfulness, volatility, quality, discovery, and dogmatism and are all part of the cloud-based big data contents. As of March 2019, there were 4,168,461,500 people online, or 50.08 percent of the global population. As of current year, there are an estimated 2.77 billion social media networking users globally, or 35.9% of the world's population, and by 2021, that figure is projected to rise to 3.02 billion. There is a wide range of ages, nationalities, faiths, social attitudes, and habits, as well as gadgets used to access social media among these individuals. Considering the widespread usage of social networking sites, it's no surprise that people of all walks of life go there to connect with old friends, make new ones, and broadcast their everyday exploits to the people they care about. People from all areas of life are signing up for these social networking sites, and their information is being stored in the cloud. The habits we've developed over time in the internet environment have implications for our personal safety and security. An surge in the volume, pace, diversity, and validity of data in social media networking has recently emerged as a major obstacle. This has given rise to a number of concerns,

including those connected to privacy and security. Twitter, Facebook, and other social media sites, blogs, content sharing (such as photographs and videos), and mobile texting are just a few of the many methods individuals use today to communicate and share information in this "information age."

Social Media and Cybercrime

The National White Collar Crime Centre's (NW3C) "Criminal Usage of Social Media" white paper notes that the prevalence of criminal activity on social media has increased over the last few years, altering the nature of online communication. Facebook, Twitter, and YouTube attract hundreds of millions of unique visitors each month. People are able to easily and quickly get in touch with one another using these websites. People use social media to connect with one another, and organizations utilize it to spread news and find new personnel. Figure 1.1 displays the social media user statistics collected by Statista as of January 2019.

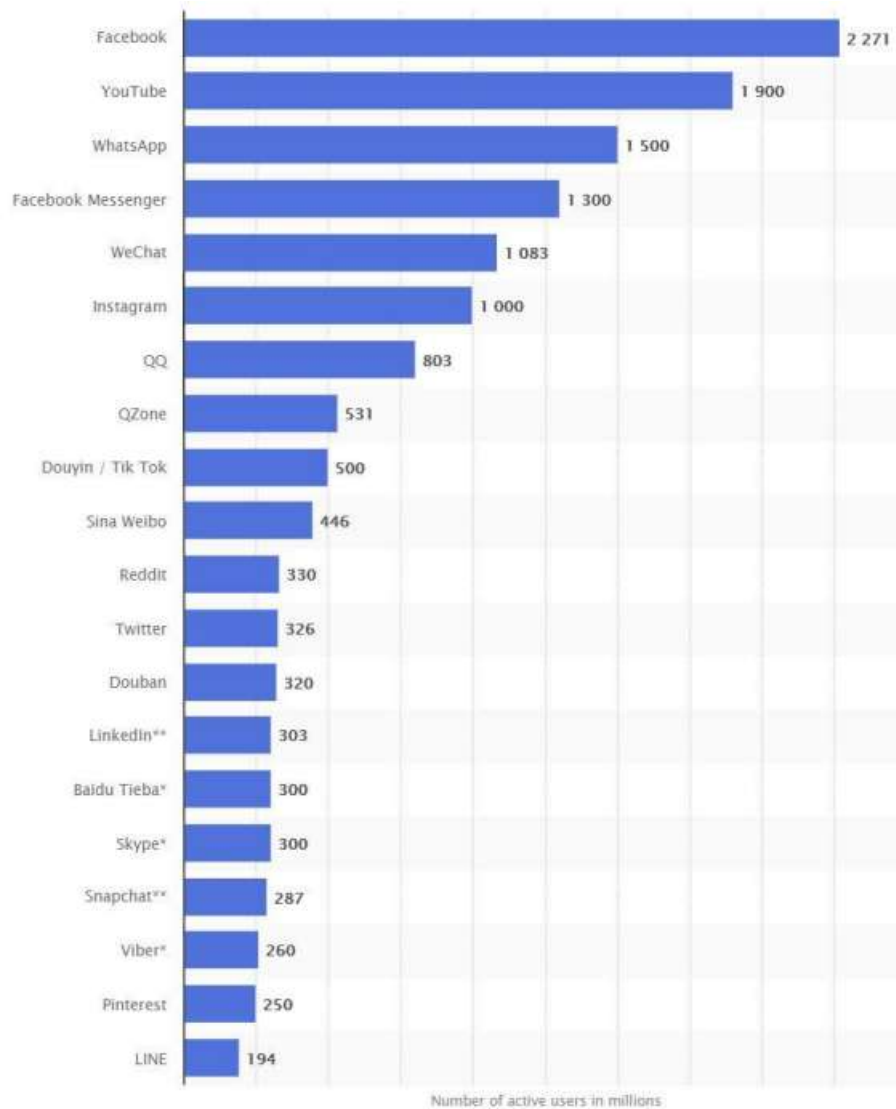


Fig. 1.1 Social media users

Problematic Social Media Use

Research on the mental, cultural, and social impacts of social media has exploded in recent years. Previous studies on this subject provide a more complex picture of the effects of social media. Examples include enhanced life happiness, social trust, and political involvement, all of which have been linked to social media usage in a number of studies. Use that satisfies people's socioemotional needs, such as sharing feelings and obtaining social support on social media platforms, is generally cited as the cause of the beneficial impacts seen.

Yet, there is a countervailing body of research that links social media usage to a variety of unfavorable outcomes, such as stress, anxiety, and diminished sense of self-worth. It's also typical to read about unfavorable results including sadness, lower subjective well-being, and more isolation. Social comparison and FOMO are often cited as explanations for the unintended consequences of

social media usage. In general, it seems that the most harmful effect on users' health and well-being is caused by the sort of usage that does not promote interpersonal interaction.

Researchers believe that certain subsets of users are at a higher risk of suffering unfavorable effects due to social media usage, despite the fact that past research on the topic has given somewhat inconsistent findings. In particular, the researchers have highlighted the fact that there is a subset of the population that struggles to limit their time spent on social media. Thus, in order to measure excessive usage, new notions like problematic social media use and social networking addiction have emerged. The widely used idea of problematic social media usage (PSMU) is used in this study. Consistently negative consequences in numerous aspects of life are predicted by PSMU, in contrast to evidence of social media usage in general, including lower subjective well-being, sadness, and loneliness.

Just a small number of research have examined whether or not PSMU increases a person's likelihood of being a victim of cybercrime. Both an international survey of young people and a study of Spanish teenagers discovered that PSMU is significantly and consistently related to becoming the target of cyber bullying. Another research of Italian teenagers discovered that cyber bullying was related to the amount of Instagram followers one had. Previous research had obvious gaps since it had a juvenile population and dealt with issues like cyber bullying and harassment. Thus, the findings cannot be extrapolated to adult populations or used to predict other types of cybercrime victimization with any degree of certainty. Notwithstanding this, there are several fundamental presumptions concerning cybercrime victims that must be taken into account.

Theories of Cybercrime Prevalence, Prevention, and Exposure

Cybercrime is a term borrowed from criminology to describe a wide range of unlawful behaviors committed by electronic means (computers, smart phones, etc.). Cybercrime, as a term, is used to explain a broad variety of criminal occurrences, from the victimization of an individual to the manipulation of a whole community. In this investigation, we use the term "cybercrime" to refer to online acts of illegality and injury committed against others, with an emphasis on victims' own accounts of being targeted by cybercriminals. As a result, we avoid discussing whether or not respondents really reported being victims of crime.

Slander, hacking, malware, online fraud, and cyber bullying are some of the most frequent forms of cybercrime in Finland and other European nations. Previous criminological study has struggled to provide precise figures of cybercrime victims, however estimates place that number anywhere from 1 to 15 percent of the European population. Similarly, it's hard to put a number on how often illegal action is facilitated by social media. But, as more and more of our online conversations take place on social media, it stands to reason that more and more people will become victims of cybercrime while using these sites. Previous studies have shown that social media is often used for criminal activities such as identity theft, cyber bullying, hate speech, and stalking. Previous research has mostly focused on cyber victimization among youth and young adults because of their heightened vulnerability.

Routine activity theory is a popular theoretical paradigm for understanding victimization (RAT). According to RAT, regular activities of social actors expose people to potentially harmful interactions with others and to unsafe environments. According on this idea, criminal activity is more likely to take place when the right time, place, and combination of offender motivation, victim characteristics, and available adult supervision all come together. RAT is similar to lifestyle-exposure theory (LET), which investigates how people's habits in various social settings make them vulnerable to abuse.

In this research, we combine RAT and LET to look at how the internet might encourage certain risky behaviors and personality types. All told, these theories simply accept as given the presence of motivated criminals and provide no explanation for why they commit crimes. Instead, we look at how everyday behaviors and a lack of a responsible guardian combine to increase one's risk of being a victim.

Several research have looked at how LET and RAT might help victims of cybercrime. Based on the findings, it seems that not all theoretical frameworks can be applied in the same way to online settings, and that some are more fruitful than others. For instance, while there has been a lot of debate about how to evaluate risk exposure, it is generally agreed that it is consistent with online victimization. In contrast, it is widely acknowledged to be more challenging to operationalize target attractiveness and lack of guardianship in the context of technology-mediated victimization.

Literature Review

Stošić, Lazar & Janković, Aleksandra (2022) In 2022, rumors on the internet claimed that bombs had been placed in schools and other public buildings around Serbia. These incidents have sparked a discussion over whether or not cybercrime authorities are prepared to effectively counteract threats. States have a greater responsibility to safeguard their people against cybercrime as the number of internet users rises. Recent instances have shown society's susceptibility to and danger from high-tech crime. The article examines statistics from the Ministry of Interior Affairs and examines the regulatory and administrative framework for fighting cybercrime. The goal of this article is to provide suggestions for improving cybercrime protection based on an examination of current laws and the institutional architecture in the India and several European nations. The report presents the steps implemented in other nations using both a normative and a comparative approach. The information was examined using descriptive statistics.

Conclusion: despite a robust regulatory framework, the battle against cybercrime is insufficient, largely due to a much too small number of workers in particular departments and divisions of the prosecutor's office and the police, especially considering the rising annual rate of cybercrime. Another risk is that many users are unaware of the potential threats posed by the internet. Thus, it will soon be necessary to focus more on teaching residents of all ages about the risks and forms of cybercrime.

Chuma Benard, Masese & Charles(2021) Because of the ease with which social media facilitates two-way connection, the volume of electronic discourse has expanded. Internet users run the danger of being attacked by cybercriminals wherever they go online. Cybercrime is the newest and most complex issue facing the Internet today. Computer fraud, unauthorized hacking, forgery, privacy invasion, online gambling, harmful content dissemination, phishing, computer viruses, prostitution impersonation, theft, espionage, copyright infringement, financial crimes, illegal product sales, pornography, intellectual property crime, e-mail spoofing, cyber defamation, and cyber stalking are all examples of cybercrime. The goals of the research were to identify the many types of social media-based cybercrime that exist and to investigate how these crimes affect the safety of social media platforms. A total of 132 participants were chosen from the study population at the selective universities. Respondents were chosen at random using a simple sampling process.

Biswal, Chandra & Pani, Dr. Subhendu (2020) Recently, the Internet has undergone rapid transformation across a wide spectrum of industries, from the realms of education and business to those of sports and entertainment. As a result, the internet has become the go-to source of information for everyone, including those who aren't very tech savvy. The benefits and drawbacks of internet usage are not without equal. Cyber-crime is the internet's worst drawback. Cybercrime is a growing problem that endangers everyone who uses the internet or a computer. As a result, governments, police forces, and intelligence agencies in a wide range of nations have become more reactive and stricter in the face of new cyber dangers and the proliferation of cybercrime. Governments have begun adopting measures to combat cybercrime of all kind, including international cyber threats, dark web activities, and so on. Governments worldwide, including India's, have established cyber units in police departments and are actively training officers to combat cybercrime. Our study primarily focuses on recent fraud and cybercrime events in India, as well as numerous cybercrime categories and potential remedies.

Nurse, Jason (2018) Victims of cybercrime can suffer more than the general public as a result of the crime. In this chapter, we examine cybercrimes against people in depth and in light of current events. It also delves into the human and psychological components that contribute to cybercriminals' success, as well as their motivation for launching such assaults. Cyberbullying, trolling, revenge pornography, hate crimes, and identity-related crimes like doxing and identity theft are all evaluated, as are hacking techniques like malware and cryptojacking as well as denial-of-service attacks. The chapter makes a case for why cybercrimes against people would persist in the absence of concentrated multidisciplinary efforts and provides a basic taxonomy of these crimes.

Dayalan, Muthu (2017) Cybercrime has emerged as a major threat to modern enterprises, particularly those that conduct their operations online. The government and traditional enterprises are also feeling the effects of this economic downturn. Cybercrime, often known as computer crime, is the commission of illicit acts using electronic means of communication and processing financial transactions. The internet is the primary driver of all of these events. The purpose of this study is to catalog the many ways in which cybercrime poses a risk to today's enterprises. The effects of cyber menace and the havoc it has wreaked around the globe are examined in this study. What are the most significant dangers that might cause severe damage to a business in a variety of ways? The article goes on to investigate the growing trend of cybercriminal gangs. What's more, they've been using an increasing number of sophisticated methods to steal from businesses in recent years. Businesses should reevaluate their security practices to better safeguard sensitive information in light of the findings of this research.

Methodology:-

All information comes from the aforementioned reliable sources. Statista, the Pew Research Center, and the IC3 are all mined for information on cyber bullying. It provides additional information regarding users' exposure to, beliefs about, and reactions to online harassment, as well as its repercussions on the victim. Both the Pew Research Center and the NCES collect statistics on cyber bullying. I'd also be keeping an eye out for things like account activity, account privatization, defensive measures taken on social media, and user complaints. The emphasis, though, will be on Facebook members. The economic losses from cybercrime on social media are also included in. The IC3 report contains this kind of information. Users of various social media platforms have varying perspectives on social media-related criminality. Users' responses to cyber bullying and online harassment varied widely, as did the severity of their encounters. Some people may alter their social media routines after being moved to do so by a recent occurrence.

Participants

Human subjects are not used in any way in my paper. Nonetheless, it does make use of data that is available to the public. The Internet Crime Center, a branch of the FBI dedicated to cybercrime, the Pew Research Center, a nonpartisan think tank that collects and disseminates information on a wide range of topics, Statista, a digital data platform used by businesses and industries around the world, and the National Center for Education Statistics (NCES), a federal organization within the Department of Education that provides stats and information on education.

Data Analysis

Information has been gathered and sorted such that it pertains to the paper's central theme. As was previously noted, the four groups were established to facilitate research on the link between cybercrime and social media. The study questions were informed by the selection of appropriate surveys and yearly reports. The presented statistics showed a correlation between social media and the rising tide of cyber bullying. Many users are becoming more aware of this problem, yet opinions on these crimes vary widely. People's opinions on whether social media sites should help safeguard their users and who should do so vary widely across the data. Differences in perspective across sexes and generations provide for fascinating comparisons. All the information has been compared to determine whether a link can be drawn. A narrative style will be used to display the data.

Results:-

The advent of social media introduces a new dynamic to the realm of cybercrime. Users may now do research on, and engage with, both known and unknown individuals. The scope of the online community is global rather than regional. Almost anybody may become a victim of crimes like cyber bullying and internet abuse. Users of social media platforms are particularly vulnerable to this trend; yet, responses vary widely.

Online Harassment

Harassment in the digital realm is not dissimilar to harassment in the real world. The setting is the only distinguishing factor. Several other forms of criminal behavior, such as cyber stalking, the leaving of upsetting or threatening messages, the posting of hate speech remarks, etc., are integral parts of this offence. According to the graph below from Statista, 44% of all internet users have experienced harassment of some kind, with 28% experiencing severe harassment.

Table 4.1 As of January 2020, what percentage of American adults who use the internet have experienced some kind of cyber bullying?

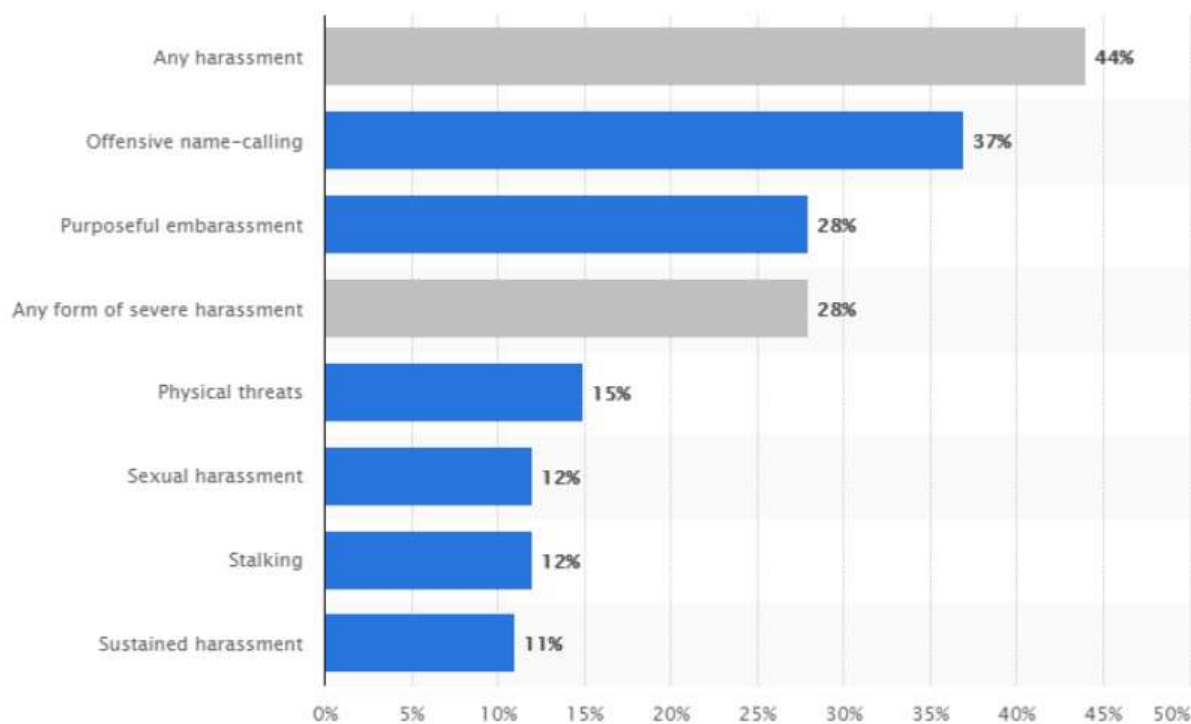
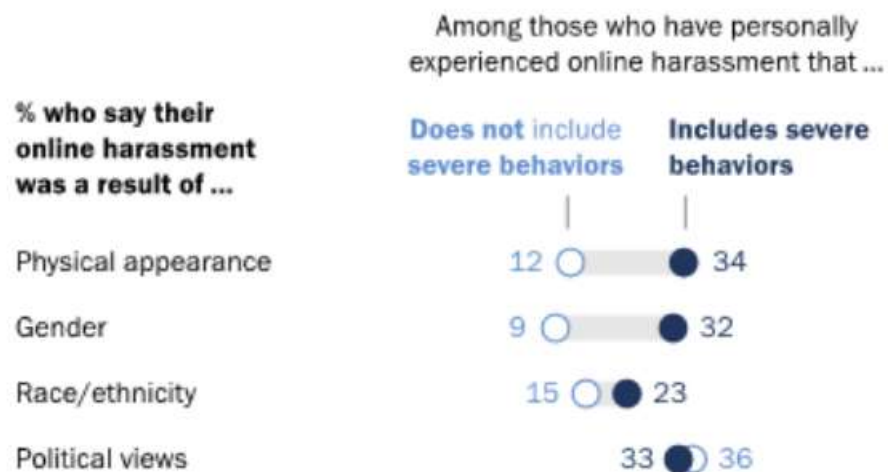


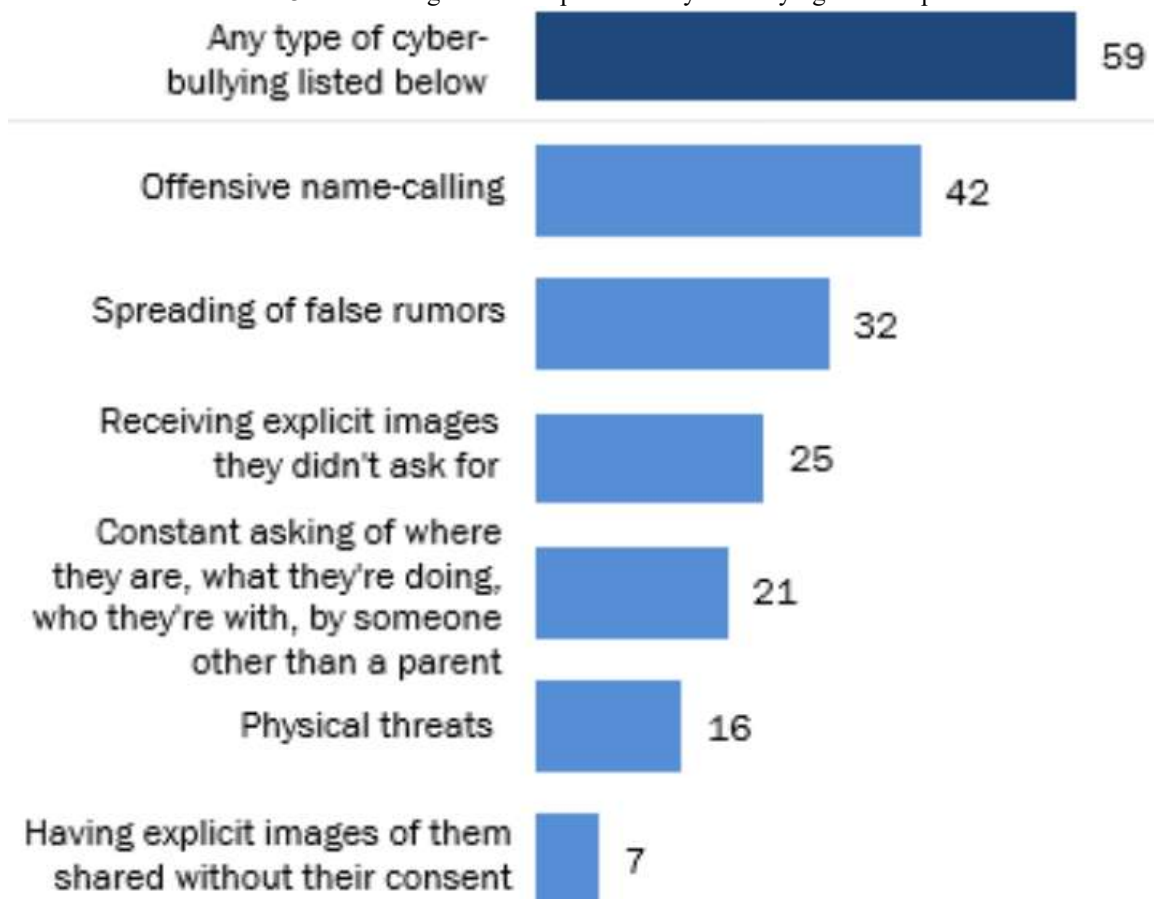
Table 4.2 Individuals who have experienced extreme kinds of cyberbullying



Cyber bullying

The NCES compiled data on instances of cyber bullying in the India. Since it is so easy to transition from conventional bullying to cyber bullying, this issue is rising rapidly. Several people equated cyber bullying with internet harassment. The victims' ages are what set these two cases apart. Children are disproportionately affected by cyber bullying, whereas adults are not. At least once a week, cyber bullying occurred throughout the 2017–18 school year. The National Center for Education Statistics found that cyber bullying occurs in 15 percent of all public schools. In contrast, this rate is 33.1% in middle schools and 30.2% in high schools.

Table 4.3 Most teenagers have experienced cyber bullying at some point

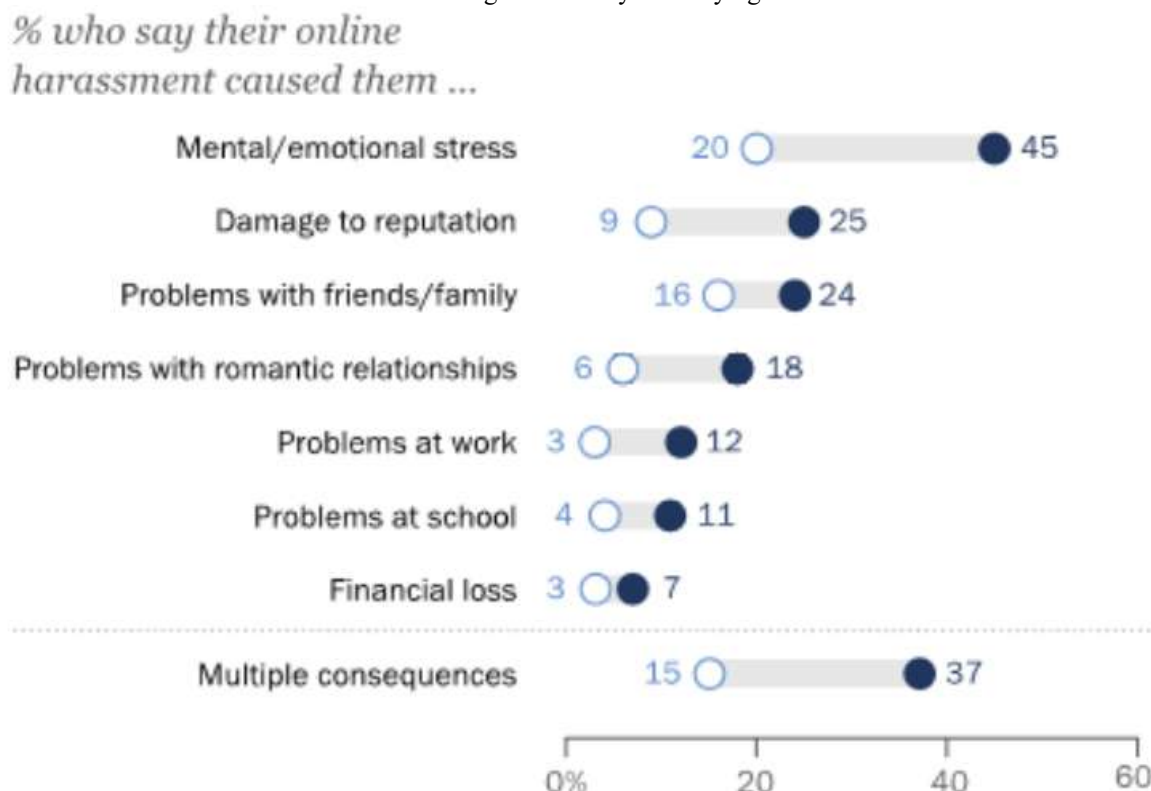


Total Cost Loss

The effects of cybercrime on victims and the economy may be long-lasting. This category of crime encompasses anything from petty theft to international terrorism. In this way, social media is just another avenue for criminal activity. According to the IC3, the average number of complaints per day in 2019 was above 1,200, with a total loss of \$3.5 billion. There were about 29,093

occurrences of social media-related crime that resulted in a total of \$78,775,408. There were 15,502 victims of offenses like harassment and threats of violence, resulting in a total cost of \$19,866,654.

Table 4.4 Who is claiming that their cyber bullying was the cause?



Conclusion:-

Offenders, it appears, will go after their victims regardless of how much is known about them. Nonetheless, there is a link between social media and online crimes. Online harassment is a symptom of a larger problem: a rise in crime, disproportionately affecting males. Interestingly, victims often opt to forget about what happened in these situations. As more and more individuals express their views, it seems that the use of profanity and assaults on personal attributes by complete strangers is becoming the norm. It is a symbol of the ambiguity around what constitutes free speech and the power that users' anonymity affords them to act viciously. Topical themes, such as politics, show how individuals prefer to act poorly against others despite their being no immediate repercussions and a greater likelihood that they will not confront the victims offline. Mob mentality is also applicable here since people who share similar values tend to act in lockstep with their peers.

Reference:-

1. Stošić, Lazar & Janković, Aleksandra. (2022). Cybercrime in the Republic of Serbia: Prevalence, Situation and Perspectives. *Kultura polisa*. 19. 82-99. 10.51738/Kpolisa2022.19.4r.82sj.
2. Chuma Benard, Masese & Charles, Masoud & Charo, Joel & Mgala, Mvurya. (2021). Cyber-Crimes Issues on Social Media Usage Among Higher Learning Institutions Students in Dar ES Salaam Region, Tanzania. *International Journal of Scientific Research in Science, Engineering and Technology*. 138-148. 10.32628/IJSRSET218418.
3. Biswal, Chandra & Pani, Dr. Subhendu. (2020). Cyber-Crime Prevention Methodology. 10.1002/9781119711629.ch14.
4. Nurse, Jason. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. 10.1093/oxfordhb/9780198812746.013.35.
5. Dayalan, Muthu. (2017). Cyber Risks, the Growing Threat. 2. 10.1726/IJNRD.17046.
6. C. Lekha and S. Prakasam, "Implementation Of Data Mining Techniques For Cyber Crime Detection," *International Journal of Engineering, Science and Mathematics*, vol. 7, no. 4, January 2018
7. X. Feng, A. Asante, E. Short and I. Abeykoon, "Cyberstalking Issues," in 2017 IEEE 15th Intl. Conf. on Dependable, Autonomic and Secure Computing, 15th Intl. Conf. on Pervasive Intelligence and Computing, 3rd Intl. Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 2017, pp. 373–376. <https://doi.org/10.1109/DASC-PiComDataCom-CyberSciTec.2017.78>
8. E. Spyrou and P. Mylonas, "A Survey of Geo-tagged Multimedia Content," in IFIP International Conference on Artificial Intelligence Applications and Innovations, Paphos, pp. 126–135, 2014. https://doi.org/10.1007/978-3-662-44722-2_14

9. G. Suresh and R. J. Raj, "A Study on Credit Card Fraud Detection using Data Mining Techniques," International Journal of Data Mining Techniques and Applications, vol. 7, no. 1, pp. 21–24, June 2018.
10. X. Li, J. Chen, Z. Lin, L. Zhang, Z. Wang, M. Zhou and W. Xie, "A Mining Approach to Obtain the Software Vulnerability Characteristics," in Fifth International Conference on Advanced Cloud and Big Data (CBD), Shanghai, 2017.
<https://doi.org/10.1109/CBD.2017.58>