ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2022; 8(10): 201-204
www.allresearchjournal.com
Received: 19-08-2022
Accepted: 23-09-2022

Apoorv Singh
BA. LL.B (H), 5th Year, Institute of Legal Studies and Research, GLA University, Bharthia, Uttar Pradesh, India

Tushar Dixit
BA. LL.B (H), 5th Year, Institute of Legal Studies and Research, GLA University, Bharthia, Uttar Pradesh, India

Corresponding Author:
Apoorv Singh
BA. LL.B (H), 5th Year, Institute of Legal Studies and Research, GLA University, Bharthia, Uttar Pradesh, India

An overview of cyber crimes: A major threat to society and legal remedies to it around the world

Apoorv Singh and Tushar Dixit

DOI: https://doi.org/10.22271/allresearch.2022.v8.i10c.10221

Abstract
The internet poses a particularly challenging balancing act between criminal activity and allowed use due to its flexible proposed system with stress on ease of communication. A more favourable atmosphere for it in an upsurge in cybercrimes has been generated by the emergence of several social media platforms. This project was inspired by the vagueness of what exactly defines cybercrime due to a lack of agreement on what should be included in the calculation. This essay outlines the various methods that cyber criminals use to commit crimes on various social media outlets. Since there are no procedures in place to verify identification, this presents a problem. The goal of this essay is to ascertain the degree to which the exponential rise in social media use has aided in cybercrime. We used the doctrinal approach of legal research for this essay. The research found that social media platforms' accessibility, affordability, and ease of use have made it incredibly an desirable location for business. The study concludes that making people aware of such crimes can significantly reduce the threat of cybercrime. The article finishes by underlining the necessity of creating a legislative framework specific to cybercrime to deter social media cybercrimes. It suggests among many people believe that revealing personal information or data on social media sites should be avoided.

Keywords: Cyber bullying, cyber-crimes, social media, legal guidance

1. Introduction
Daily communications on social media sites number in the millions. Social media has successfully created a huge and powerful platform that serves as both a playground for cyber criminals as well as for the exchange of ideas and images. Social media sites contain a wealth of personal information. People seem comfortable disclosing private information on social networking sites. However, if care is not taken, personal information including a person's name, phone number, address, etc. Even a person's location can be taken and utilised to steal their identity or create fake identities. However, the fact that social networking is not entirely terrible is important to highlight. It provides a means of staying in touch with loved ones and friends. It provides a platform for sales, advertising, and instantaneous access to a larger audience. Professional LinkedIn and other social media sites are crucial for staying up to date on business news. Social media sites are now quickly ingrained in people's daily lives, with millions of people using them to network social media platforms are used by people. Despite having many advantages, social media posed a significant danger that could have negative effects. Social media has been used by cyber criminals as a channel for executing their illicit behaviour. In a society where users of various social media platforms often divulge their personal information. They serve as a lure for cyber criminals to obtain the information. They demand. The use of computers and internet to commit cybercrimes such as stealing other people's locating victims and personal information as well as identities. Unfortunately, social media has favoured method for online thieves to take out their evil deeds. Therefore, it is not surprising that the internet and social media has resulted in numerous criminal behaviour vectors. What is simple a phone or computer, internet connectivity, and criminal intent are required to commit a crime. The internet gives everyone the ability to transmit false information and commercially sensitive information, which could be harmful. As a result, social media service providers must monitor and manage content platforms.

2. Cybercrime: What Is It

Cybercrime, also referred to as crime, involves the use of a pc as a tool to further illegal activities like fraud, the trafficking of child pornography and other intellectual property, identity theft, and privacy violations. Additionally, it is described as a "umbrella" word for a variety of crimes that occur on internet or where computer is used as a weapon or a target in an attack. A cybercrime is one that is a crime that can only be perpetrated through the use of a computer, computer networks, or another information source IT for communications. Cyberspace enabled offences are those that are made possible by our ever-expanding technology capabilities, such as online fraud, the sale of illegal products like narcotics or firearms online, and the exploitation and abuse of children online. Criminal activity online also affects people's privacy. The word "cybercrime" is used by the Council of Europe's Cybercrime Treaty to relate to offences ranging from data theft to copyright violations, interaction, and criminal conduct.

Zeriar-Geese, however, contends that a larger definition that include offences like fraud, unauthorised access, child pornography, and cyber-stalking is necessary. Fraud, forgery, and illegal access are all considered forms of cybercrime under the United Nations Manual on the Prevention and Control of Computer Related Crimes.

Therefore, it is important to note that there isn't a general title for such software and tools which are employed when committing specific internet crimes. Despite the apparent familiarity and acceptance of there are radically differing interpretations of what cybercrime is, to use the phrase. This absence of widely acknowledged definition is difficult since it has an impact on every aspect of prevention and correction.

3. Cybercrimes on Social Media: Types

Hacking: is the phrase used to describe an intrusion made by a third party who gained access to your computer system without your consent. It also refers to unauthorised access to any computer or digital device made through different social media sites. Computer hackers are essentially those who engage in the act of hacking. People who are proficient with computers frequently abuse their expertise for nefarious motives Hackers breach networks to steal financial data from businesses and personal banking information from individual’s data, etc. They also attempt to alter processes so that they can carry out jobs according to their whims and fancies. Hackers also use social media to communicate with people. Whenever the visitors click on each of those separate links, they are then linked by thieves. Hackers use internet communities extensively, sharing information and resources, executing recruitment and coordinating tasks, etc.

Cyber stalking: This is frequently done by horning or peeping into the private lives of the person to cause distress, tension, concern, and anxiety. The act of pursuing, harassing, or contacting someone on an electronic media used in an uninvited manner. Cyber stalking cause’s mental distress as a result. It is known as a "mental offence" or even a "psychological statutory offence." An online stalker harass his or her victims since the anonymity of the cyber stalker gives them an advantage. This privacy gives a variety of techniques, including the use of dated version of computer software termed "mail daemons" or completely fraudulent user information may be used when registering online on social media networks A cyber stalker may also send obscene email threats, including those containing explicit content like naked photos or videos of abuse or obscenity, and they may leave harsh remarks online that the victim may find annoying. Feeling emotionally disturbed and violated.

Phishing: is a method of obtaining private data, including credit card info and username and password combination by pretending to be a reliable company. Phishing is frequently practised by sending a bogus email. In phishing, the hackers impersonate well-known websites by using their names and logos their sufferers. The email's usage of images and web domains is eerily similar to real ones, but they are made to direct you to humorous websites. Phishing is not always conducted through email or websites, though. Voice phishing, also known as vislung, involves calling victims while using a false identity to trick them into thinking the call is coming from a reliable source.

Malware: Malicious software created to damage or control over any computer system is referred to as malware. Devices are harmed, data is stolen, and mayhem results. Malware is an abbreviation for malicious software, which is software designed by a group of hackers to engage in evil deeds. The majority of online attackers are motivated by malware. It sets up a virus in the user's machine prevents them from opening attachments sent by other users or clicking links they don't recognise people on your friend list, the user is putting themselves at risk of contracting malware. Before clicking on or downloading any files, it is crucial that social network users always make sure the source is reliable. Malware comes in several forms, including as viruses, Trojans, worms, transom ware, adware, and botnets. A Trojan, for instance, is a worm that contains hidden code for stealing a person's private information.

Identity Fraud: Identifying fraud is a type of theft where a person poses as someone else and commits crimes online under that person's name. It is among the most prevalent cybercrimes on social media. Someone can impersonate another person by using their name, address, and images as identification committing a crime like scamming gullible members of the public. The incorrect actor even conduct business with businesses and organisations using the fictitious account or profile.

Theft of FTP Passwords: This is yet another very popular method for accessing someone's data on their phone or website. The FTP password hacking makes use of the fact that many users and website administrators save their login credentials on their insecure phones and PCs. These unlawful searches Hacker probes the victim's machine for FTP login information and then sends the information to his own distant computer. Then he logs through the remote computer into the website/platform and changes the web pages/platform as desired. This will grant the criminal access to the victim's bank accounts and other mobile-based applications websites.

Debit or credit card fraud: is a kind of identity fraud in which an unauthorised person makes use of a card to make purchases a person uses another person's credit card number to withdraw money or make purchases. Use the internet or

go in person to commit credit card theft. There are numerous ways to engage in this unauthorised use, taking control of an account by using a stolen or lost card and reporting it stolen or lost after gathering enough information and by "skimming," which entails using a digital attachment that appears to be legitimate, like a self-service credit using a card at a petrol station, etc.

The most frequent sorts of social media-related crimes are those listed above. As a result, several crimes are committed on the platforms and/or spaces of social media.

4. Laws Regarding Cyber security around the world

Australia: The Australian Parliament approved a divisive measure to stop the "weaponization" of social networking sites. Act of 2019 to amend the Criminal Code (Sharing of Abhorrent Violent Material) which added offences for neglecting to report repugnant acts, amending the Criminal Code Act of 1995 material and neglecting to remove offensive stuff. The Act mandates that if any offensive violent materials involving offensive behavior in Australia is made available online, internet service providers, content providers, and hosting service providers must inform the Australian Federal Police within a "reasonable period "regardless of whether the service provider is located in Australia, the platform. This is true for all platforms, therefore if they host or provide the necessary content available, service providers worldwide. Failing to inform and failing removing the pertinent text is punishable by harsh fines. Even still, vile violent content is posted online as cybercrime for internet providers to analyze. This implies that the various social media platforms should be held accountable for any crimes committed via those platforms. Aggressive behavior that is abhorrent was defined as behavior in which a person commits a terrorist attack, kills another person, or tries to kidnap another person. It is argued that this Act's application is restricted because it does not address other types of cybercrimes committed using social media. However, as a result of Australia's decision, social media sites like Facebook now employ a significant number of content checkers and frequently work with outside content verifiers. The Enhancing Online Safety Act of 2015 also created an eSafety Commissioner in Australia to advocate for everyone in Australia's internet safety. The Online Content Scheme, which offers a complaints procedure for forbidden content based on the categorization areas in the National Classification Scheme, is administered by the eSafety Commissioner. There have, however, been requests for the review and update of this statute to the Online Safety Act and a brand-new uniform code of professional conduct.

China: Websites like Twitter, Google, and WhatsApp are restricted in China. Instead, Chinese providers like Weibo, Baidu, and WeChat offer their services. Accessibility to the viral secure networks that certain users have used to get around barriers has also been somewhat effectively restricted by Chinese authorities in places. At the end of January 2019, the Chinese Cyberspace Administration revealed that the preceding Thanks to social media, 733 websites had been shut down and 9,382 mobile apps had been "cleaned up" in the previous six months. Numerous social media platforms are monitored by China's several hundred thousand of cyber police, who also filter posts that are regarded to be politically controversial. China also made technological investments in security placing restrictions on e-commerce businesses and monitoring consumers. certain rules for When the state passed the Security Protection of Computers ordinance in 1994, cybercrime first emerged (State Council Decree No. 147, 1994) Information System. The Ordinance established legal penalties for five different forms of behaviour:

1. Threats to computer information systems and violations of their security ranking protection systems;
2. Violations of their registration systems. International networking of information systems
3. Failing to disclose computer-related incidents information systems within the allotted period
4. Refusing to make improvements after being notified by the public security agency calling for an improvement in the security environment and
5. Other conduct posing a threat to system for computing and information.

The overlap of requirements, the absence of referred rules and laws, and the tardy application of punishments are the main issues with China's substantive law provisions. However, in order to ensure security, China employed a number of measures that were characterized by content screening and activity tracking both state stability and cyber security.

America's United States: The Federal Government has not yet passed legislation that treat cyber security in depth. There are, however, some laws that are designed to stop cybercrimes. They include the Sarbanes-Oxley Act of 2002, the Children's Online Privacy Protection Act of 1998, and Federal the Federal Information Security Modernization Act of 2014, the Information Security Management Act of 2002, and2015's Cyber security Information Sharing Act. A handful of states have enacted their own, more thorough cyber security laws in addition to the federal rules and statutes. Examples include the New York Stop Hacks and Improve Electronic Data Security Act of 2019 and the California Consumer Privacy Act of 2018. Additionally to the Global businesses must adapt their cyber security in accordance with various state legislation around the United States adherence to international legal measures.

5. Concluding Remarks and Suggestions

Like other internet-related practices, the rapid development and popularity of social media networking site has brought to light a variety of social media cybercrime issues that have an ever-worsening impact. It is important to emphasize that the primary method of preventing crimes committed on social media is done by media corporations through voluntary self-regulation and content control. This is going to backed by the government and outside parties who provide further help through influencing policies, volunteer actions and sensibilization through education. A variety of problems have hindered the precise cybercrime tracking and measurement. First, there is no precise definition of what cybercrime is. This is made even more difficult by the fact that cybercrimes frequently overlap with non-cybercrimes in the globalized world, making it difficult to assess their severity the whole extent of cybercrime. The following actions could be beneficial. These ought to be implemented in Nigeria a comprehensive law that will address all facets and varieties of cybercrime. There needs to be created a

cyber-tribunal for the swift and efficient resolution of matters involving cybercrime. Both the Criminal Code and the Penal Code need to be updated to reflect contemporary technology advancements and reality. The various Federation states ought to develop their own cyber security legislation as well. In the United States of America, attainable. A cyber police/monitoring force should be established to find online offences. The Nigerian government should make significant investments in security technology and impose standards for electronic businesses and user surveillance. The general populace ought to be educated on the tactics and methods used by online fraudsters. In order to prevent cybercrimes, social media platform and networking site providers must also be aware of the content uploaded on their platforms.

6. References

1. (n.d.). Wikipedia. Retrieved September 5, 2022, from https://www.beds.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/
2. The 12 types of Cyber Crime | Chapter No.2 | Fast-track To Cyber Crime. (n.d.). Digit. Retrieved September 10, 2022, from https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html/
3. Dennis MA. (n.d.). Cybercrime | Definition, Statistics, & Examples | Britannica. Encyclopedia Britannica. Retrieved October 1, 2022, from https://www.britannica.com/topic/cybercrime
4. How Social Media is used in Cybercrimes. (n.d.). The Defence Works. Retrieved October 8, 2022, from https://thedefenceworks.com/services/cyber-and-security-awareness/guides/how-social-media-is-used-in-cybercrimes/index.
5. (n.d.). UNODC. Retrieved September 12, 2022, from https://www.unodc.org/unodc/en/cybercrime/index.html
6. Regulation of Australian online content: cyber safety and harm. (n.d.). Parliament of Australia. Retrieved September 16, 2022, from https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/Cybersafety
7. Social media execs will face jail in Australia if their platforms host violent content. (2019, April 4). CNBC. Retrieved October 2, 2022, from https://www.cnbc.com/2019/04/04/social-media-execs-will-face-jail-in-australia-if-their-platforms-host-violent-content.html
8. Social media: How do other governments regulate it? (2020, February 12). BBC. Retrieved September 20, 2022, from https://www.bbc.com/news/technology-47135058
9. Social Media-Related Cybercrimes and Techniques for Their Prevention. (2012, November 7). Sciendo. Retrieved September 18, 2022, from https://sciendo.com/article/10.2478/acss-2019-0002
10. What is Malware? - Definition and Examples. (n.d.). Cisco. Retrieved September 25, 2022, from https://www.cisco.com/c/en_in/products/security/advanced-malware-protection/what-is-malware.html