International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 14 Issue 3 || March 2025 || PP. 97-100

A Study of Cyber Crime Awareness among the Youth

MR. Ronak Gupta and Dr. Neha dubey
Researcher master of social work – Parul University
Assistant professor, faculty of Social Work, Parul University, Vadodara

ABSTRACT:
The swift rise in teenage internet usage in the digital age has made them vulnerable to a number of cybercrimes, such as identity theft, phishing, hacking, cyberbullying, and online fraud. Since they utilize the internet the most, young people are especially susceptible to these risks, which can affect their social, mental, and financial well-being. The likelihood of becoming a victim of cybercrime is further increased by low digital literacy and ignorance of online safety procedures. To safeguard young people from online dangers and encourage appropriate digital conduct, it is crucial to raise their understanding of cybercrime. Reducing cybercrime events requires effective strategies including digital education, strict privacy policies, parental supervision, and government initiatives. Communities and institutions must also work together to increase awareness through campaigns, workshops, and educational initiative We can protect young people from online dangers and create a safe online environment by promoting a culture of cyber safety. Young people will be more equipped to identify possible hazards, report instances, and take preventative action if they are more aware. This study highlights the value of ongoing education, legislative frameworks, and cooperative initiatives to lower cybercrime and encourage young people to practice responsible digital citizenship.

Keywords:
Cybercrime, Youth Awareness, Online Safety, Cyber bullying, Digital Literacy, Identity Theft, Online Fraud, Privacy Protection, Cyber security, Digital Responsibility

I. INTRODUCTION:

1. Introduction to Youth Awareness of Cybercrime

The way people live, work, and communicate has changed dramatically as a result of the internet's broad use and the quick development of technology. Numerous advantages have resulted from the incorporation of technology into daily life, particularly for young people who depend on digital platforms for information sharing, social connection, education, and entertainment. Youth are now more vulnerable to a variety of cyberthreats, which are commonly referred to as cybercrime, as a result of their greater reliance on technology. Cybercrime is the term used to describe illegal actions taken against people, businesses, or systems using the internet or digital platforms. Information theft, user exploitation, financial loss, and reputational harm are the main goals of cybercriminals.

2. Comprehending Youth Cybercrime

Any illegal conduct involving a computer, digital device, or network that primarily targets data, money, or personal information is referred to as cybercrime. Cybercrime can take many different forms for young people, such as identity theft, online fraud, hacking, phishing, and cyber bullying. Young people find it more and more difficult to recognize and defend themselves against these threats as the digital world and the tactics and methods used by cybercriminals change.

1. Cyberbullying: Online harassment, bullying, or intimidation through social media, messaging apps, or gaming platforms.
2. Phishing: Deceptive emails, messages, or websites aimed at stealing personal information like passwords, credit card details, or social security numbers.
3. Identity Theft: Unauthorized use of personal information to commit fraud, access bank accounts, or engage in criminal activities.
4. Hacking: Gaining unauthorized access to a person's computer, account, or device to steal data or cause disruption.
5. Online Fraud: Deceptive schemes that manipulate individuals into transferring money or revealing confidential information.

3. Causes of Cybercrime Among Youth

The vulnerability of youth to cybercrime can be attributed to several factors, including:

3.1. Increased Digital Dependency

In modern times, the internet has become an integral part of daily life for young individuals. They use the internet for education, communication, socializing, and entertainment. This extensive digital exposure increases the likelihood of encountering cyber threats.

3.2. Lack of Cyber Awareness

A significant number of young individuals lack adequate knowledge about online security, privacy settings, and preventive measures. This ignorance makes them easy targets for cybercriminals.

3.3. Peer Pressure and Social Media Influence

Social media platforms have become a hub for communication and social validation. Youth often share personal information, photos, and videos without considering the potential misuse of their data. Peer pressure to stay socially connected also contributes to vulnerability.

3.4. Lack of Parental Control

In many cases, parents have limited knowledge about digital platforms and do not monitor their children's online activities. This lack of supervision increases the chances of young individuals falling victim to cybercrime.

3.5. Technological Advancement

The rapid evolution of technology has made it easier for cybercriminals to exploit young users. Emerging technologies like Artificial Intelligence (AI), the Internet of Things (IoT), and cloud computing have created new opportunities for cyber threats.

II. OBJECTIVES OF THE STUDY:

The primary objective of this study is to explore and promote cybercrime awareness among the youth, focusing on their vulnerability to various online threats such as cyber bullying, identity theft, phishing, hacking, and online fraud. The study aims to identify the factors contributing to youth becoming victims of cybercrime and to analyze the impact of these crimes on their mental health, financial stability, and social well-being. Additionally, the study seeks to recommend effective preventive measures, including digital literacy, parental guidance, and cyber security education, to safeguard young individuals and promote responsible online behavior for a safer digital environment.

III. REVIEW OF LITERATURE:

The increasing prevalence of cybercrime has raised significant concerns about the safety and security of youth in the digital space. Several studies have explored the nature, impact, and preventive measures of cybercrime, emphasizing the importance of cybercrime awareness among young individuals. According to Hinduja and Patchin (2019), cyber bullying remains one of the most common forms of cybercrime among youth, significantly affecting their mental health and social well-being. Similarly, Arachchilage and Love (2014) highlighted that lack of cyber security awareness contributes to the vulnerability of young individuals to phishing attacks and identity theft.

Research by Dhir et al. (2021) demonstrated that social media overuse and digital dependence increase the risk of falling victim to online fraud, hacking, and privacy breaches among youth. Furthermore, studies by O'Keeffe and Clarke-Pearson (2011) emphasize that inadequate parental supervision and digital literacy significantly contribute to the rise of cybercrimes among young users. The literature collectively suggests that promoting cybercrime awareness through education, social campaigns, and policy reforms can significantly reduce the vulnerability of youth to cybercrime. It also emphasizes the role of educational institutions, families, and governments in creating a safe digital environment through continuous awareness and preventive measures.

IV. Research Methodology:

4.1 Research design:

The framework developed to look for answers to the research questions is known as the research design. A research design is essentially the study's road map or blueprint. The current study is descriptive by design since it details young people's awareness of cybercrime. A survey study

Design is the field that focuses on characterizing the traits of a specific young person. The description of the events and situations is the main goal of this design. The study also seeks to characterize the type and scope of victimization as well as its effects.

4.2 Sampling Design:

selecting a representative sample from various age groups, educational backgrounds, and regions to ensure diverse, accurate insights into their awareness levels.

4.3 Data collection:
Primary Data: Interview schedule
Secondary Data: Internet, books, magazines, previous dissertation, journals

4.4 Sample size:
The study of awareness of cyber crime **38 male** and **24 women** who aware about cyber crime.

V. MAJOR FINDINGS:

SOME OF THE IMPORTANT FINDINGS OF STUDY ARE BEING DISCUSSESED BELOW:

- The study found that 61% of male youth (38 respondents) were aware of cyber crimes, but many lacked knowledge about legal measures and reporting procedures, highlighting the need for more awareness programs.
- The major finding reveals that the age group of 21-25 exhibits the highest awareness of cyber crime, with many individuals recognizing risks, yet a significant gap in understanding preventive measures
- The study revealed that a majority of youth respondents were postgraduates, indicating a higher level of educational attainment. This suggests that educated individuals tend to have greater awareness of cyber crimes, enabling them to recognize potential threats and adopt preventive measures to safeguard their online presence.
- a significant portion of youth feels only slightly educated about cyber crime. Despite using the internet regularly, they lack adequate knowledge about cyber threats, prevention measures, and legal actions, emphasizing the need for comprehensive awareness programs to enhance their understanding and safety.
- The study found that many youth feel safe while being online, despite the growing risks of cyber crime. This false sense of security highlights a lack of awareness about potential threats like hacking, phishing, and identity theft, emphasizing the need for effective educational programs to promote online safety practices.
- The study found that many youth feel safe while being online, despite the growing risks of cyber crime. This false sense of security highlights a lack of awareness about potential threats like hacking, phishing, and identity theft, emphasizing the need for effective educational programs to promote online safety practices.
- The study revealed that 47 youth reported not being victims of cybercrime, indicating a perceived sense of safety online. However, this does not imply immunity from potential threats, emphasizing the need for continuous awareness programs to ensure they remain cautious and informed about cybercrime prevention measures.
- The study revealed that 53 respondents stated they had not lost any money due to cyber crime, indicating a positive experience with online safety. However, this does not eliminate the potential risk, emphasizing the need for continued awareness and education to prevent future financial losses through cyber crimes.
- The study revealed that 30 youth believe cyber crimes are primarily committed for financial gain. This perception highlights their awareness of economic motives behind cyber crimes, such as fraud, hacking, and identity theft, emphasizing the need for educational initiatives to broaden their understanding of various cyber threats.
- The study is that 33 youth participants emphasized the importance of increasing awareness and education on cyber crime. They believe that enhanced knowledge about online threats, preventive measures, and legal actions can significantly reduce cyber crime risks, promoting safer online behavior among young individuals.

VI. Suggestions:

To tackle the issue of cybercrime effectively, a range of measures should be implemented to educate and protect internet users.

First and foremost, educating students about the risks of cybercrime should be prioritized in schools. The same educational approach should be applied at the collegiate level, offering seminars and workshops on cybercrime prevention. It is also important to engage experts, such as cyber security professionals and ethical hackers, in workshops and orientations to provide a clear understanding of cybercrime and how to avoid it.

The government should take proactive steps to increase public awareness by launching state-wide awareness programs. These programs should emphasize the importance of creating secure and unique passwords for online accounts, particularly on social media platforms. Additionally, the government should ensure that laws and policies addressing cybercrime are reinforced to create a sense of security for internet users.

Social media platforms can play a crucial role in raising awareness about specific types of cybercrime, such as identity theft and fraudulent user profiles. By using these platforms, individuals can be educated on how to protect themselves and how to report cybercrimes. To support this, the government should consider establishing more cyber cells throughout the state to handle the increasing number of cybercrime cases. Even if the financial loss from a cybercrime incident is small, these cyber cells should offer support and assistance to the victims.

Alongside governmental efforts, regular awareness programs, such as free webinars and poster campaigns, should be conducted in public places. These programs should cover essential topics such as protecting against identity theft, securing personal data, and recognizing common cybercrime scams. Public awareness can also be increased through advertisements, media publications, and social media channels.

Additionally, training and enhancing cyber security education is critical for the general public. Teaching people to be cautious while using gadgets, reading messages before forwarding them, and avoiding sharing false information on social media can help minimize risks. It is essential to promote a healthy balance in technology use by encouraging people to limit their smartphone usage.

By focusing on these measures—awareness, education, and government action—cybercrime can be effectively mitigated, providing internet users with the knowledge and tools needed to stay safe online.

VII. Conclusion:

The study reveals that most users have a basic awareness of cybercrime, with hackers being the most recognized form. However, many respondents lack knowledge about cybercrime laws and data security. Although most spend over two hours online daily, they are unsure about the safety of their personal information, highlighting a lack of understanding in protecting their data.

A small number of respondents reported financial losses from online transactions, and many rarely change their account passwords, which increases security risks. While aware of cybercrime, respondents engage in risky activities like downloading content linked to cybercrime.

The study also found that while many respondents receive spam calls and messages, few report these incidents to authorities, indicating a lack of proactive measures in preventing further cybercrime.

Cybercrime, a category of crime driven by technology and advanced methods, has become more prominent with technological advancements. Unlike traditional crimes, cybercrimes are committed using machinery and formulas, involving both blue-collar and white-collar criminals. Although the names may differ, these crimes share similarities with other crimes, as they are carried out by individuals with a scientific understanding of technology.

Given the rise of cybercrime, greater awareness and proactive steps are needed to protect individuals from becoming victims.

References:

[1]. Astt Narayan – LK Thakur, 'Internet Marketing E-Commerce and Cyber Laws' Authors Press, Delhi, 2000.
[2]. Bama, Yogesh, 'Criminal Activities in Cyber world.' Dominant Pubhshers and
[3]. Distributei-s, New Delhi, 2005
[4]. Chopra Deepti and Keith Merill, 'Cyber Cops, Cyber Criminals and the Internet: I.K. International. Ltd., New Delhi, 2002.
[5]. Chris Reed & John Angel, 'Computer Crime & Computer Law.' Ed.-S, Oxford University Press, Delhi, 2005.
[6]. Dr Gandhi; K.P.C, 'Introduction to computer related crimes.' CBI Bulletin, Delhi.
[7]. Dr. Ahmad Farroq, 'Cyber Law in India (Law on Internet).' New Era Law Publications, Delhi, 2011.