IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 10, October 2024

Impact Factor: 5.731

Study on Awareness on Cyber Crime as Well as Prevention to Deal Effectively with Cybercrime in Cuttack City of Odisha State

Satya Narayan Mishra[1] and Dr. Sanjaya Choudhary[2]

Research Scholar, Law, Bhagwant University, Ajmer, Rajasthan, India[1]

Professor, Law, Bhagwant University, Ajmer, Rajasthan, India[2]

Abstract: *Cybercrime is really getting the recognition it deserves. However, it is not going to be banned so easily. In fact, it is highly likely that cybercrime and its hackers will continue to evolve and upgrade to stay ahead of the law. Cybercrime refers to any act committed with criminal intent in cyberspace. Cybercrime includes acts like hacking, uploading absentee material on the internet, sending absentee emails and hacking individuals e-banking account to withdraw money. Cybercrime refers to any crime that involves a computer or its network. The term Cybercrime is a misnomer. The term is now defined in any law/act passed or enacted by the Indian Parliament. In this research, I will mention the impact of Cybercrime committed by people to destroy organized networks, theft of data, documents, hacking of bank accounts. My research will give you detailed information about cybercrime, its types, methods and security measures including awareness as well as prevention to deal with Cybercrime effectively in Cuttack city of Odisha state. I will give detailed information about some Cybercrime areas like banking fraud crimes, cyber pornography. Cyber Gambling, Fraud, Cyber Defamation, Email Spoofing, Email Bombing, Virus/Worm Attacks, Salute Attacks, Web Jacking, Denial of Service Attacks, Intellectual Property Crimes with Facts and File of Cuttack City of Odisha State.*

Keywords: Cyber Gambling, Fraud, Cyber Defamation, Email Spoofing etc.

I. INTRODUCTION

As the Internet has evolved, become more accessible and has been given greater importance in our societies, terrorists have logically followed this trend and have increasingly used it. But the combination of this new medium and the growing threat of global crime calls into question and shakes traditional legal responses to their core. States face three major difficulties in responding effectively to cybercrime. The need to identify both perpetrators and regional capacity is significantly challenged by the loose and transnational structure of cyber-terrorist groups. The anonymity afforded by the Internet shakes both the judicial principle of police investigation and the personal nature of punishment. Similarly, the importance of understanding the methods and risks that trigger criminal activity is largely complex due to the highly technical nature of the devices and networks used, requiring specially trained experts in the fight against cybercrime. It occurs. The need to adequately respond to a terrorist cyber threat is also thwarted by the intensity of communications and the virtual nature of information exchanged by terrorists over the Internet. Furthermore, crime goes hand in hand with political demands or goals. Because liberal democracy is based on allowing free debate of political ideas, prosecutions based on the spread of terrorist messages or material on the Internet raise questions at the core of our fundamental principles. Reaching the proper balance between civil liberties and the fight against the attackers of our society is difficult and always fluid. The first difficulty comes from the inability of states to reach agreement on a universal definition of the crime, although a European definition has been adopted. Arguably, “cyber-crime” as a concept is much discussed. Some scholars argue that it should be limited to cyber attacks carried out by terrorists, while others argue that it should include all uses of the Internet for terrorist purposes. Throughout history, mankind has waged war in an attempt to advance national agendas in the ever-changing international game of power. From the sword fights of the past to the unmanned drone attacks of today, this game of power is constantly driven by technology to change

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

and evolve. The development of armored vehicles, aircraft, ships, and the use of electronics and telecommunications have expanded the battlefield and introduced new and innovative ways to gain an edge over adversaries. Just as technological innovation in flight sparked a race to dominate the skies, the emergence of cyberspace has opened up new strategic possibilities and threats, leading to a race to gain a dominant position within it. Governments are also acutely aware of the need to take action in response to threats from cyberspace.

Former US President Barack Obama has declared America's digital infrastructure a strategic national asset and formed CYBERCOM: a division inside the Pentagon whose stated function is to "conduct full spectrum operations". Leaked documents from the National Security Agency in the US also confirm that national security figures are calling for establishing offensive cyber capabilities (in the UK, government officials have warned of a lack of preparedness for cyber warfare and called for strengthening defences. have announced new investments to do so, such as a national cyber security program (UK is 'complacent' on the risk of military cyber attack, MPs warned, 2013). NATO is also raising awareness, advising nations is releasing a manual on international law applicable to cyber warfare in an effort to better understand how to operate legally in this new battlefield. Looking at this evidence it is clear that cyber warfare is a matter of global concern.

Here are some information about Cybercrime in Cuttack city of Odisha state, India:

- As per Odisha police statistics, the number of cybercrime cases saw a huge spike from 385 in 2015 to 2037 in 2021, a whopping increase of 492%, showing the vulnerability of people to such offences during the period.
- The state government has set up 15 Cybercrime police stations at different sensitive places of the State.
- There has been some sensational Cybercrime frauds in Cuttack
- A week of friendship with a stranger on instagram made a 34 years old woman from Cuttack poorer by Rs. 30 lakhs as she lost the amount to a cyber crook to get 90,000 Euros from him.
- A retired doctor living in Cuttack city, was duped of Rs. 77 lakhs from his SBI account by cyber criminals. The criminals cheated the doctor on the pretext of activating the SIM card of his mobile phone. The incident came to light when the doctor lodged FIR regarding the fraudulent transaction amount to Rs. 77,86,727 with the cyber police station in Cuttack.
- The Cuttack district cyber offence police station has arrested two persons in connection to a major Cybercrime racket operating in the city.
- The Government of India has taken steps to increase awareness about Cybercrime and improve cyber security.
- National Cybercrime Reporting Portal (NCRP) is a government initiative that allows victims to report cybercrimes online.
- Teachers can help raise awareness about cybercrime and how to use the Internet safely.
- Cybercrime is a board term that includes many types of illegal activities such as hacking, identity theft and online fraud.
- Bhubaneswar-Cuttack Police Commissioner conducted cyber security campaign on October 5, 2023.

Cybercrime

Cybercrime is a crime that involves computers and networks. Finding any computer at a criminal place or committing any crime using a computer is called computer crime. Computer crimes do not involve networks. Obtaining and misusing someone's personal information. Extracting or stealing personal information from anyone's computer is also a cybercrime. Computer crimes are also committed in many ways such as stealing information, erasing information, altering information, giving someone's information to someone else or stealing or destroying computer parts. There are many types of cybercrimes such as spam emails, hacking, phishing, inserting viruses, obtaining someone's information online or keeping an eye on someone all the time.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

Type

Types of Computer Crime

- **Stealing information** – Extracting personal information from someone's computer, such as username or password.
- **Erasing information** - Erasing information from someone's computer so as to cause harm to it or erasing important information.
- **To alter-** To change or add something to the information.
- **External damage –** Destroying, breaking or stealing parts also comes under computer crime.

Types of Cybercrime

- **Spam Email-** There are many types of emails in which there are emails which only cause harm to the computer. Those emails cause the entire computer to malfunction.
- **Hacking-** Hacking someone's personal information such as username or password and then changing it. **Cyberphishing-** Sending spam email to someone so that he gives his personal information and that information can cause harm to him. This email is anonymous.
- **Spreading viruses -** Cyber criminals send some software to your computer in which viruses may be hidden, these include viruses like virus, worm, Trozan horse, logic Bomb etc., these can cause a lot of harm to your computer. **Software Piracy -** Making copies of software and selling it at cheap prices also comes under cybercrime, due to this the software companies have to suffer huge losses and at the same time your valuable equipment also does not work properly.
- **Fake bank call –** You receive a fake email, message or phone call that impersonates your bank asking you to provide your ATM number and password and if you do not provide this information, your account will be closed or Give information on the link. Remember, such information is never asked by any bank in this manner and do not share any such information through internet, phone call or message.
- **Spreading rumors on social networking sites -** Many people spread social, ideological, religious and political rumors on social networking sites, but users do not understand their intentions and keep sharing such links knowingly or unknowingly, but This also comes under the category of Cybercrime and cyber-terrorism.
- **Cyber Bullying -** Making indecent comments on social networking sites like Facebook, making threats on the internet, making fun of someone to the point of being harassed, embarrassing someone in front of others on the internet is called cyber bullying. Children often become victims of this. This also affects their health.

Provisions related to jurisdiction in cyberspace under the Information Technology Act, 2000

From the point of view of the development of human society, the discovery of information and communication technologies can be considered the most important invention of the twentieth century. The importance of its use in various areas of social development, especially in the judicial process, cannot be underestimated because due to its qualities like fast speed, freedom from many minor problems, lack of human errors, being less expensive, etc. Can play an important role in making it credible. Not only this, in the execution of such cases, where physical presence of all the concerned parties is not mandatory, it can prove to be the best option. The list of charges mentioned under the Information Technology Act is as follows:

- Attempt to tamper with computer resources - Section 65
- Attempt to hack the data stored in the computer by tampering with it - Section 66
- Provision of punishment for sending prohibited information through communication services - Section 66A
- Provision of punishment for wrongfully obtaining stolen information from a computer or any other electronic gadget - Section 66B
- Provision of punishment for stealing someone's identity - Section 66C
- Provision of punishment for accessing someone's personal data with the help of computer by hiding one's identity - Section 66D

- Provision of punishment for violating someone's privacy - Section 66E
- Provision of punishment for cyber terrorism - Section 66F
- Provisions related to publication of objectionable information - Section 67
- Provision of punishment for publishing or disseminating sex or obscene information through electronic means - Section 67A
- Publication or transmission of such objectionable material through electronic means, in which children are shown in obscene condition - Section 67B
- Provision of punishment for obstructing or withholding information by intermediaries - Section 67C
- Provisions related to unauthorized access to secured computers - Section 70
- Misrepresenting data or figures - Section 71
- Provisions related to breach of mutual trust and privacy – Section 72A
- Provisions related to making information public in violation of the terms of the contract - Section 72A
- Publication of fake digital signature - Section 73
- Under Section 78 of the Information Technology Act, Inspector level police officers have the authority to investigate these cases.

Provisions related to cybercrimes in the Indian Penal Code (IPC)

- Sending threatening messages through email - Section 503 of IPC
- Sending such messages through email which constitute defamation - Section 499 of IPC
- Use of fake electronic records – Section 463 of IPC
- Fake websites or cyber fraud-section 420 of IPC
- Surreptitiously monitoring someone's email - Section 463 of IPC
- Web Jacking-Section 383 of IPC
- Misuse of email - Section 500 of IPC
- Selling medicines online-NDPS Act
- Online buying and selling of weapons - Arms Act

66-F: Provision of punishment for cyber terrorism

Section 66-F has been included in the Information Technology Act, 2000 for penal legislation in cases of cyber terrorism.

(1) If any-

(a) to subvert the unity, integrity, security or sovereignty of India or to terrorize its inhabitants - (K). Prevents or causes any authorized person to be prevented from using the computer.

(b) Attempts to forcibly use any computer without authority or in excess of his authority.

(c) introduces or attempts to introduce into the computer any such thing as a virus, which is likely to cause danger to the life of people or there is danger of damage to property or deliberately tries to disrupt the services essential to life. Does this or there is a possibility of adverse impact on sensitive information under section 70 or-

(b) knowingly obtains from any computer any information which is sensitive from the point of view of the security of the country or its relations with other countries or any confidential information with such intention that, by trespass or violation of rights, Does or is likely to adversely affect the security, unity, integrity and sovereignty of India, its relations with other countries, public life or morality, or is likely to cause contempt or defamation of the courts of the country. If there is apprehension, promotion or apprehension of any crime, any foreign nation or group of persons or anyone else benefits from such information, then he can be considered accused of cyber terrorism.

(2) If any person commits cyber terrorism or is involved in any conspiracy to commit cyber terrorism, he may be sentenced to imprisonment for life.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

The term cyberspace is also defined on similar lines in the third edition of the Advanced Law Lexicon, published in 2005. In this, special emphasis has been laid on the word floating in electronic mediums, because it can be accessed from any part of the world. The author has further defined the term cyber theft in the context of the use of online computer services. Cyber law is defined in this dictionary as the area of law that deals with computers and the Internet and includes intellectual property rights, freedom of expression, and unrestricted access to information.

Some more things have been defined in the Information Technology Law, which are as follows, Computer means any electronic, magnetic, optical or any such device for exchanging data at high speed, which is based on various technologies. Is capable of doing mathematical, logical or computational work with the help of. This includes every program and software connected to or related to a computer system.

As per Section 1 (2) of the Information Technology Act, 2000, the provisions of this Act are effective throughout the country, except as mentioned above. Also, under the above mentioned provisions, the said provisions will be effective even in case of any crime committed outside the borders of the country.

Implications for social change

With the increase in cybercrimes, individuals, organizations, businesses and governments are looking for relevant and efficient solutions to prevent or fight the compromise of their data. The impact of this study in terms of positive social change may increase people's awareness about keeping themselves safe while using the Internet and social media platforms. Additionally, the study may help organizations ameliorate the ethical and financial biases associated with cyber attacks. The study can also help identify best practices for cyber security awareness that are necessary to protect personal data and prevent cybercrimes in the long run. Social technologies related to user awareness contribute significantly to preventing harassment, and social networking services should provide appropriate controls to protect personal information.

Result Analysis

The Result Analysis to create awareness about Cybercrime and its prevention in Cuttack city of Odisha is necessary for several reasons:

Increasing incidents of cybercrime:

With the increasing digitalization of services and communications, there is a parallel increase in the incidents of cybercrime. Cuttack city is not immune to these threats, and awareness programs are important to educate the public about the potential risks and vulnerabilities.

Security of personal and financial information:

Like elsewhere, individuals in Cuttack city also conduct a significant portion of their personal and financial transactions online. Creating awareness about cyber threats helps citizens understand how to protect their sensitive information, reducing the risk of identity theft, financial fraud and other cybercrimes.

Business and Economic Impact:

Cuttack city, being an economic hub, has many businesses that depend on digital platforms for their operations. Cyber attacks can have serious economic impacts, affecting businesses, trade, and overall economic growth. Awareness initiatives can empower businesses to implement effective cyber security measures.

Legal Literacy:

Many individuals may not be fully aware of the legal aspects of Cybercrime and its consequences. Awareness programs can help educate the public about relevant laws, reporting mechanisms and legal remedies available to victims. This can contribute to a safe online environment and effective law enforcement.

Community Resilience:

Cyber security is a collective responsibility. Creating awareness fosters a sense of community resilience, where individuals, businesses and institutions collaborate to create a safe online ecosystem. Informed and alert communities are better equipped to quickly identify and report cyber threats.

Prevention through education:

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 10, October 2024
Impact Factor: 5.731

Prevention is a key aspect of tackling cybercrime. By educating individuals about common cyber threats, phishing attacks, malware, and other malicious activities, the Result Analysis aims to empower people to take proactive measures to prevent cyber incidents before they occur.

Adaptation to Technological Progress:

The technology landscape is constantly evolving, and new cyber threats emerge regularly. Awareness programs ensure that the public is informed about the latest cyber security trends and practices. This knowledge prepares individuals to effectively adapt to technological changes and emerging cyber threats.

Government and law enforcement assistance

Awareness initiatives may receive support from government bodies and law enforcement agencies. Educated citizens are more likely to report cybercrimes, enabling authorities to respond quickly and effectively. This collaboration between the public and law enforcement is critical to comprehensively combating cyber threats.

The Result Analysis to create awareness about Cybercrime and its prevention in Cuttack city addresses the critical need to protect individuals, businesses and the overall community from the growing threat of cybercrime. By promoting a culture of education, legal literacy and cyber security, this initiative contributes to creating a resilient and secure digital environment in the city of Cuttack, Odisha.

The generic qualitative design study was to address the strategies used for security awareness by information security officers in the prevention of cybercrimes by cybercriminals. The population was information security officers who are currently in charge of managing information security within their organizations and located on the Northeast Coast of the United States, listed on social media such as LinkedIn and Facebook. Implications for positive social change include the ability to develop a culture of prevention based on knowledge of cybersecurity awareness. Additionally, implementing a strategic plan to prevent cybercrimes can help users understand cybercrimes and increase vigilance when exposed to the Internet and social media.

As the Internet is becoming a medium for all walks of life such as commerce, education, social and economic space, etc., there are many technologies that reduce the opportunity to commit crimes related to the Internet and PC (computer/system). The basic and old techniques and principles are not sufficient to determine the presence of criminals motivated by criminal activity and methodology and as a result cyber criminals are increasing day by day due to the absence of capable guardians. The criminal justice administration system is not equipped to deal with the highly smart and hybrid technological crimes occurring in cyberspace. Internet vandalism is deliberately destroying people's rights and movable and immovable property and also affecting and harming others. We are aware of the intention to see and examine the effect or impact of technological leap on criminal areas, it is better to understand the whole exercise of its development and the problem of all the people regarding it. The research work is inspired by the authors' articles on Cybercrime and other law reports about Cybercrime and many other people who have been Cybercrime experts in this field. This research extends to throwing light on the legal problems faced by the entire world in the area of Cybercrime with special reference to the city of Cuttack, Odisha.

II. CONCLUSION

A study on cybercrime awareness and prevention in Odisha's Cuttack city highlights the growing concern about cyber threats in an ever-digitizing world. As technology continues to integrate into daily life, cases of cybercrime such as hacking, phishing, identity theft, and online fraud have increased significantly. In Cuttack, the level of awareness among residents about cybercrime and its potential risks varies. While a segment of the population, particularly young and tech-savvy individuals, display a moderate understanding of cyber threats, many remain unaware of the nature of these crimes and the available preventive measures. The lack of widespread digital literacy contributes to the vulnerability of individuals and businesses in the city. Efforts to prevent cybercrime emphasize the importance of public awareness campaigns, education, and promoting safe online practices. Officials in Cuttack are working to educate citizens on how to recognize potential cyber threats and protect personal information through strong passwords, updated software, and avoiding suspicious links or emails. Law enforcement agencies in Cuttack are enhancing their capabilities to combat cybercrime by establishing dedicated cyber cells and improving the legal and technical infrastructure needed to track and prosecute criminals. Collaborative efforts between law enforcement, academic

institutions, and the private sector are seen as crucial to effectively combat cybercrime. In summary, while Cuttack is taking steps to raise awareness and prevention of cybercrime, continued efforts in education, law enforcement, and public engagement are necessary to ensure long- term cybersecurity for its residents. Over the past decade, cybercrime has become a primary concern of governments around the world. However, cybersecurity awareness culture is still in its infancy, and knowledge of the topic is limited and ill-defined. According to Harrison and Jurgens (2017), an average of 23.66% of organizations classified across three economic branches, known as banks, automobiles and fintech startups respectively, are suffering from lack of security awareness training initiatives. The common IT problem is the lack of successful security awareness strategies by employees to prevent cybercrimes. The specific IT problem is that some information security officers lack security awareness strategies to prevent cybercrimes by cyber criminals. The impact of cybercrimes is high in terms of business financial losses and national security threats. Therefore, it is important to create an awareness culture as part of best practices to understand cybercrimes that are spreading rapidly and negatively impacting people, organizations, businesses and governments around the world. Security awareness significantly influences perceived severity, response efficacy, self-efficacy, and response cost. The significance of this study for IT practice may be to make end users aware of the risks they face when exposed to cybercrimes and offer successful strategies to prevent such crimes. The present study will study security awareness schemes that can support the culture in positively influencing the impact of cybercrimes by making the usage aware in terms of severity and understanding of the causes, consequences and operation mode of such incident. Confident users are less likely to perceive cybercriminal risk, which highlights the importance of end-user education.

REFERENCES

[1]. Brahme, p. d. (2013). Cybercrime and cyber law in India. research, 106-109.
[2]. Broadhurst, r. (2006). development in the global law enforcement of cyber-crime. research, 408-433.
[3]. Koranteng, A. a. (2019). impact of cybercrime and trust on the use of E-commerce technologies. an application of the theroy of planned behavior, 228-250.
[4]. Natah. (2015). e-commerce security and the purview of cyber law factors. research, 1-14. [5]. Npnp.(2014). review on Cybercrime and security. research, 48-51.
[6]. Saini, r. a. (2012). cyber-crime and their impact. research, 202-209.
[7]. Sarmah, a. a. (2017). a brief study on cybercrime and cyberlaw's of India. research, 1633-1641. [8]. Zhang, y. (2011). a survey of cybercrime. research, 422-437.
[9]. https://arcticwolf.com/resources/blog/
[10]. https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
[11]. https://arcticwolf.com/resources/blog/decade-of-cybercrime/
[12]. Cybercrime (no date) INTERPOL. Available at: https://www.interpol.int/en/Crimes/Cybercrime (Accessed: April 19, 2023).
[13]. Kaspersky (2023) What is cybercrime? how to protect yourself from Cybercrime, www.kaspersky.co.in. Available at: https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime (Accessed: April 19, 2023).
[14]. Literature review on cybercrime (no date) Bartleby. Available at: https://www.bartleby.com/essay/Literature-Review-On-Cyber-Crime-PJP6L3WT26 (Accessed: April 19, 2023)
[15]. Literature review on cybercrime (no date) Bartleby. Available at: https://www.bartleby.com/essay/Literature-Review-On-Cyber-Crime-PJP6L3WT26 (Accessed: April 19, 2023)
[16]. Literature review on cybercrimes and its prevention mechanisms (no date). Available at: https://www.researchgate.net/publication/331010726_Literature_review_on_Cyber_Crimes_and_its_Prevention_Mechanisms (Accessed: April 19, 2023).