JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

From Field to Firewalls: Strengthening Cyber Security in Rural Communities

Dr. B. Sravanthi
Assistant professor of Law
University College of law,Telangana University, Dichpally, Nizamabad-503322

Abstract

The Soul of India Lives In Its Villages - Mahatma Gandhi.

65% of the country's population is residing in rural India safety and security is the primary concerns for every community in the era of digital technology replaced the traditional form of crimes to Cyber crimes the increasing cases of Cybercrimes ringing the alarm to urgent need for the crime security public awareness and strict regulatory measures for the same. Rural India is experiencing a rapid expansion of internet connectivity with new opportunities for communication commerce and education while utilising these are opportunities rural people are subjected to Cybercrimes due to lack of basic digital literacy cyber security awareness. The lack of digital literacy among the rural communities is the primary factor for their vulnerability.

As per digital empowerment foundation states that more than 90% of Indians lack basic digital literacy. The gap between growing internet usage and lack of awareness creates a platform for Cybercrimes and posing challenges to overcome. To handle these challenges it is necessary to implement robust digital literacy programs at the grassroots levels like awareness campaigns and sensitizing the villages regarding cyber security measures, preventive practices and reporting mechanisms. In addition to it legislative framework is needed for the protection of rural communities from Cybercrimes.

Key Words: Cyber Crimes, Cyber Security, Digital Technology, Digital Literacy, Rural Communities.

Introduction

From 2015 to 20-25 India has Wednesday explosive increase in cybercrime demonstrating countries Fast track digital transformation consistent rise in cybercrimes since 2019 the cybercrimes in India has been increasing. As per Indian Cybercrime Coordination Centre (I4C) over 7400 00 Cybercrimes were reported in the first quarter of 2024.

The shift to towards online banking from 2019 the customers increasingly shifted to digital transactions through online banking more 20% higher in rural regions are using the internet than in urban regions shows the paradigm shift of internet users in rural community. The impact of internet use in rural communities particularly on youth, they are in hopes of easy and quick financial gains.

The rapid penetration of the internet into rural India has made these communities more vulnerable. In the era of technology digitisation plays a crucial role. The digital Era is a double edged sword that opens up opportunities as well as Cybercrimes. These digital technologies are creating advanced economy as well as empowered criminals. This leads to more challenges to the banks, financial institutions, and law enforcement agencies. As per the India Cyber Crime Coordination (I4C) centre 85% of complaints had been registered relating to the online fraud between January and April 2024. As per the RBI report a fivefold increase in digital payment frauds and mounting to Rs. 14.57 billion (approximately Rs. 1,457 crore) in the last fiscal year alone.

Prime Minister Narendra Modi launched Digital India on July 1st, 2015, with the goal of transforming the nation into a knowledge economy and society enabled by technology. By enhancing online infrastructure, expanding internet connectivity nationwide, promoting digital literacy, and fortifying cyber security measures, the main goal of digital India is to guarantee that individuals may access government services electronically. In addition, the Indian government passed the Digital India Act 2023 in order to create a safe

and welcoming online space that exposes and empowers residents by fostering digital literacy, building digital infrastructure, and closing the digital divide between rural and urban areas. Individuals are not the only ones concerned about the exponential rise in cybercrimes; rural communities' financial viability is also at risk. These populations are at risk for cybercrimes due to a lack of digital literacy and knowledge about cyber security. Accessing digital technology is a necessary component of development, and it's also critical to recognize the risks involved.

Objectives

1. The first goal is to research cybercrime in rural regions.
2. To research the different kinds of cybercrimes that occurs in rural areas.
3. To be aware of the law enforcement organizations that support rural areas in the fight against cybercrimes.

Research Design:

Understanding the legal sources and cyber security measures that are currently in place in India is the primary goal of the study, which has adopted doctrinal research.

The Cyber Crime Landscape in Rural Areas

The cybercrime landscape in rural communities in India is a growing concern, presenting unique challenges due to different factors like limited internet access, digital literacy, poor infrastructure, language barriers, and more trust.

Cybercrimes are any criminal activity that involves a computer, network and network devices. The primary outcome of Cybercrime is the financial loss to the victims. Cybercrimes are in different types like ransomware email or internet fraud, credit card fraud, illegal interception of data etc.

Since 2019, the number of cybercrimes has increased. India's rural people embraced digital technology in their daily lives as a result of COVID-19. It's possible that the majority of rural communities are utilizing digital technologies for the first time. The use of digital technology necessitates appropriate security measures as well, whether it be for online shopping, banking, government services, or other purposes. They are susceptible to cybercrimes because to a lack of security measures.

Prevalent Types of Cyber Crimes

The following are the various cybercrimes in existence as per the Telangana cybercrime police station

1. Vishing Calls.
2. Phising Mails.
3. Gift Frauds.
4. Job Frauds.
5. Loan Frauds.
6. Lottery Frauds.
7. Advertising Portal Fraud.
8. Card Skimming Frauds.
9. PAYTM KYC Update Fraud.
10. Dating and Female Escort Fraud.
11. Matrimonial Frauds.
12. Google Fake Customer Care Fraud.
13. Online Friendship Frauds.
14. Cyber Crime against Women.
15. Corporate Crime.

Empowering Rural Community: Practical Steps For Cyber Security

Rural communities often face unique cyber security challenges due to limited resources, infrastructure, and awareness. It is primary need to address these challenges through practical security measures to empower them with taken precautions while using digital technology for better cyber security.

The following are the few preventive steps to overcome the challenges facing through digital technology in rural communities.

1. **Training programs**: Putting together several training courses for local government workers, farmers, Dwakra organizations, small business owners, community leaders, and educational institutions. Describing the program in plain language with examples from everyday life and stressing the value of coming up with secure passwords. Educating student's safe online practices and incorporating fundamental cyber security teachings within the curriculum. Working together to empower the villages through local bodies, NGOs, and organizations. Provide best practices and recommendations for cyber security and make them accessible through community centres and local libraries.

2. **Explaining Risks and Consequences**

Giving first-hand accounts of how cybercrimes have affected rural communities' lives and means of subsistence. Stress how important it is to implement cyber security measures in order to prevent cybercrimes. Additionally, it provides information about pertinent cyberthreats to the communities, such as smartphone scams, gamming apps, hospital frauds, phony Facebook money requests, and lucky lottery scams. APK files, transferring OTPs, and unknown web URLs are a few examples of how cybercrimes can result in monetary losses.

3. **Establishing a Cyber-Security Networks**

Finding volunteers who are interested in cyber security and willing to help their communities by educating them about cybercrimes and cyber security can help establish cyber security networks in remote areas. Give the volunteers the skills and information they need to teach the community digital technology best practices.

4. Empowering with Practical Security Measures

Raise practical understanding of the value of multi-factor authentication and secure passwords, talk about software upgrades, and concentrate on keeping firewalls and anti-virus software up to date.

5. Creating Awareness to Identify Cyber Crime and Prevent To Actions

The most crucial thing is to raise knowledge about cybercrime detection. Similar to typical phishing techniques, what's App, Facebook, and other social media platforms make urgent requests for money, identify dubious links, and stress the significance of avoiding clicking on them. Communities should be advised not to reply to emails or phone calls for personal information. Talk about data backup, suggest several backup techniques, and inform people about the dangers of mobile security. Strong passwords and fingerprints are encouraged in order to safeguard mobile devices, with a focus on threads via public Wi-Fi.

6. Improvements in Intro Structure and Policy

The most crucial element in preventing cybercrimes is financing for infrastructure upgrades, training initiatives, and cyber security equipment. Creation and execution of cyber security guidelines for local government organizations. Offering training courses to personnel of the local government.

7. Supporting Mechanism

It is advised that incidents of cybercrime be reported to the proper authorities by calling 1903, using the National Cybercrime Reporting Portal, contacting the local police station for assistance, or visiting www.cybercrime.gov.in.

Law Enforcement Agencies in Empowering Rural Communities

In order to prevent cybercrimes, law enforcement organizations are essential. Investigating and prosecuting cybercrimes is only one aspect of it; other preventative methods include identifying cybercrime hotspots, promoting digital literacy, and using AI-powered threat detection systems. The primary tool for enforcing the reporting and prevention of cybercrimes is the National Cyber Crime Reporting Portal (NCCRP). The initial point of contact for reporting instances of cybercrime is the National Cyber Crime Reporting Portal (NCCRP). When a citizen uses the National Cyber Crime Reporting Portal (NCCRP) to file a complaint, the portal records the complaint, determines the victim's location, and details the type of offense. The local police station receives the report from NCCRP and conducts a father investigation. Anyone with an Internet connection can access NCCRP because it is available online around-the-clock. However, it simply makes it easier to report cybercrimes; the local police have a larger role in the context of court adjudication, arrest, prosecution, and investigation. In addition to the NCCRP, a Cyber Crime Police Station (CCPS) is a specialized organization that handles cybercrimes. Telangana state has about seven police stations. Filing FIRs, offering advice on how to submit FIRs, and receiving complaints are the duties of cybercrime police stations. Digital forensics, data recovery, network analysis, malware analysis, IP address tracing, social media investigations, arresting and detaining cybercriminals, searching and seizing evidence, preparing charge sheets, and serving as a point of contact for victims of cybercrimes are all competencies of the offices in cybercrime police stations.

Recommendations

A strong ecosystem of law enforcement and cyber security is required to successfully handle these issues. I would like to make the following recommendations in order to get beyond these obstacles:

1. Making law enforcement organizations stronger
2. Improving awareness and literacy of digital
3. Fortifying the legal and regulatory structure
4. Using digital technology to empower rural communities
5. Fostering innovation and research.

Conclusion

India's cybercrime scene is expanding quickly. Preventing the nation's security is at an alarming point. It is crucial to effectively address the changing challenges of cybercrimes in the upcoming year, especially in rural communities, as the digital divide, limited cyber literacy infrastructure, lack of awareness, and lack of preventive approaches are the main issues with regard to cybercrimes.

References

[1]. https://timesofindia.indiatimes.com/india/india-ranked-second-in-global-cyber-attack-targets-report/articleshow/116893292.cms#:~:text=India%20has%20become%20the%20second,finance%2C%20banking%2C%20and%20government

[2]. https://www.cyberabadpolice.gov.in/know-your-police-station/cyber-crimes.html

[3]. https://www.finextra.com/blogposting/27444/scammed-in-silence-unveiling-the-digital-fraud-crisis-in-rural-areas

[4]. https://www.statista.com/statistics/1499739/india-cyber-crime-cases-reported-to-i4c/#:~:text=Published%20by,related%20to%20online%20financial%20fraud

[5]. https://cybervolunteer.mha.gov.in/

[6]. https://cybercrime.gov.in/

[7]. https://www.researchgate.net/publication/383156489_A_STUDY_ON_AWARENESS_OF_CYBER_CRIMES_AMONG_PEOPLE_IN_RURAL_AREAS_AT_GOBICHETTIPALAYAM

[8]. https://ijarsct.co.in/Paper1372.pdf

[9]. https://www.researchgate.net/publication/357839318_CYBER_CRIME_IN_INDIA

[10]. Sahu and Shukla (2024). A Study on Cyber-Crime Awareness Among Students in Chhattisgarh. Journal of Ravishankar University (Part-A: SOCIAL-SCIENCE), 30(1), pp.54-60. DOI:

[11]. https://www.mdpi.com/2071-1050/14/21/14487

[12]. Sindakis, S., Showkat, G. The digital revolution in India: bridging the gap in rural technology adoption. J Innov Entrep **13**, 29 (2024). https://doi.org/10.1186/s13731-024-00380-w

[13]. https://aag-it.com/the-latest-cyber-crime-statistics/

[14]. Anupreet Kaur Mokha. A Study on Awareness of Cyber Crime and Security. Research J. Humanities and Social Sciences. 8(4): October -December, 2017, 459-464. doi: 10.5958/2321-5828.2017.00067.5

[15]. https://www.legalserviceindia.com/legal/article-10200-jamtara-india-the-hub-of-cyber-crime.html

[16]. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

[17]. https://www.forbesindia.com/article/take-one-big-story-of-the-day/cyber-criminals-are-getting-smarter-laws-and-awareness-need-to-keep-up/90377/1