DOI: https://doi.org/10.36094/sc.v92.2026.Role_of_ICT_in_Cyber_Awareness.Bera_Bera.152

ARTICLE

Sci. and Cult. 92 (1–2) : 152-154 (2026)

ROLE OF ICT IN CYBER AWARENESS FOR RURAL DEVELOPMENT

SOUVIK BERA[1] AND ANIRBAN BERA[1]*

Rural areas now require all forms of digital development and growth because people might not be very familiar with technology, the internet, and other digital tools are not fully accessible, and individuals lack sufficient information about internet security. The widespread use of smartphones, online banking, government services, and social media has created opportunities for rural residents to improve their lives, but it has also exposed them to threats such as scams, identity theft, fake information, and misuse of personal data. This review examines the impact of technology on how rural individuals are educated about cyber dangers, the challenges they encounter, the tools currently available, and new technological solutions. These include local training, safe use of digital tools, awareness-building applications, regional-language lessons, and AI-based safety services. The findings show that understanding cyber risks is essential not only for safety but also for long-term rural development.

Introduction

The pace of digital change among rural areas has been fuelled in the last ten years by the growing accessibility of smartphones, the growth of mobile networks, affordable data charging platforms, and the popularity of e-governance systems. Online financial transactions, tele-health, online learning, digital agriculture platforms and government benefits via ICT systems are some of the rural activities undertaken by the citizens. As per national surveys, over fifty percent of the internet users living in India are in the rural regions, and the number keeps on increasing with every passing year[1]. Although this change will help to empower rural people and boost the economy, it also subjects digitally-unsophisticated nations to cybercrimes like phishing, UPI frauds, malware, identity theft, and misinformation. Research has always shown that rural customers are more susceptible to cyber exploitation because of poor cyber literacy, unawareness, weak security measures, and overreliance on smartphones to complete nearly all online activities. ICT is a two-fold catalyst in rural development and also in reducing cyber awareness. ICTs like mobile applications, online learning platforms, WhatsApp chat rooms, government websites, and community radio have become effective platforms through which cyber safety is communicated[2]. The purpose of this review is to assess the role of ICT in facilitating cyber awareness, assess the problem of rural areas, and suggest ways of enhancing the practice of cyber hygiene. The work is based on the synthesis of the recent research, field surveys, and governmental efforts to make an updated picture of the rural cybersecurity situation.

ICT Contribution Towards Cyber Awareness

ICT has been used as a potent tool to disseminate cyber knowledge, enhance security systems and decrease the digital awareness gap in rural societies[4]. It promotes communication, education, monitoring and capacity building using mobile phones, local radio, IVR services, social media and village digital centers. The Multimedia content (videos, audio message, infographics, and short animations) will assist the first-generation digital users to grasp the basic practices like password safety, safe

1 Assistant Professor, Brainware University, Kolkata, India

* Corresponding author: anb.es@brainwareuniversity.ac.in

browsing, online payments, and fraud detection. Audio visual learning is found to enhance retention and ICT plays an essential role in cyber safety education. Through government interventions such as DISHA, PMGDISHA, DIKSHA, Cyber Swachhta Kendra and CERT-In ICT modules in local languages are also being utilised to prevent unsafe digital practices. Real-time alerts on threats are also facilitated by ICT in the form of SMS, mobile warnings and AI-operated anomaly alerts that are used by banks and fintech applications. WhatsApp group, SHGs, and farmer collectives also enhance awareness on cultural environments that are well understood. Also, ICT eases the reporting of cyber incidents by using helplines such as 1930 and web portals to seek immediate help and awareness of the law[3].

Difficulties

ICT presents a great prospect of raising the awareness of rural people on cyber, but some obstacles interfere with its proper use. Digital literacy gap is the most significant obstacle because most people who are the first and have used a smartphone do not have simple knowledge about device settings, privacy settings, app permissions and safe browsing. Even though ICT can be used in learning, rural users find it difficult to use digital interfaces, and studies indicate that they can only have partial knowledge unless they receive regular and frequent training. Inaccessibility of language is also a constraint of program effectiveness. Although government portals provide multilingual functionalities, most of the cybersecurity materials, particularly technical advice, are provided only in English or Hindi. Information presented in local dialects is more meaningful to older learners especially, although region specific learning materials are wanting. ICT reach is also lowered by infrastructure limitations. Access to video-based modules is inhibited by poor connectivity, low bandwidth, and old or low-storage devices, which demoralize the participation of learners. Leveraging on cheap smartphones makes one prone to cyber-attacks and restrictions on more robust security measures. There are behavioural issues that add to the challenges. In the rural community, interpersonal trust is so high that many users do not fear sharing OTPs, passwords, or Aadhaar numbers, which is used to commit social engineering attacks[9-10]. These behaviours take time and a culturally relevant ICT interaction to change. Making matters worse is the fact that few trained cybersecurity educators are available; most of these programs use teachers or volunteers that lack sufficient technical expertise. Socio-economic factors such as low income, low education, gender imbalance, and device addiction amplify the digital participation more so among women and the aged. Cyber threats are constantly changing and require the current changes and co-ordination of government agencies, telecom providers and local institutions to sustain effective ICT-based awareness measures in the rural regions.

Analysis

The trends in cyber awareness in rural India help to identify a significant disparity between the digital use and digital safety. In a survey carried out by the authors in 2023, it was discovered that 68 percent of non-urban digital users did not have basic cybersecurity research, such as finding phishing links or applying two-factor authentication. Additionally, 72 percent had not been trained on cyber safety at all, and this indicates a great lack of awareness. The most frequently used cybercrime is mobile payment fraud, and 40% of users have received fraudulent calls or messages with rewards[5]. Research also indicates that the rural women are also more susceptible to impersonation through social media because their privacy settings are weak. According to the government statistics, cybercrime reporting increased sharply, with complaints in semi-urban and rural districts increasing by 70-100 percent between 2021 and 2024 due to the introduction of more and more digital payments and easier reporting of complaints. It is also proved by research that ICT-based interventions are efficient. Role-play video and gamified module experiments resulted in the increase of the ability to detect fraud by 35-50 percent and vernacular voice-based modules were the most adopted ones. All in all, ICT can be viewed as a weak point, but also a potent facilitator of cyber awareness, where the long-term approaches to rural population should be situation-sensitive[7-8]. The major metrics in the chart are the level of awareness, training gaps, exposure to fraud, increase in

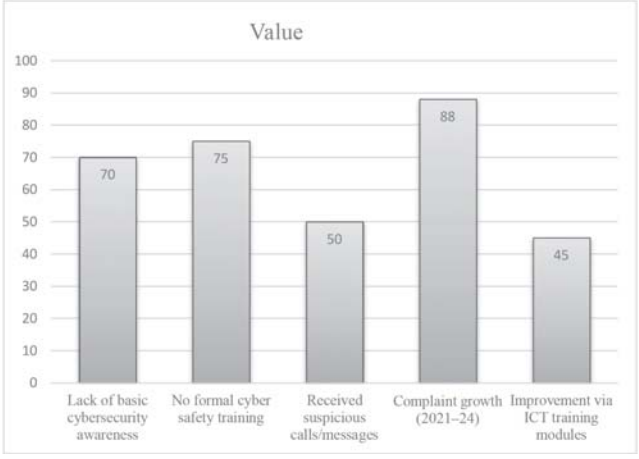

Fig. 1: Key Cyber Awareness Indicators in Rural India

the number of complaints and the percentage of improvements using ICT is given in fig 1.

Solutions and Recommendation

To maximize ICT's role in rural cyber awareness, several strategies are essential. Vernacular multimedia content—local audio-visual modules, short videos, and IVR systems can effectively reach users of varied literacy levels. Cyber awareness should be integrated into all public digital services through ICT-based safety toolkits for CSCs, banks, and SHGs. Village cyber kiosks can serve as resource hubs for training and support[6]. AI-enabled safety features on low-end smartphones, school-based digital literacy, and periodic ICT reminders via WhatsApp or SMS can reinforce safe behaviour. Empowering local digital champions and ensuring affordable data, devices, and community Wi-Fi can bridge digital gaps[9].

Conclusion:

The importance of ICT in cyber awareness and protection of the rural communities in an ever-increasing digital world has been observed to be very critical and multi-dimensional. Since the rural people are switching to digital payment systems, online government, agricultural e-platforms, and social media communications, their vulnerability to cyber threats also increases. The risk medium and the most appropriate risk mitigation tool is ICT. Even in the face of digital illiteracy, language barriers and infrastructural issues, ICT-based solutions can make a significant contribution to cyber hygiene provided they are created in an inclusive and context-specific manner. Enhancement of ICT-based awareness measures by use of localized content, community education, AI-based safety measures, and policy facilitation will empower the rural population to engage in digital economy in a more confident and safe way. Rural development over the long term will require more than just digital connectivity, but it must also create resilient and cyber-conscious communities. ❐

References

1. S. Raghavan and L. Parthiban, *International Journal of Innovative Research in Computer and Communication Engineering*, **7**, 5, 2019.
2. S. Rani and V. Kumar, *Journal of Rural Development*, **40**, 3, 2021.
3. P. Singh and G. Kaur, *International Journal of Advanced Research in Computer Science*, **10**, 5, 2019.
4. A. Gupta and A. Jain, "UPI Fraud and Cyber Awareness in Rural India: An Empirical Study." Journal of Financial Crime, Emerald Publishing, 2022.
5. A. Thomas and S. George, *Telematics and Informatics*, Elsevier, **58**, 2021.
6. S. Verma and A. Kumari, *Indian Journal of Public Administration*, **67**, 2, 2021.
7. N. Chawla and S. Bhatt, "ICT Interventions for Digital Literacy in Developing Countries." *Information Development*, SAGE, 2020.
8. CERT-In. "Annual Cyber Security Report." Ministry of Electronics and IT, Government of India, 2023.
9. R. Sharma, "Mobile-Based Cybersecurity Training for Rural Users." *Education and Information Technologies*, Springer, 2022.
10. P. Kumar and S. Sahu, "Socio-Technical Dimensions of Cybersecurity in Rural India." *Journal of Information Security and Applications*, Elsevier, 2023.