



Role of Digital Literacy Awareness Programme in Preventing Cyber Crime among Rural Communities of Durg District, Chhattisgarh

*Pranjal Verma¹, Subuhi Nishad², Payal Jaiswal³ and Gagendra Singh Rajput⁴

¹Department of Floriculture and Landscaping, College of Horticulture and Research Station, Sankara, Patan, Mahatma Gandhi Udyanikee Evam Vanikee Vishwavidyalaya, Durg, Chhattisgarh, 491111, India

²NSS Co-ordinator, IGKV, Raipur, Chhattisgarh, 492012, India

³NSS Programme Officer, IGKV, Raipur, Chhattisgarh, 492012, India

⁴NSS Programme Officer, Mahatma Gandhi Udyanikee Evam Vanikee Vishwavidyalaya, Durg, Chhattisgarh, 491111, India

*Corresponding Author's email: pranjalbmkj14@gmail.com

Cyber crime has emerged as a major concern with the rapid growth of internet use, smartphones, social media, online banking, and digital payment services. Lack of awareness and unsafe digital practices can increase an individual's vulnerability to phishing, online financial fraud, identity theft, hacking, cyber bullying, malware, and other cyber threats. The findings indicated that respondents possessed a basic level of awareness regarding common cyber crimes; however, gaps were observed in the consistent adoption of recommended digital safety practices such as using strong and unique passwords, enabling two-factor authentication, verifying suspicious links and websites, and protecting personal and financial information. The study emphasizes that awareness alone may not always lead to safe online behaviour. Continuous and practical cyber safety awareness programmes are therefore essential to improve digital literacy, encourage responsible online behaviour, and reduce vulnerability to cyber crime. Strengthening public awareness and preventive practices can contribute significantly to creating a safer digital environment.

Keywords: Cyber crime, Cyber awareness, Digital safety, Cybersecurity, Online fraud, Phishing, Digital literacy, Preventive measures, Internet safety, Cyber security awareness.

Introduction

The rapid growth of information and communication technology has transformed the way people communicate, access information, perform financial transactions, and use essential services. The increasing use of smartphones, social media, online banking, digital payment platforms, and other internet-based services has made daily life more convenient. However, this rapid digital expansion has also increased the risk of cyber crimes and other online threats. Cyber crime refers to illegal activities carried out using computers, mobile devices, networks, or the internet, including phishing, identity theft, online financial fraud, hacking, cyberbullying, malware attacks, and misuse of personal information. Cyber crime has become a significant concern because individuals may unknowingly share sensitive information, click on fraudulent links, use weak passwords, or interact with unverified websites and applications. Lack of awareness about common cyber threats and safe digital practices can make individuals particularly vulnerable to financial loss, identity theft, privacy violations, and psychological distress.

Digital safety involves responsible and secure use of digital devices, online platforms, applications, and internet services. Practices such as using strong and unique passwords, enabling two-factor authentication, regularly updating software, avoiding suspicious links and attachments, protecting personal information, verifying online communications, and reporting cyber incidents can significantly reduce the risk of cyber attacks. Therefore, improving awareness and promoting safe digital behaviour are essential components of cyber crime prevention. Awareness programmes can play an important role in educating individuals about different forms of cyber crime, warning signs of online fraud, methods of protecting personal and financial information, and appropriate steps to take when a cyber incident occurs. Such programmes can help develop responsible digital behaviour and encourage individuals to use technology safely and confidently.

Materials and Methods

The study was conducted among selected individuals from the study area. The respondents were approached at their respective educational institutions, workplaces, community settings, or other accessible locations depending upon the study population. The study population consisted of individuals who regularly used digital devices and internet-based services such as smartphones, social media, online banking, digital payment applications, and other online platforms.

Data Collection Tool

- Awareness regarding different types of cyber crimes.
- Knowledge of common online threats such as phishing, identity theft, online fraud, hacking, malware, and cyberbullying.
- Awareness of digital safety practices.
- Password and account security practices.
- Safe use of social media and digital payment platforms.
- Awareness regarding reporting cyber crime.
- Preventive measures adopted by the respondents.

Data Collection Procedure

Before data collection, the purpose of the study was explained to the respondents. Informed consent was obtained from the participants. The questionnaire was distributed to the selected respondents and sufficient time was provided for completion. The completed questionnaires were collected and checked for completeness. Confidentiality and privacy of the respondents were maintained throughout the study.

Results and Discussion

The findings indicated that most respondents were regular users of smartphones and internet-based services, including social media, online banking, digital payment applications, and online communication platforms. A majority of respondents were aware of online financial fraud, phishing, hacking, identity theft, and cyberbullying. However, some respondents had limited knowledge regarding sophisticated cyber threats, fraudulent websites, malicious applications, and methods used by cyber criminals to obtain personal information. Regarding digital safety, many respondents reported using passwords to protect their accounts and were aware of the importance of keeping personal information confidential. However, practices such as regularly changing passwords, using unique passwords for different accounts, enabling two-factor authentication, checking website authenticity, and avoiding suspicious links were not consistently followed by all respondents.

The findings related to preventive measures showed that respondents commonly avoided sharing passwords, personal identification details, and banking information with unknown persons. Many respondents also reported being cautious while receiving unknown messages or calls. However, there was a need for greater awareness regarding reporting cyber crime, securing social media accounts, identifying phishing attempts, and taking immediate action after a cyber incident.

Future Scope

1. Conduct regular cyber crime awareness programmes in schools, colleges and rural communities.
2. Promote safe practices such as strong passwords, two-factor authentication and privacy protection.
3. Increase awareness about online fraud, phishing, cyber bullying and identity theft.
4. Encourage people to report cyber crimes promptly through appropriate cyber crime portals and authorities.
5. Develop digital safety training programmes for vulnerable and less digitally literate groups.
6. Use social media and digital platforms to spread updated information about emerging cyber threats.

Conclusion

The present indicates that although individuals are generally aware of common cyber crimes such as phishing, online financial fraud, hacking, identity theft, and cyber bullying, gaps may exist between knowledge and the actual practice of safe digital behaviour. The findings emphasize the need for individuals to adopt essential preventive measures such as using strong and unique passwords, enabling two-factor authentication, avoiding suspicious links and messages, protecting personal and financial information, regularly updating digital devices, and verifying websites and online communications before sharing information. Individuals should also be aware of appropriate mechanisms for reporting cyber crimes and should take prompt action when suspicious activities occur. Cyber security awareness should be considered a continuous process rather than a one-time activity. Regular awareness programmes, practical demonstrations, educational campaigns, and community-based training can improve digital safety practices and encourage responsible use of technology. Educational institutions, workplaces, government agencies, and digital service providers can play an important role in strengthening cyber security awareness.

References

1. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), 1049–1092.
2. Alshaikh, M., et al. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73, 102258.
3. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778.
4. Spicer, M., & Nurse, J. R. C. (2026). What makes people susceptible to phishing attacks: A systematic literature review and future research agenda. *Computers & Security*, 105096. <https://doi.org/10.1016/j.cose.2026.105096>
5. Tallyn, E., et al. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security*, 139, 103695.
6. A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness. (2024). *Journal of Systems and Software*, 208, 111899.
7. A systematic review of current cybersecurity training methods. (2024). *Computers & Security*, 136, 103585.
8. CERT-In. (2026). Cyber Security Awareness Booklets and Digital Safety Resources. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.
9. CERT-In. (2026). Digital Threat Report 2025–26. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.
10. Okeke, D. C. (2026). The impact of cybersecurity awareness on phishing attack vulnerability. *Journal of Cyber Security*, 8, 281–317. <https://doi.org/10.32604/jcs.2026.079750>