BIO PHARMACEUTICAL SCIENCE AND RESEARCH JOURNAL ISSN: 3049-2599

DOI: https://doi.org/10.63712/bpsrj-v2i1p008

AWARENESS OF CYBER SECURITY IN MOBILE DEVICE USAGE AMONG RURAL POPULATIONS

AWARENESS OF CYBER SECURITY IN MOBILE DEVICE USAGE AMONG RURAL POPULATIONS

M. Venkat, G. Rajesh, Dept. of Information Technology, C. K. Thakur A.C.S. College, New Panvel, Maharashtra.

ABSTRACT:

The rapid penetration of smartphones has significantly transformed communication, information access, and daily activities, particularly in rural regions. Despite these advantages, mobile devices are increasingly vulnerable to cyber threats due to limited user awareness and unsafe usage practices.

This study investigates the level of cyber security awareness among rural users while handling mobile devices, with particular emphasis on risks such as malware, phishing, unauthorized access, and data privacy breaches.

A survey-based approach was adopted to analyze user behavior, security practices, and knowledge levels related to mobile cyber security. The findings reveal that although rural users possess basic operational knowledge of smartphones, awareness of advanced security features and protective applications remains inadequate. The study highlights the urgent need for structured cyber security awareness programs to enhance safe mobile usage in rural areas

Keywords: Cyber security awareness, Mobile device security, Rural users, Smartphone threats, Data privacy, Malware attacks

INTRODUCTION:

Mobile computing has emerged as a dominant paradigm in modern information technology, driven by the widespread adoption of smartphones, tablets, and portable computing devices. These devices combine high processing power, advanced operating systems, and constant internet connectivity, enabling users to perform a wide range of personal and professional tasks anytime and anywhere. The affordability and portability of mobile devices have led to their increased usage over traditional desktop systems, especially in rural and semi-urban regions.

However, universal connectivity and the expansion of Internet of Things (IoT) ecosystems have significantly increased the attack surface for cybercriminals. Modern smartphones are equipped with sensors such as GPS, cameras, microphones, accelerometers, and wireless interfaces, which, if compromised, can expose sensitive personal and organizational data. The absence of a secure organizational perimeter and the rise of Bring Your Own Device (BYOD) practices further amplify security risks.

As cybercriminal activities continue to evolve, mobile devices have become attractive targets for attacks including malware infections, man-in-the-

DOI: https://doi.org/10.63712/bpsrj-v2i1p008

AWARENESS OF CYBER SECURITY IN MOBILE DEVICE USAGE AMONG RURAL POPULATIONS

middle attacks, phishing, and unauthorized data access. These risks are more pronounced in rural areas where users often lack formal cyber security training. Therefore, understanding the awareness level of rural populations regarding mobile cyber security is crucial for designing effective preventive strategies.

AIM AND OBJECTIVES

Aim

The primary aim of this study is to assess the level of awareness regarding cyber security practices among rural population while using mobile devices and to identify the security challenges they face in their day-to-day smartphone usage.

Objectives

- To evaluate the level of awareness about cyber security among rural mobile users.
- To analyze the security practices adopted by users to protect their mobile devices.
- To identify common cyber threats encountered while using smartphones in rural areas.
- To examine user behavior related to mobile application usage and permission management.
- To assess the understanding of advanced security features such as data encryption and remote wipe.
- To determine the need for cyber security awareness programs among rural populations

LITERATURE REVIEW

Previous studies emphasize the growing severity of mobile security threats. Leavitt (2011) highlighted that the rapid adoption of smartphones has created new vulnerabilities, primarily due to insecure application downloads and weak user awareness.

Bhattacharya et al. (2014) focused on the importance of mobile security education and proposed laboratory-based learning to enhance student engagement and understanding of mobile security concepts.

Wang et al. (2005) introduced a security framework for mobile agent systems, emphasizing the concept of “sufficient security” rather than absolute protection.

Asghar et al. (2008) proposed a security model aimed at protecting confidential data stored on mobile devices through secure authentication mechanisms.

Yoon et al. (2015) discussed hardware-based mobile security solutions to prevent unauthorized access and data leakage in smart devices.

Although extensive research exists on mobile security technologies, limited studies focus specifically on cyber security awareness among rural populations, indicating a significant research gap addressed by this study.

DOI: https://doi.org/10.63712/bpsrj-v2i1p008

AWARENESS OF CYBER SECURITY IN MOBILE DEVICE USAGE AMONG RURAL POPULATIONS

MATERIAL AND METHODS:

Research Design

The study adopted a descriptive research design using a survey-based approach to collect primary data from rural mobile device users.

Study Area

The research was conducted in selected rural areas of Raigad district, Maharashtra, India.

Sample Size

A total of 100 respondents were selected for the study using random sampling techniques.

Data Collection Tool

A structured questionnaire was developed and distributed through Google Forms. The questionnaire included both multiple-choice and close-ended questions related to:

- Mobile authentication methods
- App update practices
- Data backup and encryption
- Awareness of cyber security threats
- Permission management and rooting practices
- Usage of security applications

Data Collection Method

Primary data was collected directly from respondents through online survey forms. Secondary data was collected from published research papers, journals, and conference proceedings related to mobile cyber security.

Statistical Tools Used

The collected data was analyzed using:

- Percentage analysis
- Graphical representation
- Chi-square test to test the hypothesis related to awareness of cyber security among rural users.

Methodology

A survey-based research methodology was employed for this study. A structured questionnaire was designed to collect data on mobile security practices, awareness levels, and user behavior. The survey focused on issues such as malicious applications, data encryption, permission management, rooting practices, and general cyber security awareness.

PROBLEM STATEMENT

The increasing dependence on mobile devices, coupled with inadequate cyber security awareness, exposes rural users to various digital threats. The lack of knowledge regarding secure mobile practices, unsafe application usage, and insufficient understanding of data protection mechanisms results in heightened vulnerability to cyber-attacks.

CHALLENGES IN MOBILE CYBER SECURITY

Mobile devices present several security challenges due to their design and usage patterns:

DOI: https://doi.org/10.63712/bpsrj-v2i1p008

AWARENESS OF CYBER SECURITY IN MOBILE DEVICE USAGE AMONG RURAL POPULATIONS

Malicious Hotspots

Cybercriminals often create fake public Wi-Fi hotspots to capture sensitive user data such as login credentials and personal information.

Man-in-the-Middle Attacks

Attackers intercept communication between devices and networks, allowing unauthorized monitoring or data manipulation.

Shadow IT

The use of unapproved applications for storing or sharing data increases organizational and personal security risks.

Phishing and Spoofing

Fraudulent messages and emails disguised as trusted sources can deceive users, especially on small mobile screens.

Device Theft and Loss

Lost or stolen devices can lead to unauthorized access to personal contacts, emails, and confidential files.

MOTIVATION OF THE STUDY

Mobile technology has become an integral part of everyday life, supporting activities ranging from communication to online banking.

Rural users frequently install applications and share personal data without adequate consideration of security implications. Factors such as easy access to information, reduced technological costs, rapid data availability, and personalized services have accelerated mobile adoption, making cyber security awareness essential for safe usage.

SAMPLING DESIGN AND DATA COLLECTION

A sample of 100 respondents was selected from various rural areas of Raigad district. Data was collected using online questionnaires distributed through Google Forms. The responses were validated to ensure consistency and completeness.

DATA ANALYSIS AND INTERPRETATION

The collected data was analyzed using descriptive statistics and the chi-square test.

Results indicate that a significant proportion of respondents use fingerprint authentication, regularly update applications, and are familiar with features such as data encryption and remote wipe.

However, a large number of users do not install security applications or fully understand advanced cyber threats such as social engineering.

The chi-square analysis confirmed that awareness regarding secure mobile handling exists among rural users, although it remains at a moderate level.

DOI: https://doi.org/10.63712/bpsrj-v2i1p008

AWARENESS OF CYBER SECURITY IN MOBILE DEVICE USAGE AMONG RURAL POPULATIONS

RESULTS

The analysis of survey data revealed the following key findings:

- A significant proportion of respondents use fingerprint authentication to secure their smartphones.
- Nearly half of the respondents regularly update mobile applications, indicating moderate awareness of security updates.
- More than half of the users are aware of data encryption and remote wipe features, though practical usage varies.
- A considerable number of respondents have used rooted devices, which increases vulnerability to cyber attacks.
- About 50% of users have not installed any security applications, reflecting a lack of awareness regarding protective software.
- Knowledge of social engineering attacks was found to be basic or inadequate among most respondents.

The chi-square test results indicate that the null hypothesis (H_0) stating that awareness of secure mobile handling exists among rural users is accepted.

DISCUSSION

The findings of this study indicate that rural users possess a basic understanding of mobile device operation and certain security features such as authentication and app updates. However, awareness of comprehensive cyber security practices remains limited. While users demonstrate familiarity with features like fingerprint security and permission verification, the low adoption of antivirus and firewall applications highlights a critical gap in preventive security measures.

The widespread use of rooted devices and limited knowledge of social engineering techniques further expose rural users to cyber threats such as malware infections, data breaches, and phishing attacks. These results are consistent with previous studies that emphasize the role of user awareness as a key factor in mobile cyber security.

The study underscores the necessity of implementing targeted cyber security awareness programs in rural areas through digital literacy campaigns, educational workshops, and community outreach initiatives. Enhancing user knowledge will significantly reduce cyber risks and promote safer mobile device usage.

CONCLUSION

The findings of this study demonstrate that rural populations exhibit an above-average but insufficient level of cyber security awareness in mobile device usage. Although users are familiar with basic security features, limited knowledge of advanced protection mechanisms exposes them to cyber risks. Strengthening cyber security awareness through training programs, community workshops, and digital literacy initiatives is

DOI: https://doi.org/10.63712/bpsrj-v2i1p008

essential to ensure safe and secure mobile technology adoption in rural areas.

REFERENCE:

1. Yoon, S., Jeon, Y., & Kim, J. (2015). Mobile security technology for smart devices. International Conference on ICT Convergence.
2. Bhattacharya, P., Yang, L., Guo, M., Qian, K., & Yang, M. (2014). Learning mobile security with labware. IEEE Security & Privacy.
3. Leavitt, N. (2011). Mobile security: Finally a serious problem? Computer.
4. Asghar, M. T., Riaz, M., Ahmad, J., & Safdar, S. (2008). Security model for the protection of sensitive data on mobile devices.
5. Wang, S., Hu, J., Liu, A., & Wang, J. (2005). Security framework in mobile agent systems.

Source of Support: Nil. **Conflicts of Interest:** None