iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** XI **Month of publication:** November 2026

DOI: https://doi.org/10.22214/ijraset.2026.85643

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue XI Nov 2026- Available at www.ijraset.com

Cyber Security: Workshops on Fraud, Phishing Awareness, and Secure Online Transactions

Yogesh Putpakajwar[1], Taha Sheikh[2], Rohit Mankar[3], Tanmay Rathod[4], Om Wankhade[5], Gaurav Waghole[6], Ms. Nikita Datta Chandure[7]
Computer Science and Engineering, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal

Abstract: ***The increasing use of the internet, social media, digital banking, and online payment applications has made daily activities easier. However, it has also increased the risk of cyber fraud, phishing attacks, identity theft, and online transaction scams. Many users may not have sufficient knowledge of these threats or the precautions required to protect their personal and financial information.***
This research paper focuses on creating cyber security awareness through workshops, educational activities, and a survey of 35 participants. The study examines awareness of common online frauds, phishing messages, social media risks, and secure online transactions. The survey was conducted using Printed Questionnaires among 9th and 10th Standard School Students. The collected responses were analysed to identify awareness gaps and common security practices.
The proposed approach emphasizes practical demonstrations, simple educational materials, and awareness sessions to encourage safe digital behaviour. The study aims to help users recognize suspicious activities, protect sensitive information, and use digital payment services more safely.
Keywords: Cyber Security, Phishing Awareness, Online Fraud, Digital Payments, Cyber Safety, Awareness Workshops.

I. INTRODUCTION

Cyber security refers to the protection of computers, mobile devices, networks, applications, and personal information from unauthorized access, attacks, and misuse. In today's digital world, people use the internet for education, communication, banking, shopping, and financial transactions. Although digital services provide convenience, they also expose users to various cyber threats. Cybercriminals may use fake websites, fraudulent phone calls, suspicious messages, and misleading social media posts to steal personal information or money. Phishing is a common cyberattack in which attackers pretend to be trusted individuals or organizations to obtain sensitive information. Online fraud may involve fake job offers, lottery messages, fraudulent payment requests, impersonation, and deceptive investment schemes. Secure online transactions require users to follow basic safety practices, such as verifying payment details, protecting their PINs and passwords, and avoiding suspicious links. The Indian Computer Emergency Response Team (CERT-In) and the Reserve Bank of India (RBI) provide guidance to help users recognize and prevent online scams [1], [2], [4]. Therefore, cyber security awareness is important for students and the general public. Educational workshops and community awareness activities can communicate essential safety practices in a simple and practical way.

A. Problem Statement

Many internet users rely on digital services without fully understanding the risks associated with suspicious links, fake websites, fraudulent calls, social media scams, and unsafe online transactions. This creates a need for accessible cyber security education and awareness activities.

B. Objectives

The main objectives of this study are:

- To study awareness of common cyber frauds and phishing attacks.
- To understand users' knowledge of secure online transactions.
- To identify common cyber security awareness gaps through a survey.
- To promote safe use of social media and digital payment applications.
- To propose awareness workshops and practical educational activities.
- To encourage responsible and secure digital behaviour.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue XI Nov 2026- Available at www.ijraset.com

II. LITERATURE SURVEY AND EXISTING SYSTEM

Cyber security awareness has become an important part of digital safety. Government organizations and financial institutions publish guidelines to help people identify online threats and protect their information.

CERT-In provides educational material on phishing websites, online scams, suspicious links, and safe digital practices. Its guidance recommends checking links carefully, avoiding unknown applications, and protecting sensitive information [1].

The Reserve Bank of India provides information about safe digital banking. Its guidance advises users not to disclose passwords, PINs, OTPs, or other confidential banking details and to avoid suspicious links received through messages or social media [2].

The National Payments Corporation of India (NPCI) also provides fraud awareness information relating to UPI payments, fake cashback offers, QR codes, and fraudulent payment requests [3].

A. Existing System

Existing cyber security awareness methods include:

- Online articles and educational websites.
- Government awareness campaigns.
- Banking safety messages and notifications.
- Social media awareness posts.
- Cyber security seminars and workshops.

B. Limitations of Existing Awareness Methods

Information may be available online, but not every user reads or understands it. Some users may not recognize scam techniques when they encounter them in real situations. Language barriers, limited practical exposure, and a lack of regular awareness activities can also reduce the effectiveness of cyber safety education.

The present study focuses on communicating safety information through a survey-based assessment and a proposed practical awareness approach.

III. RESEARCH METHODOLOGY

The study follows a survey-based approach to understand people's awareness of cyber security threats and safe online behaviour.

A. Research Design

A descriptive survey method is used to collect information about participants' awareness of phishing, online fraud, social media security, and digital payment safety.

B. Data Collection

The survey was conducted among 35 participants belonging to 9th and 10th Standard School Students in Vedharini Vidyalaya, Pimpalgaon, Yavatmal. Data were collected through printed questionnaire.

The questionnaire included questions about:

- Awareness of phishing messages and suspicious links.
- Recognition of fraudulent phone calls and online offers.
- Knowledge of OTP, UPI PIN, and password safety.
- Use of privacy and security settings on social media.
- Previous exposure to online scams.
- Interest in participating in cyber security awareness activities.

C. Data Analysis

The collected responses were organized and analysed using counts and percentages. The findings were used to identify areas where additional cyber security education may be useful.

The percentage for each response can be calculated as:

$$Percentage = (Number\ of\ responses\ in\ a\ category / Total\ valid\ responses) \times 100$$

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Ethical Considerations

Participation should be voluntary. Personal banking details, passwords, OTPs, and other sensitive information must not be collected. Survey findings should be reported honestly, and participants' identities should be protected.

IV. SURVEY APPROACH AND FINDINGS

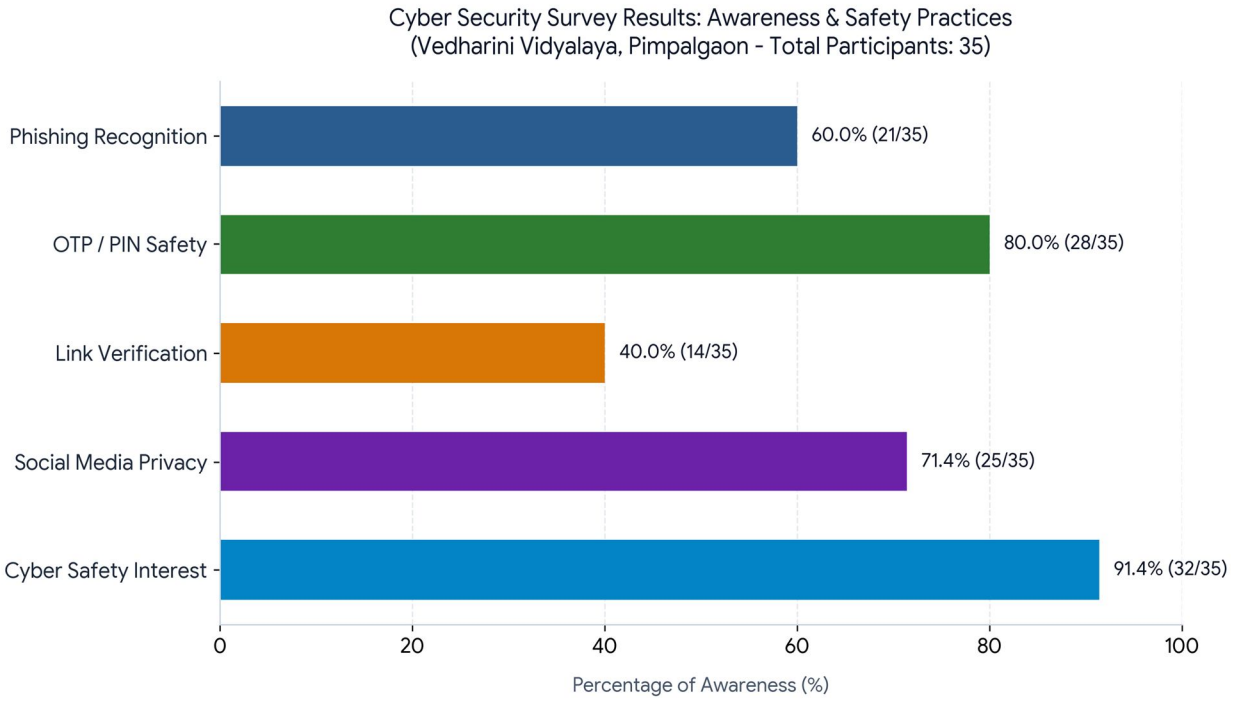
The survey aimed to understand participants' awareness of common online threats and secure digital practices. The questionnaire covered phishing messages, suspicious links, online payment safety, social media privacy, and common fraud techniques.

- Total participants: 35
- Participant group: 9th and 10th Standard School Students
- Survey location: Vedharini Vidyalaya, Pimpalgaon, Yavatmal.
- Data collection method: Printed Questionnaire
- Survey period: On Date-17/10/2026

A. Survey Results

The results should be presented using the actual responses collected during the survey.

Survey Indicator	Result (Number / Percentage)
Participants who recognize phishing	21 (60%)
Participants who know not to share OTPs or PINs	28 (80%)
Participants who verify suspicious links	14 (40%)
Participants aware of social media privacy risks	25 (71.4%)
Participants interested in cyber safety awareness	32 (91.4%)



B. Discussion

The survey responses can help identify the topics in which participants have sufficient knowledge and the topics requiring further awareness. For example, if respondents have difficulty identifying suspicious links, educational activities can focus on checking website addresses, verifying senders, and avoiding unexpected attachments.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

If participants show limited knowledge of digital payment safety, the awareness activity can explain the importance of protecting payment credentials and verifying the recipient before making a transaction.

The discussion should be finalized after reviewing the actual survey results. No numerical findings should be assumed without supporting data.

V. PROPOSED APPROACH: CYBER SECURITY AWARENESS ACTIVITIES

Since students represent the core demographic vulnerable to online risks, tailoring these awareness workshops directly to school students ensures maximum safety and preventive impact.

A. Awareness Workshop

An awareness session can explain common cyber threats using simple language, examples, posters, and presentations. The topics may include phishing, fake job offers, fraudulent calls, social media impersonation, and online payment scams.

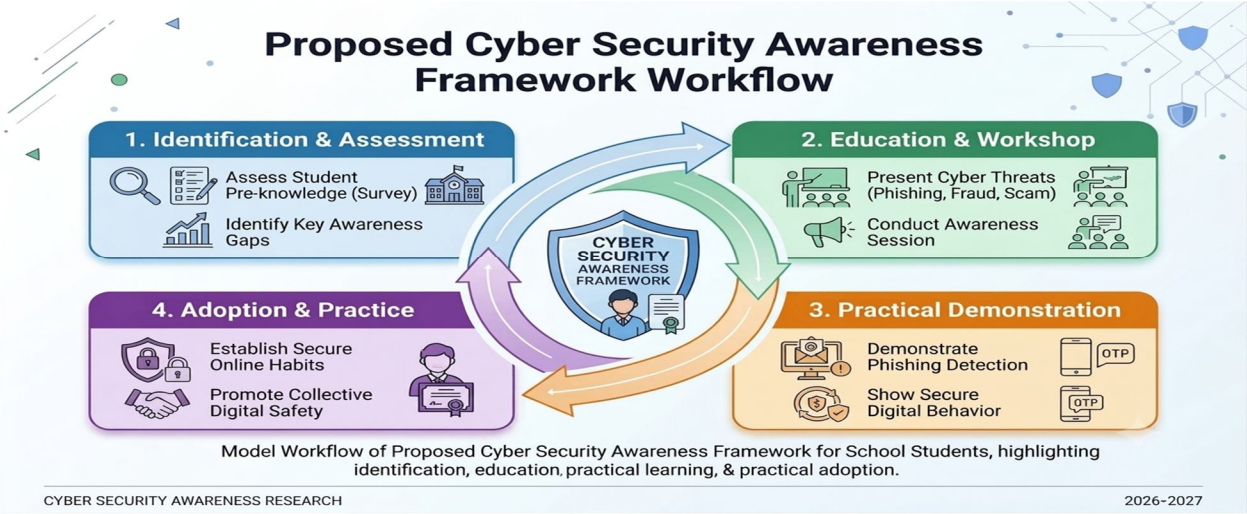
B. Phishing Awareness

Participants can learn to identify warning signs such as:

- Unexpected messages requesting urgent action.
- Links leading to unfamiliar or misleading websites.
- Requests for passwords, OTPs, or banking information.
- Fake offers, prizes, or account suspension warnings.
- Messages pretending to come from trusted organizations.

Demonstrations should use safe, fictional examples rather than collecting participants' real credentials.

Model Workflow of Proposed Cyber Security Awareness Framework for School Students.



C. Secure Online Transactions

Participants should be encouraged to follow these practices:

- Never share an OTP, UPI PIN, password, or CVV with another person.
- Verify the recipient and amount before confirming a payment.
- Remember that receiving money through UPI does not require entering a UPI PIN.
- Avoid unknown payment links and suspicious QR codes.
- Use official applications and verified websites.
- Enable appropriate device locks and account security features.
- Contact the bank promptly if an unauthorized transaction occurs.

These recommendations are consistent with official RBI and NPCI safety guidance [2], [3].

D. Social Media Safety

Participants should use strong, unique passwords, enable two-factor authentication where available, review privacy settings, avoid accepting suspicious requests, and verify unusual messages from friends or relatives through another trusted channel.
They should also avoid sharing sensitive personal information publicly and report suspicious accounts through the platform's official reporting mechanism.

E. Evaluation of Awareness Activities

If an awareness session is conducted, participants may complete a short questionnaire before and after the session. Comparing the two sets of responses can help assess changes in knowledge.
If no workshop or post-session assessment has yet been conducted, this evaluation should be presented as a proposed activity rather than a completed result.

VI. CONCLUSION

Cyber security awareness is essential for safer use of the internet, social media, digital banking, and online payment services. Phishing, fraudulent messages, impersonation, and deceptive payment requests can expose users to financial and privacy risks.
This study uses a survey-based approach to examine awareness of common cyber threats and identify topics requiring further education. The proposed approach emphasizes practical demonstrations, accessible educational material, and awareness activities.
By improving knowledge of suspicious links, password protection, UPI safety, and social media privacy, cyber security education can encourage more responsible digital behaviour. The final conclusions of the study should be based on the actual survey findings.

VII. FUTURE SCOPE

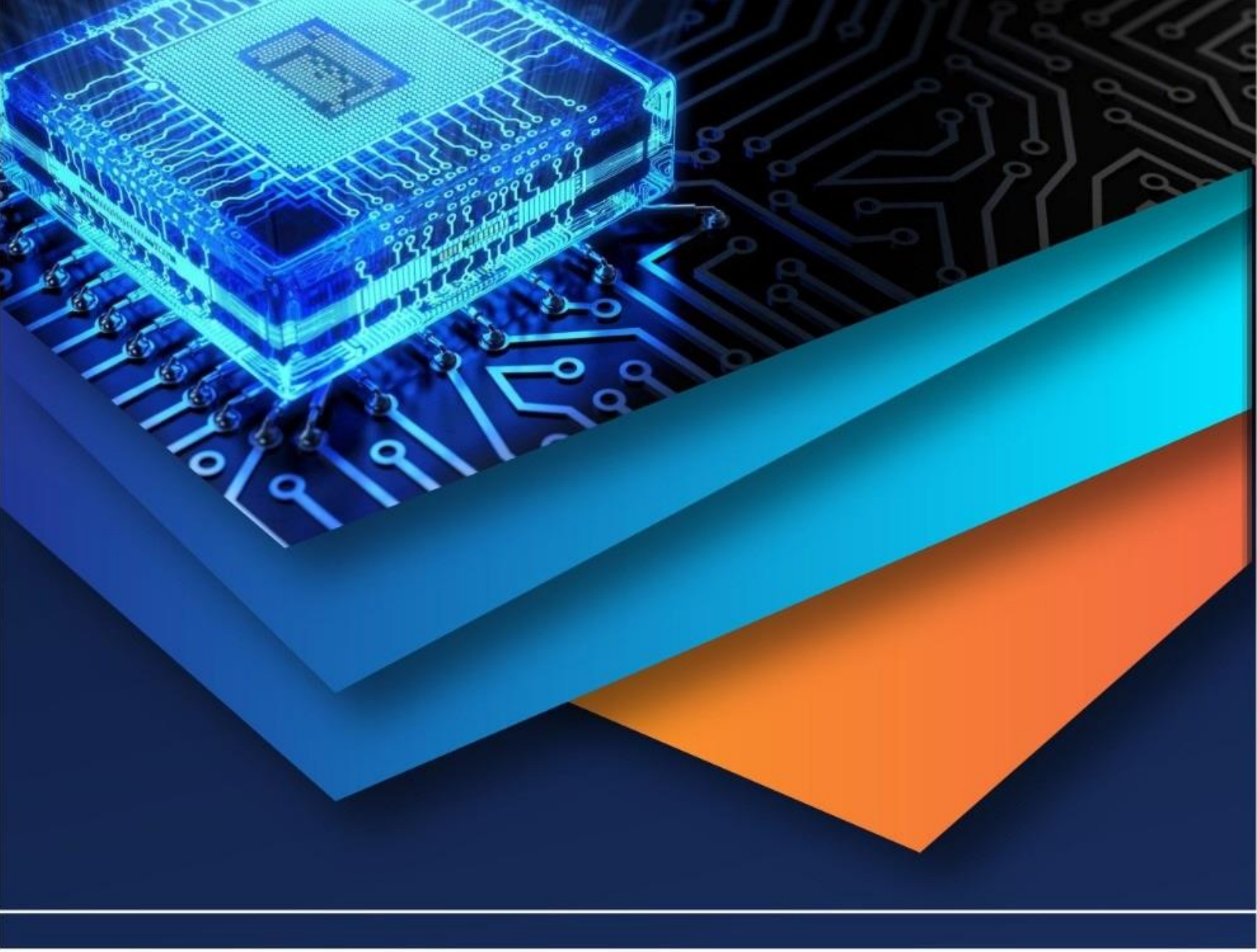
The study can be extended in the following ways:

- Conduct awareness workshops in schools, colleges, and local communities.
- Develop cyber safety posters and educational material in regional languages.
- Compare awareness levels before and after training.
- Increase the number and diversity of survey participants.
- Develop a simple website or mobile application containing cyber safety guidelines and quizzes.
- Conduct follow-up surveys to examine whether participants retain and apply the information.

REFERENCES

[1] Indian Computer Emergency Response Team (CERT-In), CERT-In's Digital Safety Compass Handbook. Available at: https://www.cert-in.org.in/PDF/CSH_Booklet25.pdf
[2] Reserve Bank of India (RBI), Digital Banking Cyber Security. Available at: https://rbikehtahai.rbi.org.in/digital-banking-cyber-security.html
[3] National Payments Corporation of India (NPCI), Fraud Awareness. Available at: https://www.npci.org.in/fraud-awareness
[4] Indian Computer Emergency Response Team (CERT-In), Advisory on Preventing Online Scams, October 24, 2024. Available at: https://www.cert-in.org.in/s2cMainServlet?VLCODE=CIAD-2024-0050&pageid=PUBVLNOTES02

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)