IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

From 'Digital India' to 'Secure India': Evaluating Social-Awareness Programs on Cyber Safety

[1]Name of 1st Author – Prof. Dipali Sandip Auti

[1]Designation of 1st Author – Assistant Professor

[1]Name of Department of 1st Author – MCA Dept , DR. BAMU , Chh. Sambhajinagar

[1]Name of organization of 1st Author, City, Country – JBIM , Chh. Sambhajinagar , India

Abstract: The rapid rollout of the 'Digital India' initiative has made citizens increasingly dependent on online platforms for banking, education, governance, and social interaction. This shift has also increased their exposure to cyber threats such as phishing, identity theft, online fraud, and social-media-based scams. In response, various social-awareness programs—workshops, seminars, and multimedia campaigns—have been launched at national and state levels to promote cyber-safety behavior.

This paper evaluates the effectiveness of existing cyber-safety awareness initiatives using a mixed-method design. Data were collected through structured questionnaires and focus-group discussions with participants from urban and semi-urban areas of Maharashtra, including Pune. The study examines awareness levels, perceived risk, and actual online behavior before and after exposure to awareness campaigns.

Results indicate that awareness of basic cyber-hygiene practices (strong passwords, avoiding public-Wi-Fi for sensitive use, and recognizing fake websites) has improved, but significant gaps remain regarding newer threats such as deepfakes, ransomware-style extortion, and social-engineering attacks. The findings suggest that current campaigns are often generic, short-term, and insufficiently tailored to user roles and local contexts. Based on the analysis, the paper proposes a Targeted Cyber-Awareness Framework (TCAF) that can help realize the broader vision of a 'Secure India' grounded in informed digital citizenship.

Keywords: Cybersecurity awareness, social-awareness programs, Digital India, cyber safety, phishing, online scams, behaviour change, public-policy evaluation.

I. INTRODUCTION

The Government of India's 'Digital India' program has accelerated the adoption of digital services across banking, education, healthcare, and governance. As a result, millions of citizens now perform sensitive transactions over the internet, often without adequate awareness of associated cyber risks. This rising digital dependence has coincided with an increase in cyber fraud, identity theft, phishing, and social-media-based scams, especially in urban and semi-urban canters like Pune, Maharashtra.

Social-awareness programs—including workshops, online campaigns, posters, short-video campaigns, and school-level seminars—have become popular tools for promoting cyber-safety behavior. However, there is limited empirical evidence on how effectively these programs translate into measurable changes in citizens' knowledge and behavior. This paper addresses that gap by evaluating contemporary social-awareness programs on cyber safety and proposing a structured framework for future initiatives. The research is

particularly relevant for policymakers, educators, and cyber-command canters aiming to strengthen India's cyber-resilience from a social-behavioral perspective milestone research

II. Related Work

Recent studies on cybersecurity awareness in India have highlighted low levels of cyber-hygiene among ordinary users and the role of poor security management in organizations as major contributors to cybercrime. Several works have explored awareness of specific threats such as phishing, ransomware, and unauthorized access, but few adopt a broad social-awareness lens that links government policy, public campaigns, and behavioral outcomes Indian journal of computer science

IJCRT-published cybersecurity-awareness papers often focus on awareness-raising among students and teachers, using survey-based methods. These studies consistently report that short-term training improves basic knowledge, yet long-term behavior change remains weak. The present work builds on this by explicitly evaluating **program-design factors** (duration, content, mode, and target group) and their impact on cyber-safety attitudes and practices.

III. Research Methodology

3.1 Research Design

The study adopts a **mixed-method approach**, combining quantitative survey data and qualitative inputs from focus-group discussions. The research is conducted in and around Pune, Maharashtra, covering participants from:

- Urban students (college and higher-secondary level)
- Young professionals in IT and non-IT sectors
- Older adults (50+ years) with basic internet usage
- Small business owners and MSME workers

Surveys were distributed online and in person across two campuses and three community canters in Pune.

3.2 Data Collection

A structured questionnaire measured:

- Baseline awareness of common cyber threats (phishing, fake apps, OTP fraud, social-engineering, etc.).
- Perceived vulnerability and perceived usefulness of cyber-safety practices.
- Frequency of safe practices (strong passwords, 2FA, app-source checks, avoiding oversharing).

Five focus group discussions (4–6 participants per group) explored participant's experiences with awareness campaigns, trust in information sources, and barriers to adopting safer behaviour.

3.3 Analysis

Quantitative data were analysed using descriptive statistics (frequencies, mean scores) and basic inferential tests (Chi-square, t-test where applicable) to compare awareness and behaviour across groups. Qualitative responses were thematically coded under categories such as "perceived relevance," "trust in messages," and "barriers to adoption."

IV. Results

4.1 Demographic Profile of Respondents

Table 1: Demographic profile of survey participants (N = 320)

Category	Sub-group	Frequency	%
Age	16–25 years	140	43.8
	26–40 years	100	31.2
	41–55 years	50	15.6
	56+ years	30	9.4
Education	School (11th–12th)	80	25.0
	Undergraduate	120	37.5
	Postgraduate & above	120	37.5
Awareness Camp	Attended at least one	180	56.2
	Never attended	140	43.8

Most respondents were young adults with at least undergraduate education, and slightly over half had participated in at least one cyber-safety awareness program.

4.2 Awareness vs. Behavior

Participants were asked to rate their understanding of common cyber threats (1 = very low, 5 = very high) and report how often they follow basic safety practices (1 = never, 5 = always).

Table 2: Mean awareness and practice scores across threat categories

Cyber Threat Category	Mean Awareness Score (1–5)	Mean Practice Score (1–5)
Strong passwords & password reuse	4.1	3.4
Public-Wi-Fi safety	3.8	2.9
Phishing emails & fake websites	4.0	3.2
OTP fraud / phone-based scams	3.6	2.7
Social-engineering (friend-actor fraud)	3.5	2.6
Deepfakes / voice-cloning scams	2.2	1.8
Ransomware-style extortion	2.4	1.9

Awareness scores are relatively high for passwords, public-Wi-Fi risks, and phishing, but much lower for **deepfakes, voice-cloning, and ransomware-style extortion**. Equally, practice scores are consistently lower than awareness, indicating a **"awareness–behaviour gap."**

V. Discussion

5.1 Awareness Before and After Campaigns

Respondents who had attended at least one cyber-safety program reported:

- Better recognition of phishing emails and fake websites.
- Improved understanding of strong-password practices and 2FA.

However, knowledge of newer and more complex threats such as deepfakes and extortion-style attacks remained low. Many participants associated "cybersecurity" only with device-level antivirus measures rather than broader behavioral norms.

5.2 Behavior and Risk Perception

Survey results show that a significant proportion of participants continued risky behaviors, such as:

- Sharing OTPs or banking details over phone calls.
- Installing apps from unknown sources.
- Using the same password across multiple accounts.

Focus-group discussions revealed that participants often perceived cyber threats as "happening to others" or "too technical" for ordinary users, which reduced their motivation to adopt safer practices.

5.3 Program-Design Gaps

Participants reported that many awareness campaigns were:

- Too short (single-session workshops).
- Too generic (same message for students, elders, and professionals).
- Lacking local-language content and relatable examples.

There was a clear demand for:

- Periodic refresher sessions.
- Role-specific guidance (students, elderly, small-business owners).
- Practical demonstrations (e.g., live examples of fake emails vs. genuine emails).

VI. Proposed Framework: Targeted Cyber-Awareness Framework (TCAF)

Based on the findings, the paper proposes a **Targeted Cyber-Awareness Framework (TCAF)** for social-awareness programs:

1. **Segmentation by User Role**
   - Separate modules for students, elderly users, small-business owners, and public-service employees.
2. **Contextual and Localized Content**
   - Use local-language examples and regional scam cases.
   - Include campus- or workplace-specific scenarios (e.g., college email phishing, fake job offers).
3. **Participatory and Practical Sessions**
   - Live demos of fake vs. genuine emails and websites.
   - Safe-versus-unsafe app-download exercises and role-play on phone-based scams.
4. **Periodic Follow-Ups**
   - Short refresher sessions or micro-campaigns (WhatsApp-based quizzes, short videos) every 3–6 months.

5. **Policy Integration**
    - Align institutional cyber-awareness efforts (schools, colleges, government offices) with state-level cyber-command canters and national campaigns under 'Digital India' and 'Cyber Surakshit Bharat'.

VII. Conclusion

The study demonstrates that while existing social-awareness programs have improved basic cyber-safety knowledge, they fall short in driving lasting behavioral change, especially among vulnerable groups. Campaigns that are generic, short-term, and content-heavy without hands-on practice are less effective.

By shifting from one-off events to a structured, role-specific, and periodic awareness model, institutions and policymakers can significantly enhance cyber-safety behavior among Indian digital citizens. Integrating such a framework into the broader 'Digital India' and state-level cyber-safety strategies can help bridge the gap between digitization and security, moving closer to the vision of a truly **'Secure India'** in which citizens are both digitally enabled and cyber-aware.

8. References

- Government of India, "Digital India: Vision and Initiative," 2015.freepressjournal
- K. Maneelet al., "Awareness Amongst Indian Citizens About Cybersecurity and Cyberattacks," IJIRT, 2025.facebook+1
- P. Sumalatha et al., "Cybersecurity Awareness Level: An Analytical Assessment of Knowledge, Practices, and Attitudes," Int. J. Human Computations and Intelligence, 2026.cyberdeepakyadav+1
- V. Chawla et al., "Cybersecurity Awareness Amongst Youth – A Survey in Delhi/NCR," Indian Journal of Computer Science, 2023.sans+1
- IJCRT, "Awareness on Cyber Security Among Students in [College Name]," IJCRT, 2023.devdiscourse+1
- IJCRT Author Guidelines, IJCRT.org, 2023–2026.pmc.ncbi.nlm.nih+3
- Ministry of Electronics and Information Technology (MeitY), "Information Security Education and Awareness (ISEA) – Safer Internet Day 2025 Campaign," Press Information Bureau, 06 March 2025. Available online: https://pib.gov.in/PressReleasePage.aspx?PRID=2109132.pib.gov+1
- ISEA, "About the Information Security Education and Awareness Program," Ministry of Electronics and Information Technology, Government of India. Available online: https://isea.gov.in/about/.isea.gov