CYBERSECURITY

Cyber Security Awareness Campaign

Daksh Patel, Trisha Dey, Dr. Bhojraj Y. Shewale

[1]Amity Business School, Amity University Mumbai, Maharashtra, India
[2]Guide, Amity Business School, Amity University Mumbai, Maharashtra, India

Published November 2026

Abstract

This study looks at baseline cyber safety awareness and digital threat resilience in a local community sample of 30 respondents in Panvel (Rural), Navi Mumbai. A quantitative, descriptive research design was used with a structured 12-point primary survey. The survey looked at a range of threat vectors including phishing, smishing, vishing, UPI, job scams, MFA, and emergency reporting. The findings show a high level of primary awareness of a number of the protocols, with 96.7% correctly stating that a UPI PIN is not required to receive funds, 83.3% always using MFA, and 73.3% being aware of the 1930 National Cyber Crime Helpline. There is, however, a significant level of exposure to threat: 86.7% have been directly targeted by phishing/smishing, 50% have been the victim of a part-time job scam, and a high level of self-reported confidence (60% very confident) is indicative of a degree of behavioural complacency. The study concludes that technical security infrastructure must be combined with scenario-based behavioural interventions to close the gap between knowledge and actual threat mitigation.

1 Introduction

The pace of digital transformation in India has been absolutely staggering and has completely changed the way users interact with financial services, e-commerce, and social media. With the availability of affordable smartphones and high-speed internet for all, the number of first-time users on digital platforms has exploded. That explosion has, of course, massively increased the attack surface for cybercriminals. India's digital payments infrastructure is the prime example of this, with UPI alone processing billions of transactions every month. The technology underneath is sound, but the attack surface is being exploited by criminals who are using social engineering in all its forms (vishing, smishing, threats of disconnection of electricity, fake job offers, etc). Financial fraud is a source of real socio-economic distress, so cybersecurity is no longer just an enterprise issue; it's a life skill. This study looks at the baseline level of cyber safety awareness across various demographic groups in order to identify the gaps and inform the work that needs to be done at the grassroots level.

2 Problem statement

Despite the very high levels of smartphone uptake and the fact that people use apps on a daily basis, there's a huge gap between operational digital literacy (i.e., knowing how to use an app) and security literacy (i.e., knowing how to protect yourself). The threat actors will use human cognitive biases (fear, urgency, greed, deference to authority, etc.) to get around the technical controls that an enterprise will have in place. The sheer volume of people that are exposed to automated phishing and to social engineering syndicates means that the community as a whole is very much at risk of financial loss and identity theft. This study looks at the fundamental issue of identifying the specific

behavioural and awareness gaps that exist in the local community in order to be able to effectively counter the threat of social engineering.

3 Objectives of the study

1. To assess the extent to which people perceive their confidence in detecting cybersecurity threats against the behavioral implementation of proper cybersecurity measures.
2. To assess the extent to which communities have been exposed to various forms of cyber attacks that include phishing, smishing, vishing, and online job fraud.
3. To assess the extent of public knowledge about fundamental cybersecurity techniques in terms of digital payment system security, namely UPI transactions.
4. To assess the adoption rates of key security hygiene practices, including multi-factor authentication and proper password handling.
5. To assess public knowledge about the emergency response structures, including the National Cyber Crime Helpline (1930) and the 'Golden Hour'.

4 Research questions and hypotheses

4.1 Research questions

RQ1: How successful have existing public awareness programs been in informing users about the UPI system and emergency reporting for cybercrimes?

RQ2: How exposed are people in the community to social engineering attacks such as phishing, smishing, and employment scams?

RQ3: Can high confidence in security protection be linked to full protection against online threats, or is it an indication of potential overconfidence bias?

4.2 Research hypotheses

H0 (Null Hypothesis): Theoretical knowledge regarding cyber safety protocols helps users avoid being victims of social engineering scams.

H1 (Alternative Hypothesis): There is a large discrepancy between theory and practice with regard to cyber security when people are placed under high emotional pressure.

5 Literature review

- **RBI (2025):** Focuses on protecting consumers in the realm of digital payment systems and mandatory security practices in digital payment systems, underlining the importance of steps involved in user authentication.
- **I4C, Ministry of Home Affairs (2026):** Talks about the increasing trend of cyber fraud syndicates in India and mentions that social engineering and financial impersonation make up the majority of complaints raised by citizens.
- **CISA (2024):** Highlights that Multi-Factor Authentication (MFA) and phishing-resistant credentials significantly decrease the chances of account takeover by more than 90%, making these two measures basic security standards for people.

- **NPCI (2025):** Discusses operational guidelines of UPI, mentioning that a PIN is nothing but a mechanism of debiting and is never required for receiving money.
- **Kaspersky Lab (2026):** Studies the development of a combination of phishing, smishing, and vishing threats in emerging digital economies, seeing the transition from unencrypted messengers to encrypted ones and task-based financial scams.
- **WEF (2025):** Discusses human vulnerability as the major threat vector in international cyber incidents and suggests continuous human-based educational intervention over policy-based ones.

6 Research methodology

- **Research Design:** Descriptive quantitative research design based on a pragmatic research paradigm for the objective analysis of user awareness and behavior.
- **Population:** Community individuals residing within the geographical boundaries of Panvel (rural), Navi Mumbai, representing all different age groups and occupations.
- **Sample Size:** 30 primary participants.
- **Sampling Procedure:** Non-probability sampling using convenient sampling network to gather different types of participants including students, IT professionals, salaried employees, among others.
- **Sources of Data:** Primary data will be gathered using structured questionnaires in the field and online, while secondary data will be obtained from RBI, NPCI, I4C, and various international cybersecurity reports.
- **Method of Data Collection:** A structured questionnaire consisting of 12 items that test self-efficacy, past exposure to threats, protocol verification, and incident handling knowledge.

7 Data analysis and interpretation

7.1 Demographics – age group distribution

Data: 18–35 years: 25 respondents (83.3%); 36–60 years: 4 respondents (13.3%); Under 18 years: 1 respondent (3.3%).

Table 1. Age group distribution of respondents (N = 30).

Age Group	Number of Respondents	Percentage (%)
18–35	25	83.3%
36–60	4	13.3%
Under 18	1	3.3%

Interpretation: The sample consists largely of digital natives aged between 18 and 35 years, who regularly conduct transactions digitally. Despite being computer savvy, the fact that they constantly use computers exposes them to fraudsters.

7.2 Confidence in identifying threats

Data: Very Confident: 18 respondents (60.0%); Moderately Confident: 12 respondents (40.0%); Not Confident: 0 respondents (0.0%).

Table 2. Confidence in identifying threats (N = 30).

Response Category	Number of Respondents	Percentage (%)
Very Confident	18	60.0%
Moderately Confident	12	40.0%

Interpretation: The majority of the participants are comfortable using the internet. But being too self-confident can result in the Dunning-Kruger effect, making individuals skip the process of verification when they come across sophisticated scams.

7.3 Exposure to phishing / smishing

Data: Yes: 26 respondents (86.7%); Maybe: 2 respondents (6.7%); No: 2 respondents (6.7%).

Table 3. Exposure to phishing and smishing (N = 30).

Response Category	Number of Respondents	Percentage (%)
Yes	26	86.7%
Maybe	2	6.7%
No	2	6.7%

Interpretation: More than 86% of survey participants were exposed to deceptive text or email messages. This means that automated phishing is hard to prevent, so emphasis should be placed on the proper management of these messages.

7.4 Understanding of UPI protocol (PIN for receiving money)

Data: False (Correct): 29 respondents (96.7%); True (Incorrect): 1 respondent (3.3%).

Table 4. Understanding of the UPI protocol (PIN for receiving money) (N = 30).

Statement: 'UPI PIN required to receive money'	Number of Respondents	Percentage (%)
False (Correct)	29	96.7%
True (Incorrect)	1	3.3%

Interpretation: Awareness campaigns conducted by NPCI and financial institutions have successfully educated users that the use of UPI PIN is necessary only for money transfer. But still, the remaining 3.3% of confusion provides scope for fraud techniques such as 'Reverse Collect Request'.

7.5 Exposure to job scams

Data: No: 15 respondents (50.0%); Yes: 10 respondents (33.3%); Maybe: 5 respondents (16.7%).

Table 5. Exposure to job scams (N = 30).

Response Category	Number of Respondents	Percentage (%)
No	15	50.0%
Yes	10	33.3%

Response Category	Number of Respondents	Percentage (%)
Maybe	5	16.7%

Interpretation: "Half the respondents (combining Yes and Maybe) have had fraudulent offers for part-time jobs that required payment." The main targets of such task scams are students and young people seeking employment opportunities.

7.6 Adoption of multi-factor authentication (MFA)

Data: Yes, always: 25 respondents (83.3%); Sometimes: 5 respondents (16.7%); No: 0 respondents (0.0%).

Table 6. Adoption of multi-factor authentication (N = 30).

Response Category	Number of Respondents	Percentage (%)
Yes, always	25	83.3%
Sometimes	5	16.7%

Interpretation: There is an existing presence of strong technical defense practices among students, where 83.3% always use MFA. There is a vulnerability window created by 16.7% of those who do not always use MFA.

7.7 Awareness of the 1930 Cyber Crime Helpline

Data: Yes (Aware & know how to report): 22 respondents (73.3%); No (Not aware): 8 respondents (26.7%).

Table 7. Awareness of the 1930 Cyber Crime Helpline (N = 30).

Response Category	Number of Respondents	Percentage (%)
Yes, know how to report immediately	22	73.3%
No, not aware of this helpline	8	26.7%

Interpretation: About three out of every four individuals are aware of how to report financial fraud in the golden hour. On the other hand, over 26% of people do not know about it.

8 Findings

- **Universal Threat Exposure:** More than 86% of participants have been targeted through phishing/smishing attacks, while 50% have experienced an online job scam.
- **Sound Understanding of Rules:** The knowledge regarding basic rules of security is sound, with 96.7% of the sample identifying that UPI PINs are meant only for withdrawal.
- **Overconfidence Issue:** 60% of the participants exhibit high confidence in scam detection ability, making them vulnerable to pressure tactics employed by scammers.
- **Limited Awareness of Recourse:** 26.7% of the sample does not know about the 1930 National Cyber Crime Helpline and will end up losing money outside the 'Golden Hour'.

- **Inconsistency in Security Habits:** Though 83.3% of the participants always follow MFA, 16.7% do so occasionally, using SMS OTP instead of dedicated authenticators.

9 Suggestions and recommendations

- **Formalization of 'Tactical Pause':** Educate users about pausing for 5 minutes before responding to any critical messages to break the psychological trap being utilized by social engineering.
- **Secondary Channel Verification:** Users need to verify any emergency money requests and financial alerts using a secondary channel, like calling the sender personally.
- **Publicity for Helpline 1930:** Promote the number 1930 in banks, banking apps, ATMs, and even SMS services to be sure about the action within the first Golden Hour.
- **Incorporating Cybersecurity in School Curricula:** Integrate real-life situations related to cybersecurity modules into high school and college curricula to recognize fraudulent job postings and social media frauds.
- **Switching to Authenticator Applications:** It is recommended to switch from SMS-based OTP to TOTP applications (Google Authenticator).

10 Conclusion

The Cyber Safety Awareness Campaign research highlights the fact that despite good theoretical understanding of security protocols, such as those for the UPI PIN and MFA, the community is always at risk due to exposure to social engineering tricks. Knowledge gaps about reporting emergencies (1930 helpline) and possibly over-reliance on the ability to detect threats make users prone to elaborate scams. Community cyber safety calls for more than protocol-based learning; it necessitates behavior-oriented scenario training.

11 Limitations

- **Sample Size:** The current study is conducted with a sample size of 30 respondents, thus limiting generalized statistical application to national-level populations.
- **Geographical Boundaries:** The fieldwork conducted was confined mainly to Panvel (Rural), Navi Mumbai, and nearby areas.
- **Social Desirability Bias:** Survey data based self-reporting is bound to make the respondent exaggerate good practices of security while understating errors made.
- **Behavioral versus Theoretical Evaluation:** The survey reflects declared actions rather than behavioral actions under simulated cyber attacks.

References

[1] Cybersecurity and Infrastructure Security Agency (CISA). (2024). Best practices for multi-factor authentication and phishing-resistant credentials.

[2] Kaspersky Lab. (2026). Phishing, smishing, and vishing: Evolving threats in the digital economy of the future.

[3] Ministry of Home Affairs, Government of India. (2026). Annual report on the performance and trends of the Indian Cyber Crime Coordination Centre (I4C). *New Delhi*.

[4] National Payments Corporation of India (NPCI). (2025). Operating rules and security guidelines for the Unified Payments Interface (UPI). *Mumbai*.

[5] Reserve Bank of India (RBI). (2025). Guidelines for digital payment systems security and consumer protection framework. *Reserve Bank of India Bulletin*, Mumbai.

[6] World Economic Forum (WEF). (2025). Global cyber security outlook: Living with human vulnerability and technology challenges.