IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151075

Cyber Crime Awareness, And Fraud Prevention

Nilam Yashwant Kokanee[1], Asmita Bhaskar Kudnar[2], Prof. Sanchita Panmand[3]

Master of Computer Application, Samarth College of Engineering & Management[1,2]

Guide, Master of Computer Application, Samarth College of Engineering & Management[3]

Abstract: The growing use of smartphones, social media, instant messaging, digital banking, online shopping and electronic services has increased the convenience of everyday life. At the same time, members of the public may be exposed to cybercrime such as phishing, fake forwarded messages, online payment fraud, fraudulent job offers, impersonation, identity theft, fake customer-care numbers and malicious applications. This research project proposes to study cybercrime awareness and prevention practices among the general public, including students, working people, business owners and senior citizens. A descriptive survey using a structured questionnaire is proposed. Responses will be summarised using counts, percentages, tables and charts after genuine data are collected. A small Python-based awareness tool is also proposed to flag warning signs in a message and provide safety guidance. The tool will be educational only and cannot conclusively determine whether a message is fraudulent. No survey findings are claimed in this draft because actual responses have not yet been collected.

Keywords: Cyber crime, online fraud, phishing, fake messages, digital safety, cyber awareness, fraud prevention.

1. INTRODUCTION

Cybercrime refers to unlawful activity in which computers, mobile devices, digital accounts or networks are used as a target or a tool. Digital services are now used for communication, banking, shopping, employment, education and government services. Criminals exploit trust, urgency, fear, curiosity and limited awareness to persuade people to reveal information, transfer money or install harmful software.

Fraudulent messages may appear to come from a bank, delivery company, government department, employer, friend or family member. A message may claim that an account will be blocked, a parcel is delayed, a prize has been won or a job is available. The recipient may be directed to a fake website, asked for an OTP or PIN, or pressured to make a payment. Awareness, careful verification and timely reporting can reduce the risk of harm.

This study is designed for the general public rather than one age or education group. It considers both the human side of scams and the practical steps that people can take to protect their accounts, money and personal information.

2. PROBLEM STATEMENT

Cyber scams continue to exploit digital communication and online transactions. People may have difficulty distinguishing genuine messages from fraudulent ones, may trust a caller or forwarded message without verification, or may not know what to do after a suspected fraud. Confusion about official reporting channels can also delay action. The study therefore aims to understand public awareness, common exposure to scam attempts, protective habits and knowledge of reporting options.

3.AIM AND OBJECTIVES

Aim

To study cybercrime awareness among the general public and identify practical ways to recognise, prevent and report online scams.

Objectives

- To describe common cybercrime and online-fraud types encountered by the public.
- To examine how people recognise suspicious messages, links, calls and payment requests.
- To assess awareness of OTP, UPI PIN, passwords, KYC-related scams and fake job offers.
- To understand common reasons that make people vulnerable to scams, including urgency, impersonation and lack of verification.
- To assess awareness of official cybercrime reporting channels in India.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.151075

- To recommend practical prevention steps for different groups of people.
- To propose a simple Python awareness tool that highlights warning signs and provides safe next steps.

4. RESEARCH QUESTIONS

- What kinds of cyber scams do members of the public report encountering?
- What warning signs do people check before opening a link or acting on a message?
- How well do respondents understand the risks of sharing OTPs,PINs, passwords or remote-access permissions?
- Do respondents know where to report suspected cybercrime and financial fraud?
- What safety habits are used most often, and what awareness gaps remain?

5. SCOPE OF THE STUDY

The study covers members of the public across different age groups and occupations. It includes WhatsApp and SMS forwards, phishing links, fake government benefit messages, bank/KYC impersonation, UPI and QR-code fraud, fake payment screenshots, online shopping scams, fraudulent job and work-from-home offers, lottery/prize scams, investment scams, impersonation and malicious app downloads. The study focuses on awareness, prevention and reporting, not on investigating individual criminal cases or guaranteeing recovery of money.

Included area	Examples
Messaging scams	WhatsApp forwards, SMS links, fake alerts and impersonation
Financial fraud	UPI requests, QR-code tricks, fake payment proof and bank impersonation
Employment scams	Fake job offers, registration fees and work-from-home promises
Personal information	OTP theft, password theft, identity misuse and fake KYC
Public protection	Recognising warning signs, preserving evidence and reporting incidents

6. REVIEW OF LITERATURE

Cybersecurity awareness guidance from government and specialist organisations commonly emphasises checking links and senders, using unique passwords, enabling multi-factor authentication, installing updates and avoiding the disclosure of confidential credentials. Public cybercrime reporting services provide channels for reporting incidents, while incident-response organisations publish educational material on online safety.

A final submission should add and verify relevant peer-reviewed research articles from an academic library or Google Scholar. Each article should be checked for author names, title, publication year, journal and DOI before it is cited. The present draft lists official awareness resources in the references and does not invent research findings or bibliographic details.

7. COMMON TYPES OF CYBERCRIME

Type	How it may work	Warning sign / safer response
Phishing	A fake email, SMS or webpage imitates a trusted organisation.	Check the full web address independently; do not use unexpected links.
WhatsApp / forwarded-message scam	A message promises a prize, benefit, urgent refund or shocking news.	Verify with the named organisation through an official channel before forwarding or paying.
Bank / KYC impersonation	A caller or message threatens account suspension and requests credentials.	Never disclose OTP, PIN or password; contact the bank using its official app/card/website.
UPI / QR-code fraud	A scammer asks the victim to	Receiving money normally does

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151075

	approve a collect request or scan a QR code to receive money.	not require entering a UPI PIN; read the screen carefully.
Fake job offer	An alleged employer requests registration, training, security or interview fees.	Verify the company and vacancy independently; be wary of guaranteed high income.
Fake payment screenshot	A buyer shows an edited receipt and pressures the seller to hand over goods.	Check the actual bank/UPI account balance or transaction history.
Investment / lottery scam	Promises of guaranteed returns or winnings require an upfront payment.	Treat guaranteed profits and advance-fee demands as red flags.
Malicious app / remote access	A user is persuaded to install an unknown APK or remote-control app.	Install only trusted apps and never grant remote access to unknown callers.
Identity theft / account takeover	Personal information or stolen credentials are used to impersonate someone.	Limit public personal details, use unique passwords and enable MFA.

8. WHY CYBERCRIME HAPPENS

- Financial gain: criminals aim to steal money, banking credentials or valuable personal data.
- Social engineering: attackers manipulate emotions such as fear, urgency, trust or excitement.
- Impersonation: scammers pretend to be a bank, official, employer, delivery agent or relative.
- Low awareness: people may not know how to verify links,payment requests or caller identities.
- Easy sharing: unverified messages may spread quickly through group chats and social networks.
- Technical weaknesses: outdated software, reused passwords, insecure devices or compromised accounts can increase risk.
- Anonymity and scale: digital tools can let offenders contact many potential victims quickly.

9. HOW TO IDENTIFY A SUSPICIOUS MESSAGE

- Check the sender's number, email address and profile carefully; a display name alone proves nothing.
- Look for pressure such as 'act now', threats of account closure, secret offers or requests to keep the transaction private.
- Inspect links without opening them. Misspellings, strange domains, shortened URLs and unexpected attachments deserve caution.
- Do not trust a message solely because it has a logo, official-looking design, forwarded label or familiar profile picture.
- Never share OTPs, UPI PINs, passwords, card security codes or recovery codes with callers or message senders.
- Verify the claim independently through the organisation's official app, website or contact details you find yourself.
- Do not install unknown APK files or screen-sharing/remote-access apps at another person's request.
- Before paying, check the recipient, amount and transaction details on your own device.

10. GOVERNMENT SUPPORT AND REPORTING IN INDIA

India provides official channels for reporting cybercrime. The National Cyber Crime Reporting Portal accepts cybercrime complaints. The national helpline 1930 is used for reporting financial cyber fraud; prompt reporting is important, particularly where money has been transferred. A complaint is not a guarantee that funds will be recovered, and the relevant bank/payment provider and law-enforcement authorities may need to be contacted.

Situation	Suggested action

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151075

Money has just been transferred in a suspected cyber fraud	Call 1930 promptly; report through the official National Cyber Crime Reporting Portal and contact the bank/payment provider immediately.
Suspicious message or online account compromise	Save screenshots, sender details, URLs and timestamps; report through the platform and relevant official channel.
Threats, blackmail or impersonation	Preserve evidence, avoid further payments, secure affected accounts and report to the police/cybercrime authorities.
Need general cyber-safety information	Consult official government and CERT-In awareness resources.

Official resources:

- National Cyber Crime Reporting Portal: https://cybercrime.gov.in/
- CERT-In awareness resources: https://www.cert-in.org.in/AwarenessBooklets.jsp
- For financial cyber fraud, call 1930 promptly. Use official contact information and avoid numbers supplied by an unknown caller or message.

11. RESEARCH METHODOLOGY

Research design

A descriptive survey design is proposed to understand public awareness and self-reported safety practices.

Population and sampling

The target population is the general public, including students, employees, self-employed people, business owners, homemakers and senior citizens. A convenience sample may be used if access to a representative sample is not possible. The sampling method and respondent profile must be stated honestly in the final report.

Data collection

Primary data may be collected through a voluntary questionnaire in paper or online form. Do not collect bank details, passwords, OTPs or other unnecessary sensitive information. Participation should be voluntary and responses should be reported in aggregate.

Data analysis

After actual responses are collected, use counts and percentages to summarise answers. Tables and bar/pie charts may be created from genuine data. Do not fill the results section with invented numbers. State the number of respondents, collection dates and any missing responses.

Proposed research process

Step	Activity
1	Define research problem and objectives
2	Prepare questionnaire and obtain guide approval
3	Collect voluntary responses from members of the public
4	Check responses and remove duplicate/incomplete entries where appropriate
5	Calculate counts and percentages
6	Create tables/charts and interpret the actual findings
7	Write recommendations and final conclusion

12. QUESTIONNAIRE FOR THE GENERAL PUBLIC

Suggested questionnaire. Adapt it with the project guide before collecting responses. Do not request names, account numbers, OTPs or passwords.

Question area	Suggested response options

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151075

1. Age group	Under 18 / 18–25 / 26–40 / 41–60 / Above 60 / Prefer not to say
2. Occupation	Student / Employed / Self-employed or business / Homemaker / Retired / Other
3. Have you received a suspicious message, call or link?	Yes / No / Not sure
4. Which types have you encountered?	Fake job / Bank-KYC / UPI-payment / Lottery-prize / Shopping / Investment / Other / None
5. Do you check a link before opening it?	Always / Sometimes / Never
6. Do you know that an OTP or UPI PIN should not be shared with callers?	Yes / No / Not sure
7. Do you verify a job offer or government benefit independently?	Always / Sometimes / Never
8. Do you use different passwords for important accounts?	Always / Sometimes / Never
9. Is multi-factor authentication enabled on important accounts?	Yes / No / Not sure
10. Do you know the official reporting route for cybercrime in India?	Yes / No / Not sure
11. Do you know the financial cyber-fraud helpline 1930?	Yes / No / Not sure
12. What cyber-safety topic would help you most?	Fake messages / UPI fraud / Job scams / Account security / Reporting / Other

13. DATA ANALYSIS PLAN

This section must be completed after survey collection. The table below is a blank template; it does not represent actual findings.

Measure	Actual count	Percentage
Respondents who received suspicious messages	To be filled	To be calculated
Respondents who know not to share OTP/PIN	To be filled	To be calculated
Respondents who know helpline 1930	To be filled	To be calculated
Respondents who verify links before opening	To be filled	To be calculated
Respondents who know the reporting portal	To be filled	To be calculated

Percentage formula: (number of respondents selecting an answer ÷ total valid responses to that question) × 100.

14. PROPOSED PYTHON-BASED AWARENESS TOOL

The proposed prototype accepts a message entered by a user, checks for selected warning indicators such as urgency language, requests for OTP/PIN/password, suspicious links, prize claims or upfront fees, and displays general safety advice. It may also provide links to official reporting resources. This is a rule-based educational prototype, not a forensic system and not a definitive scam detector. A genuine message can contain warning words, and a sophisticated scam may avoid them; users must independently verify claims.

Input / feature	Expected output
Text of a suspicious message	Potential warning indicators found
Detected keywords or URL patterns	Explanation of why the indicator may be risky
Safety guidance	Do not click, do not share credentials, verify independently
Reporting information	Official portal and financial-fraud helpline 1930

15. RECOMMENDATIONS

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.151075

- Pause before acting on urgent messages, threats, prize claims or unexpected payment requests.
- Verify requests using a separate official channel rather than replying to the suspicious message.
- Never share OTPs, passwords, UPI PINs or card security codes.
- Do not scan QR codes or approve collect requests merely to receive money.
- Check the actual bank/payment transaction rather than trusting screenshots.
- Use unique passwords, a password manager where appropriate, and multi-factor authentication.
- Keep mobile operating systems and apps updated; install apps only from trusted sources.
- Limit public sharing of personal information and review privacy settings.
- Preserve screenshots, phone numbers, links, transaction IDs and timestamps when reporting a scam.
- If money is lost, contact the bank/payment provider immediately and call 1930 promptly; also use the official portal.
- Share verified safety information and avoid forwarding unverified claims.

16. LIMITATIONS OF THE STUDY

- A convenience sample may not represent the entire population.
- Self-reported answers may be affected by memory or reluctance to disclose an incident.
- A survey at one point in time cannot establish cause and effect.
- The sample size and available time may limit analysis across age and occupation groups.
- The proposed keyword-based tool cannot reliably detect every scam and may produce false positives or false negatives.
- Reporting an incident does not guarantee recovery of money or a particular legal outcome.

17. CONCLUSION

Cybercrime and online scams can affect people of any age, occupation or level of education. Fake forwarded messages, phishing links, bank and KYC impersonation, UPI fraud, fake job offers, fraudulent investments and malicious applications often rely on trust, urgency and inadequate verification. Practical habits—checking the sender and destination, refusing to share OTPs or PINs, independently verifying payment requests, securing accounts and preserving evidence—can reduce exposure to common risks. In India, people should use official reporting channels and, in cases of financial cyber fraud, call 1930 promptly and contact their bank or payment provider. The proposed survey can identify public awareness gaps only after genuine responses have been collected and analysed. The Python prototype is intended to educate users about warning signs, not to certify a message as safe or fraudulent. The final conclusion should be updated to reflect the actual survey results.

REFERENCES

[1]. Government of India. National Cyber Crime Reporting Portal. https://cybercrime.gov.in/
[2]. Indian Computer Emergency Response Team (CERT-In). Cyber security awareness resources. https://www.cert-in.org.in/AwarenessBooklets.jsp
[3]. Cybersecurity and Infrastructure Security Agency (CISA). Secure Our World. https://www.cisa.gov/secure-our-world
[4]. National Institute of Standards and Technology (NIST). Digital Identity Guidelines, Special Publication 800-63. https://pages.nist.gov/800-63-3/
[5]. Verizon. Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

 This work is licensed under a Creative Commons Attribution 4.0 International License