



Original Article

Financial Fraud through Social Engineering: Awareness

Mrs. Snehal H. Borkar

Marathwada Mitra Mandal's College of Commerce, Pune

Manuscript ID:

IJAAR-130617

ISSN: 2347-7075

Impact Factor – 8.141

Volume - 13

Issue - 6

July – August 2026

Pp. 127 - 134

Submitted: 02 August 2026

Revised: 14 August 2026

Accepted: 25 August 2026

Published: 31 August 2026

Corresponding Author:

Mrs. Snehal H. Borkar

Quick Response Code:



Website: <https://ijaar.co.in/>



DOI: 10.5281/zenodo.22206862

DOI Link:

<https://doi.org/10.5281/zenodo.22206862>



Creative Commons



Abstract:

Financial transactions became faster and more convenient now a day due to usage of digital banking and online payment services. But the usage of digital banking increased the risk of financial fraud through social engineering. Fraudsters take the advantage of emotions of people such as fear, urgency, and trust to get the personal or confidential information. The researcher has studied the level of awareness amongst digital banking users in Pune city regarding financial fraud through social engineering. The researcher has analysed that is there any relation between age, education, frequency digital banking usage and financial fraud awareness. For the study primary data collected through the questionnaire using snowball sampling technique. The total 31 digital banking users responded to the questionnaire from different age group. For hypothesis testing ANOVA test was applied by researcher with 5% level of significance. The study concludes that there is high awareness of financial fraud through social engineering amongst selected digital banking users.

Creative Commons (CC BY-NC-SA 4.0)

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits others to remix, adapt, and build upon the work non-commercially, provided that appropriate credit is given and that any new creations are licensed under identical terms.

How to cite this article:

Mrs. Snehal H. Borkar. (2026). Financial Fraud through Social Engineering: Awareness. International Journal of Advance and Applied Research, 13(6), 127 – 134. <https://doi.org/10.5281/zenodo.22206862>

Introduction:

The Pune city report shows that there was increase in the cyber enabled financial fraud in recent year. As per National Crime Report Bureau and Pune police report, the cybercrime cases increased from 238 in 2020 year to 1,505 in 2024 year. The case has been declined in the year 2025 upto 743 cases. In the year 2024, the financial loss was approximately Rs. 446 crores. Around 68.9% of

cybercrime cases were related to the financial fraud reported in the year 2023. (Source: National Crime Records Bureau. (2024).) Share market and investment related scams have been prominent amongst the different types of frauds. Fraudsters commonly use phishing links, fake investment or trading platforms, impersonation, UPI transactions, fraudulent calls and messages and OTP related methods to deceive people.



The attackers use psychological manipulation techniques to break security rules, sending money, giving private data on people is Social engineering. The attackers or scammers use human trust, curiosity, and fear, emotion to get what they want, instead of hacking or cyber-crime. There are different types of Social Engineering techniques of fraud:

a) Phishing:

The cyber-attack in which the usage of phone, email, SMS, social media, or other media of personal communication done to trap users into using fraudulent links, for gaining personal information like account numbers or passwords or downloading infected files is known as Phishing. There are different types of phishing like, bulk phishing, spear phishing, whaling, vishing, quishing, AI based impersonation etc.

b) Whaling:

It is a most targeted form of attack in which communication is designed to obtain confidential information from a user.

c) Baiting:

The fraud in which the scammers convince users to install malware on a system or to disclose personal information by offering false promises is known as Baiting.

d) Diversion Theft:

It involves misleading a person so that information, goods or communication are directed to an unintended recipient.

e) Business Email Compromise:

It is tactic of social engineering where an attack impersonates a trusted official within an organisation who is authorised to handle financial matters.

f) Smishing/SMS-Phishing:

It is also known as SMS phishing. The attackers use deceptive text messages to encourage users

to click fraudulent links or to take actions that may compromise their information or devices.

g) Quid pro quo:

In this attack, the attacker demands sensitive information from the victim in exchange for a desired service.

h) Pretexting:

It involves creating a believable situation or false identity to gain the confidence of the targeted individual and obtain sensitive information.

i) Honeytrap:

Through the online social media or dating websites the attackers target people who are into search of love. The attackers use fabricated online identities or relationships to gain a person's trust and subsequently obtain money or confidential information.

j) Tailgating/Piggybacking:

It is a physical social-engineering technique in which an unauthorised individual attempts to gain entry to a restricted location by taking advantage of an authorised person's access. The fraudster steals unattended devices or obtains confidential files once entered.

Review of Literature:

Hadnagy (2018) explained that social engineering involves the manipulation of human behaviour to obtain information or access that would otherwise remain protected. The study highlighted that attackers frequently exploit psychological factors such as trust, authority, fear and urgency. Therefore, technological security measures alone may not be sufficient unless users are also aware of manipulation techniques.

Krombholz et al. (2015) examined different dimensions of social engineering attacks and classified them according to their methods, communication channels and targets. The study



observed that social engineering attacks can take place through electronic communication as well as direct human interaction. It emphasized the importance of awareness and education as preventive measures against such attacks.

Objectives of Study:

1. To examine the relationship between age, educational qualification and financial frauds awareness among the digital banking users situated in Pune city.
2. To analyse is there any relation between financial fraud awareness and frequency of digital banking usage among the digital banking users situated in Pune city.
3. To study the level of awareness about financial fraud among digital banking users resides in Pune city.

Scope of Study:

1. The study focuses on the awareness regarding financial fraud through social engineering amongst digital banking users resides in Pune city.
2. The study is restricted to 31 digital banking users stays in Pune city.
3. The study focuses on the age, educational qualification and frequency of digital banking usage is related to the level of financial fraud awareness.

Limitations of Study:

1. The present study is limited to 31 digital banking users stays in Pune city.
2. The study is based on the primary data collected through a questionnaire.
3. The study does not focus on the actual financial losses suffered by victims; the focus is restricted towards only awareness of financial fraud.

4. The present study is restricted to the Pune city digital banking user respondents.

Hypothesis of Study:

H₀: There is no significant relation between age, education of the digital banking users and financial fraud awareness.

H₁: There is significant relation between age, education of the digital banking users and financial fraud awareness.

H₀: There is no significant relation between frequency of digital banking usage and financial fraud awareness.

H₁: There is significant relation between frequency of digital banking usage and financial fraud awareness.

Research Methodology:

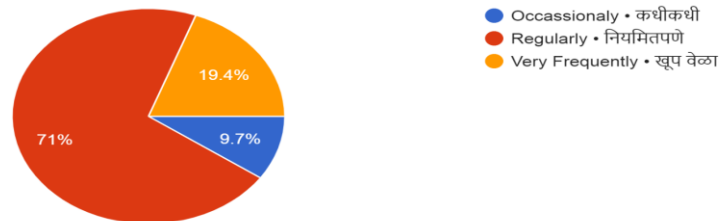
The researcher has collected data the primary data from 31 respondents located at Pune city using snow ball sampling method. The researcher could obtain 11 responses from age group between 20 to 39 years, 10 responses from age group between 40 to 59 years, 10 responses from 60 to 80 years. This ensures that the sample represents the all age groups who use digital banking methods for income and expenditure. The secondary data collected from the research papers, articles, published thesis, journals etc.



Data Analysis and Interpretation:

Frequency of digital banking payment services: आपण डिजिटल बैंकिंग / पेमेंट सेवांचा किती वेळा वापर करता?

31 responses



I know that fraudsters may pretend to be Bank officers, police officers, relatives or other trusted persons to ask for money or bank details. मला माहीत...सल्याचे भासवून पैसे किंवा बँकेची माहिती मागू शकतात.

31 responses



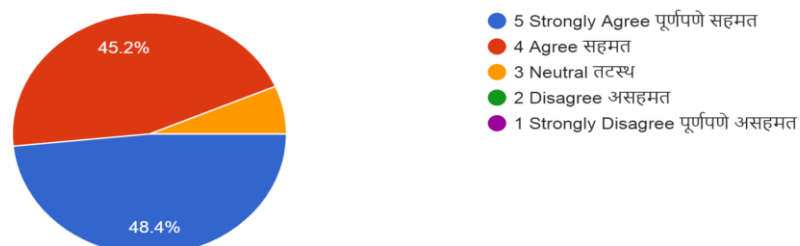
I know that I should never share my OTP, ATM PIN, CVV or banking password with anyone. मला माहीत आहे की OTP, ATM PIN, CVV किंवा बँकिंग पासवर्ड कोणालाही सांगू नये.

31 responses



I can identify suspicious phone calls, messages, links, QR codes or online payment requests. मला संशयास्पद फोन कॉल, मेसेज, लिंक, QR कोड किंवा ऑनलाइन पैसे भरण्याची विनंती ओळखता येते.

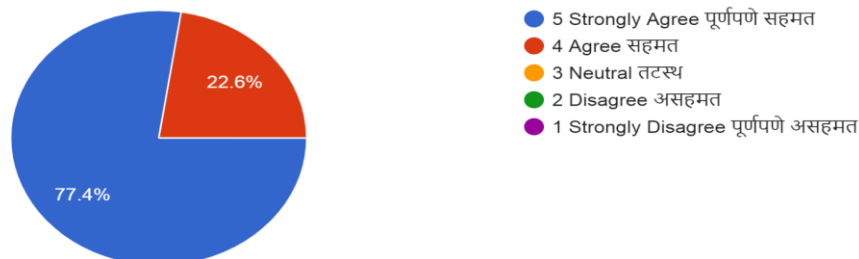
31 responses





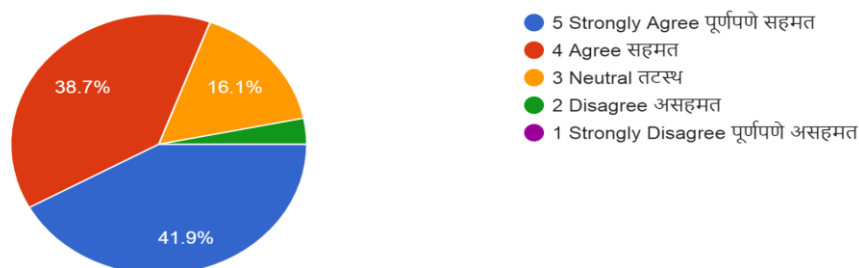
I know that fraudsters may use fear, urgency, prizes, rewards or attractive offers to make people send money or share bank details. मला माहीत आहे की ... पाठवण्यास किंवा बँकेची माहिती देण्यास सांगू शकतात.

31 responses



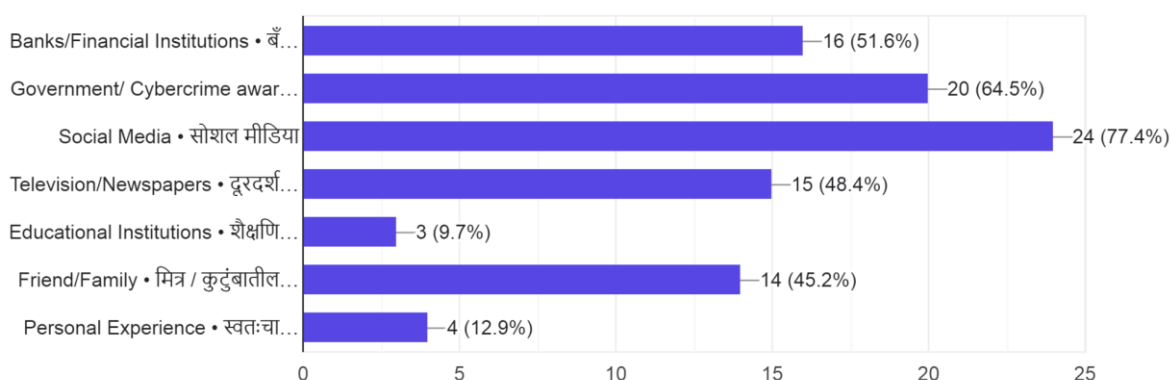
I know where and how to report a suspected online financial fraud or an unauthorised bank transaction. ऑनलाइन आर्थिक फसवणूक झाल्याचा संशय ... याची तक्रार कुठे आणि कशी करावी, हे मला माहीत आहे.

31 responses



From which sources have you received information about financial fraud and online banking safety? आर्थिक फसवणूक आणि सुरक्षित ऑनलाइन बँकिंगबा...ती मिळाली आहे? (एकापेक्षा जास्त पर्याय निवडू शकता)

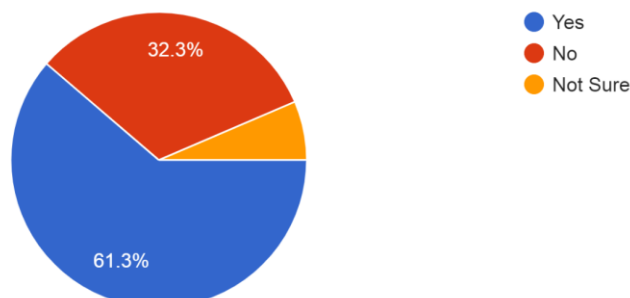
31 responses





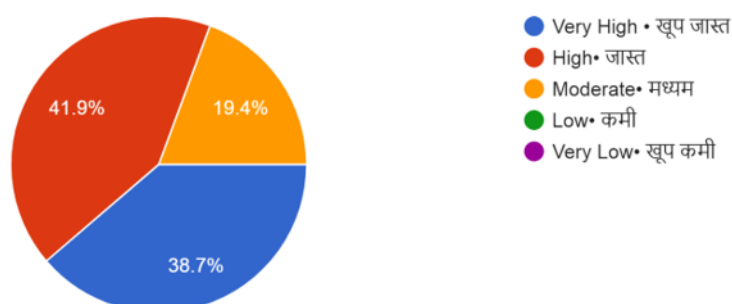
Have you ever received a suspicious call, SMS, email, social-media message or payment request that you believed could be fraudulent? आपल्याला...ली आहे का, जी फसवणूक असू शकते असे आपल्याला वाटले?

31 responses



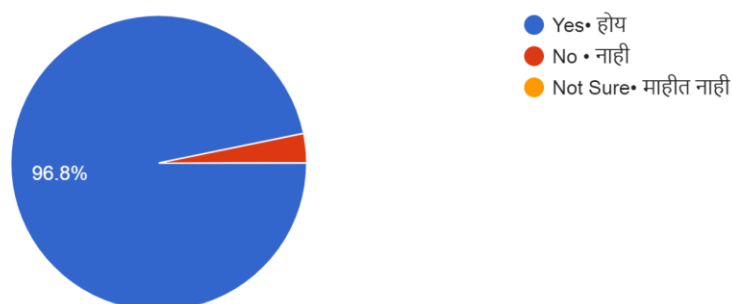
How would you rate your overall awareness of financial fraud through social engineering? सोशल इंजिनिअरिंगद्वारे होणाऱ्या आर्थिक फसवणुकीबाबत आपल्या एकूण जागरूकतेचे स्तर आपण कसे सांगाल?

31 responses



In your opinion, is there a need for greater awareness among digital banking users regarding social-engineering based financial fraud? आपल्या...कीबाबत अधिक जागरूकता निर्माण करण्याची गरज आहे का?

31 responses





Hypothesis Testing:

The researcher has used ANOVA test to test the hypothesis. The independent variables are age, education of respondents and frequency of usage of digital banking platform. The dependent variable is awareness about financial frauds through the social engineering. The researcher has used Two-factor without Replication ANOVA test for testing of hypothesis.

H_0 : There is no significant relation between age, education of the digital banking users and financial fraud awareness.

H_1 : There is significant relation between age, education of the digital banking users and financial fraud awareness.

Level of Significance: 0.05

ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Rows	14.48387097	30	0.482795699	0.647907648	0.879838	1.840872
Columns	0.14516129	1	0.14516129	0.194805195	0.662112	4.170877
Error	22.35483871	30	0.74516129			
Total	36.98387097	61				

The calculated *P-value* is greater than the 0.05. The *F* value is less than the *F critical* value, therefore the **fail to reject null hypothesis** i.e. there is no significant relation between age, education of the digital banking users and financial fraud awareness.

H_0 : There is no significant relation between frequency of digital banking usage and financial fraud awareness.

H_1 : There is significant relation between frequency of digital banking usage and financial fraud awareness.

ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Rows	14.48387097	30	0.482795699	0.647907648	0.879838	1.840872
Columns	0.14516129	1	0.14516129	0.194805195	0.662112	4.170877
Error	22.35483871	30	0.74516129			
Total	36.98387097	61				

The calculated *P-value* is greater than the 0.05. The *F* value is less than the *F critical* value, therefore the **fail to reject null hypothesis** i.e. there is no significant relation between frequency of digital banking usage and financial fraud awareness.

Conclusion:

The researcher found that the respondents have good level of awareness about the social engineering practices and financial fraud. 74.2% of respondents were aware that the fraudsters imitate



that they are bank officials; police officers etc. 90.3% respondents were strongly agreed regarding not to share confidential information like CVV, OTP, ATM PINs, and password.

The researcher has also found that, 93.6% respondents can identify suspicious phone calls, messages, links, QR codes or online payment requests. 100% of respondents were aware about the fraudsters may use psychological technique like fear, urgency, prizes, rewards or attractive offers to make people send money or share bank details. 80.6% respondents were aware about where and how to report a suspected online financial fraud or an unauthorised bank transaction if occurred. 16.1% respondents were neutral for this information and 3.2% respondents were not aware about the mechanism for financial fraud reporting.

77.4% respondents were said that they get the information about financial fraud and online banking safety from the social media platform. 64.5% respondents said that they get the information from the Government or cybercrime awareness campaign. 51.6% respondents said that they get the information from the banks and financial institutions.

The researcher found that the 87.1% respondents have received awareness message, email, call, notification or warning regarding financial fraud from your bank. But 9.7% respondents said that they have not received any awareness message, email, call, notification or warning regarding financial fraud from your bank.

3.2% respondents were confused they preferred not to say anything.

The study concludes that the respondents have awareness about financial fraud and social engineering, but continuous awareness programmes amongst users is necessary. Through survey the researcher found that 96.8% respondents were aware about the financial frauds through social engineering.

References:

1. National Crime Records Bureau. (2024). Crime in India 2023. Ministry of Home affairs, Government of India.
2. Reserve Bank of India. (n.d.). Financial awareness and safe digital banking initiatives. Reserve Bank of India.
3. Hadnagy, C. (2018). Social engineering: The science of human hacking. Indianapolis, IN: Wiley.
4. Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM computing surveys.
5. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications.
6. Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. Journal of Financial Crime.
7. Financial Frauds in India – Legal Action. (2022). S.S. Rana & Co.