Indian Journal of
Modern Research and Reviews

This Journal is a member of the 'Committee on Publication Ethics'

Online ISSN:2584-184X

Research Article

Cyber Literacy of Bank Customers: A Study in Udupi City

Jayalaxmi *
Assistant Professor, Department of Commerce and Management
Poorna Prajna College (Autonomous), Udupi, Karnataka, India

Corresponding Author: * Jayalaxmi

DOI: https://doi.org/10.5281/zenodo.18738837

Abstract

The rapid digitalisation of banking services has fundamentally transformed financial transactions in India. While online banking and digital payment platforms have enhanced convenience, efficiency, and accessibility, they have simultaneously increased customers' exposure to cyber risks. A major concern is that a significant proportion of cybercrime incidents remain unreported, indicating deficiencies in cyber awareness and response mechanisms. This study examines the level of cyber literacy among bank customers in Udupi city, focusing on awareness of cyber threats, digital behavioural practices, and responses to fraudulent activities. Primary data were collected from 88 bank customers using a structured questionnaire. The analysis reveals that although most respondents actively use e-banking services, awareness of advanced cyber threats, secure digital practices, and formal reporting procedures remains inadequate. The study highlights the urgent need for structured cyber education initiatives by banks and regulatory authorities to strengthen customer cyber literacy and ensure the long-term sustainability of digital banking systems.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 20-12-2025
- **Accepted:** 11-02-2026
- **Published:** 23-02-2026
- **MRR:**4(2); 2026: 369-373
- **©2026, All Rights Reserved**
- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Jayalaxmi. Cyber literacy of bank customers: a study in Udupi City. Indian J Mod Res Rev. 2026;4(2):369-373.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cyber literacy, cybercrime, digital banking, customer awareness, cybersecurity.

© 2026 Jayalaxmi**. This** is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

1. INTRODUCTION

The Indian banking sector has experienced a profound transformation with the adoption of digital technologies. Internet banking, mobile banking, and digital payment applications have enabled banks to improve service delivery, reduce operational costs, and enhance customer convenience. However, this rapid digital expansion has also widened the scope for cyber threats, particularly affecting individual customers who may lack adequate cybersecurity awareness.

Cybercrime in the banking sector is transnational in nature, driven by anonymity, jurisdictional limitations, and the technological sophistication of cyber offenders. Fraudulent activities such as phishing, vishing, spyware attacks, identity theft, spoofing, and malware intrusions have become increasingly common. Despite the growing prevalence of such incidents, a large proportion of cybercrimes remain unreported due to lack of awareness, fear of procedural delays, and limited trust in grievance redressal systems.

Cyber literacy has emerged as a critical factor in mitigating cyber risks in digital banking. It extends beyond basic technological usage to include awareness of cyber threats, ethical digital behaviour, preventive practices, and appropriate response strategies. Assessing customer cyber literacy is therefore essential for strengthening the security of digital banking ecosystems. This study attempts to analyse the cyber literacy of bank customers in Udupi city by examining their awareness levels, behavioural practices, and responses to cyber threats.

2. REVIEW OF RECENT LITERATURE (2020–2025)

Recent studies consistently indicate that digital banking adoption has increased customer exposure to cyber risks. Research highlights that cybercrime is increasingly facilitated by human and behavioural vulnerabilities rather than purely technical failures. Scholars emphasise that customers' lack of awareness, unsafe digital habits, and excessive reliance on institutional safeguards significantly contribute to cyber fraud incidents.

Post-2020 literature identifies cyber literacy as a multidimensional construct involving knowledge, behaviour, and response capability. Empirical studies show that while customers are generally aware of basic threats such as phishing, awareness of sophisticated attacks like pharming and spyware remains limited. Moreover, a persistent gap exists between awareness and actual behaviour, as customers often fail to adopt secure practices due to convenience or complacency.

Recent research also underlines the critical role of banks in promoting cyber literacy. Passive communication methods such as SMS alerts are found to be insufficient, while interactive awareness programmes and targeted education initiatives are more effective. The literature further highlights under-reporting of cybercrime as a major challenge, limiting institutional learning and policy response.

Overall, existing studies point to the need for region-specific empirical research focusing on customer behaviour, awareness gaps, and institutional interventions. The present study contributes to this gap by examining cyber literacy among bank customers in a semi-urban Indian context.

3. OBJECTIVES OF THE STUDY

The study is undertaken with the following objectives:

1. To identify major cyber threats associated with digital banking services.
2. To assess the level of cyber awareness among bank customers.
3. To examine customers' cyber-related behavioural practices.
4. To analyse customer responses to cyber fraud attempts.
5. To suggest measures for enhancing cyber literacy and digital security.

4. RESEARCH METHODOLOGY

The study is based on both primary and secondary data. Primary data were collected from 88 customers of different banks in Udupi City during January 2026 using a structured questionnaire. A convenience sampling technique was adopted for selecting respondents. Secondary data were collected from journals, reports, and published literature related to cybercrime and digital banking.

5. Conceptual Framework

The conceptual framework of the study is based on the premise that customer cyber literacy significantly influences vulnerability to cyber threats in digital banking. Cyber literacy is conceptualised as a combination of cyber awareness, behavioural practices, and response mechanisms. Customer awareness of cyber threats influences digital behaviour such as password management, verification of applications, and information sharing. Behavioural practices directly affect exposure to cyber risks, while timely reporting of suspicious activities moderates the impact of cyber threats. Institutional support through bank-led awareness initiatives acts as an external factor strengthening customer cyber literacy.

6. LIMITATIONS OF THE STUDY

- The study is limited to bank customers in Udupi city.
- The sample size of 88 respondents may not fully represent all bank customers in the region.
- Data were collected through an online questionnaire, which may involve response bias.

7. Data Analysis and Interpretation

7.1 Age of respondents

Age	Number of respondents	%
20 yrs -29 yrs	62	70.5%
30 yrs-39 yrs	20	22.7%
40 yrs-49 yrs	04	4.5%
50 and above	02	2.3%

70.5% of the respondents belongs to age group 20 years to 29 years. 22.7% respondents belong to age group 30 years to 39 years.

© 2026 Jayalaxmi. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

7 .2 Education level

Education	Number of respondents	%
Below graduation	01	1.1%
Graduate	9	10.2%
Post graduate	78	88.7%

88.7% of the respondents had post graduate degree in a different stream. 10.2% are graduates.

7.3 Occupation

occupation	Number of respondents	%
Employee	76	86.3%
Own Business	07	8%
Other	05	5.7%

86.4% respondents are employees in different sectors. 5.6% have their own business and 8% are engaged in other occupations

7.4 Annual income in rupees

In rupees	Number of respondents	%
1,50,000 to 2,50,000	25	28.4%
2,50,000 to 4,00,000	30	34.1%
4,00,000 to 5,50,000	06	6.8%
above 5,50,000	27	30.7%

34.1% are in income band of Rs 2,50,000 to 4,00,000. 30.7% are in income group above 5,50,000 per year and 28.4% fall in the annual income group Rs.1,50,000 to 2,50,000.

7.5 Having credit card

Response	Number of respondents	%
Yes	87	98.9%
No	1	1.1%

98.9% among the respondents have debit or credit card.

7.6 Identity theft awareness

Response	Number of respondents	%
Yes	53	60.2%
No	35	39.8%

60.2% respondents have heard identity theft. 39.8% have not heard term identity theft even though they are graduated and post graduated.

7.7 Common cyber threats that customers are aware of.

Spyware is familiar for 51% of the respondents. Phishing and bugging stand in the second position with 38.6%. skimming stands in the third position with 33% in customer awareness. But there is very less awareness about pharming (only 6.8%) and watering the whole (3.4%). Only 14.8% are aware about all the cyber threats. Notably 18.2% of the respondents are not aware about any of the threats mentioned above.

7.8 Habit of storing debit and credit card information in smartphones and computers.

Response	Number of respondents
Always	13
Sometimes	32
Never	43

48.9% replied that they never store debit and credit card information in smartphones or computers. 36.4% store the information sometimes. Now the concern is for 14.4% of the respondents those who always store information in mobile or computer. Cyber-attack chances are high.

7.9 Customer credential enquiry by bank

Response	Number of respondents	%
Yes	06	6.8%
No	80	90.9%
Don't know	02	2.3%

Among the respondents, 90.90% are aware that, banker never ask for secret information over the phone or mail.

7.10 Requesting for bank account and card detail by third party

Response	Number of respondents	%
Yes	47	53.40%
No	31	46.60%

53.4% of respondents received an enquiry and 46.60% respondents didn't receive any enquiry.

7.11 Mode through which they have received such enquiry

Out of 88 respondents, 47 respondents have received an enquiry. 55.1% of such enquiry will came through either SMS or call. Only 32.7% will come through email. High use of mobile and infrequent access to email may be the reason. 41 respondents didn't receive any.

7.12 Report to concerned authority about the enquiry

Response	Number of respondents	%
Yes, always	09	19.14%
Yes, sometimes	25	53.19%
Never	13	27.65%

Only 19.14% reported such incidents to police or bank regularly. 53.19 inform sometimes. 27.65% never reported such fake enquiries to either police or bank.

7.13 Whom they prefer to report to

To whom	Number of respondents	%
Banker	60	68.2%
Police	19	21.6%
Tele or Internet service provider	09	10.2%

© 2026 Jayalaxmi**. This** is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

68.2% of the respondents prefers to report first to banker. 21.6% prefers to report first to police.10.2% prefers to report first to Tele or Internet service provider.

7.14 Disclosing bank details to third party

Response	Number of respondents	%
Yes,	85	96.6%
No	03	3.4%

96.6% respondents not disclosed the bank details. 3.4% (3 respondents) of the respondent have disclosed bank details to third party. Out of these three, 2 respondents lost their money to internet fraudsters.

7.15 Lost money for internet fraudster

Response	Number of respondents	%
Yes,	83	94.3%
No	05	5.7%

Out of 88 respondents, 94.3% (83 respondents) respondents didn't incur any monetary loss. 5.7% (5 respondents) have lost money for internet fraudster. Out of these five, 2 respondents have shared their details.

7.16 Having E-banking and payments app

Response	Number of respondents	%
Yes,	83	92%
No	07	8%

92% have active e-banking and payment app. This may be because of Most of the respondents are belong to age group 20 year to 39 years i.e. young group and normally they are technology savvy.

7.17 Safety of online operation- customer perception

Response	Number of respondents	%
Highly secured	14	15.9%
Moderately secured	61	69.3%
Not secured	06	6.8%
I don't know	07	8%

Among the respondents 69.3% opined that online operations are moderately secured. 15.9% opined that online bank operations are highly safe. Only 6.8% said that online transactions are not safe. 8% respondents don't have any idea about it

7.18 Genuineness verification of third-party app

Response	Number of respondents
Yes	51
No	15
I don't know how to verify	21
I know how to verify, but I won't because it prolongs	1

58% of respondents (51 respondents) verify the genuineness of third-party app while downloading in mobile or computer. 23.9% (21 respondents) don't know how to verify. 17% (15 respondents) won't verify the genuineness, they simply download it. 1.1% not do because of time lag in it.

7.19 Password Creation

Response	Number of respondents
By using self-information (name, mobile number, date of birth, etc.).	16
By using name of relatives and close people.	01
Easy to remember formats (123., 0000, 1122, etc.).	04
A combination of letters, numbers and punctuation.	21
Sorry! I can't say this	46

Among the respondent 52.3% are cautious, as they were not shared anything about it. The remaining 47.7% are revealed that how they set password. Out of this 18.2% by using self-information, 4.5% easy remember format, 23.9% combination of letter number and special character.1.1% use close person name as password.

7.20 Frequency of password change

Response	Number of respondents
Once in a fortnight	12
Once in a month	16
Semi Annually	25
Once in Year	12
Never	23

Among the respondents 28.4% change only twice in a year. 26.1% never changed password since the beginning, 18.2% change once in a month, 13.6% change their password once in 15 days and 13.6% are once in a year.

7.21 Fake website recognition

response	Number of respondents
Always	16
Sometimes	47
I can't	25

When we asked about their ability to differentiate fake and real website, 53.4% were said that, sometime they are able to recognize, 28.4% (25 respondents) respondents are not in position to differentiate and Only 18.2% can identify fake websites all the time.

7.22 Cyber education by the bank to customer about cyber threats.

71.76% opined that the bank sends only text messages. 30.7% received email from their respective bank. Only 11.4% opined that banks conduct an awareness programme. 19.3% opined that banks do very less to educate their customer.

8. Findings

- The majority of respondents (60.2%) are aware of identity theft, while 39.8% are unaware despite higher education.

© 2026 Jayalaxmi**. This** is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/

- Awareness of cyber threats is inadequate; only 14.8% are aware of all major threats.
- Risky practices such as storing card details digitally persist among 14.4% of respondents.
- Over half of the respondents (53.4%) received fraudulent requests for bank details.
- Regular reporting of cyber incidents is low (19.14%).
- Majority (96.6%) did not disclose bank details; those who did faced financial loss.
- Digital banking usage is high, but cyber preparedness remains moderate.
- Weak password practices and difficulty identifying fake websites increase vulnerability.
- Banks largely rely on SMS for cyber education, with minimal structured programmes.

9. Suggestions

- Banks should conduct regular cyber awareness and training programmes.
- Customers should be educated on strong password creation and frequent updates.
- Banks must clearly communicate that confidential details are never requested digitally.
- Simplified cybercrime reporting mechanisms should be promoted.
- Awareness regarding app verification and fake website identification must be strengthened.
- Coordinated efforts among banks, regulators, and law enforcement agencies are essential.

10. CONCLUSION

The study reveals that while digital banking adoption among customers in Udupi city is widespread, cyber literacy has not progressed at the same pace. Increased dependence on technology has enhanced convenience but also heightened exposure to cyber risks. Ensuring digital banking security requires shared responsibility between banks and customers. Technological safeguards must be supported by informed customer behaviour and continuous awareness initiatives. Strengthening cyber literacy is therefore essential for reducing cybercrime, enhancing trust, and ensuring the sustainable growth of digital banking.

REFERENCES

1. Shaik S, Sameera SA. Security issues in e-banking services in Indian scenario. Asian J Manag Sci. 2014;2(3):28–30.
2. Desikan A. Mobiles making India less cash conscious. The Times of India. 2016 Feb 22.
3. Bakar MH, Ramli NN, Yahaya SN. Cyber security awareness among digital banking users in Malaysia. Int J Res Soc Sci Inf Secur. 2025;9(10).
4. Furqon MAA. Digital security literacy of bank and fintech customers. Int J Sci Soc. 2025;7(3).
5. Nagari SF, Raharja S. Cybersecurity awareness, knowledge, and behaviour of digital banking users. Asia Pac Fraud J. 2025;10(1).
6. Shukla K, Ahmad DS, Bajpai DP, Shrivastava N, Fatima R. Customer awareness of cybersecurity measures in online banking. CINEFORUM. 2025;65(2):361–386.
7. Waliullah M, et al. Cybersecurity threats and digital banking adoption: A systematic review. arXiv [Preprint]. 2025.

Creative Commons License

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution–Non-commercial–No Derivatives 4.0 International (CC BY-NC-ND 4.0) License. This license permits users to copy and redistribute the material in any medium or format for non-commercial purposes only, provided that appropriate credit is given to the original author(s) and the source. No modifications, adaptations, or derivative works are permitted.

About the corresponding author

Jayalaxmi. MCom, MBA, M.Phil. At present, working as an Assistant Professor, Department of Commerce and Management in Poornaprajna College (Autonomous), Udupi. She has 28 years of Teaching Experience. She has authored 6 reference books, has published more than 45 research papers and presented more than 85 papers in Conferences. She has guided many undergraduate and postgraduate students of different Universities for their mini-research work

© 2026 Jayalaxmi**. This** is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND).https://creativecommons.org/licenses/by/4.0/