WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Consumer data protection in online marketing

P Veerasai[1], Dr. K. V. V. Raju[2]

[1]MBA Student, Department of MBA, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Andhra Pradesh, India Mail ID:veerasaipalacharla@gmail.com

[2]Associate Professor, Department of MBA, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Andhra Pradesh, India Email ID: raju8187@kluniversity.in

ABSTRACT:

Online banking, often referred to as e-banking or internet banking, enables users to carry out financial transactions over the internet. As digitalization continues to grow, it has become an essential aspect of modern banking. However, the security of personal and financial information in online banking raises significant concerns. With more data being shared online, the risks of data breaches, phishing scams, and identity theft have surged. Consequently, safeguarding consumers has become a top priority in banking regulations and practices.

So, what exactly is consumer data protection? In the context of online banking, it refers to the safeguarding of sensitive financial and personal information that customers provide through online banking platforms. This includes protecting against unauthorized access, cyber theft, data diversion, and tampering

INTRODUCTION:

Online banking, also known as e-banking or internet banking, allows consumers to perform financial transactions through the internet. With growing digitalization, it has become a fundamental part of modern banking. However, the security of personal and financial data in online banking is a critical concern. As more data is shared electronically, the risk of data breaches, phishing attacks, and identity theft has increased. Therefore, consumer data protection is now a central issue in banking regulations and operations.

Definition of Consumer Data Protection:

Consumer data protection in internet banking is the protection of sensitive financial and personal information provided by customers via online banking websites. This involves protection against illegal access, cyber theft, misappropriation, and tampering.
With digital transformation, banks have incorporated online and mobile banking services on a large scale. Even though such portals provide convenience, they also expose the users to cyber threats. With more and more cases of data breaches and identity theft happening, consumer data protection is no longer an option but a must.

RESEARCH METHODS:

Research Approach
This research employs a mixed-method approach, utilizing both quantitative and qualitative methods to explore consumer data protection in online banking. This combination helps to gain a comprehensive understanding of the topic.

2. Research Type
Quantitative: This aspect focuses on assessing consumer awareness, perceptions, and satisfaction through structured surveys.
Qualitative: This part aims to gather insights into policies, practices, and expert opinions through document analysis and open-ended responses.

3. Research Design
The study adopts a descriptive and analytical research design.
Descriptive: This provides an overview of the current state of consumer data protection in online banking.
Analytical: This examines how banking practices influence consumer trust.

DATA SOURCES:

Primary Data Sources
Primary data is collected directly from respondents to understand consumer awareness, perceptions, and experiences.
Online Surveys and Questionnaires distributed to:
Customers of public and private sector banks
Users of online/mobile banking platforms

Secondary Data Sources
Secondary data is collected from existing published materials and official websites to understand policies, regulations, and industry practices.
Regulatory Bodies:
Reserve Bank of India (RBI) guidelines on cybersecurity and digital banking
Ministry of Electronics and Information Technology (MeitY) – IT Act and Digital Personal Data Protection Act

DATA EXTRACTION:

Primary Data Extraction
We gather primary data from responses collected through structured questionnaires or online surveys targeted at online banking users. These responses are collected using tools like Google Forms or printed questionnaires. Once collected, the data is downloaded or exported into Microsoft Excel or SPSS format for further processing.

Secondary Data Extraction
For secondary data, we turn to reliable published and online sources, including government reports, bank websites, research journals, and news portals. Some key sources include:
- RBI Guidelines on cybersecurity in online banking
- Digital Personal Data Protection Act, 2023 (India)
- Annual reports from banks like SBI, ICICI, and HDFC
- Journal articles from UGC/Scopus-listed journals
- Case studies and reports on cybersecurity incidents

ETHICAL CONSIDERATIONS:

To ensure your data is both accurate and transparent, it's crucial to rely solely on verified financial reports from trusted sources. At the same time, it's important to protect sensitive or proprietary bank information and keep it confidential. Avoid bias in your analysis by using objective financial metrics and standardized CAMELS criteria. Always adhere to the regulatory and ethical guidelines set forth by RBI, SEBI, and Financial Reporting Standards.

REVIEW OF LITERATURE:

1.Title:Impact of Awareness on Data Security
Authors :Gupta & Dhillon (2020)
Published In :Journal of Cybersecurity and Information Management
Volume:Vol. 12, Issue 1
Methodology :Quantitative survey (150 respondents)
Hypothesis :Lack of awareness increases data vulnerability
Findings :Many customers were unaware of bank privacy policies; awareness improves protection behavior

2.Title:Cybersecurity in Indian Banking
Authors :Kaur & Arora (2021)
Published In :Int. Journal of Banking Technology
Volume :Vol. 9, Issue 2
Methodology :Case study of 3 Indian banks
Hypothesis :Cybersecurity measures reduce consumer fraud
Findings :Banks with 2FA and encryption reported fewer fraud incidents

3.Title:Trust and Transparency in Online Banking
Authors :Singh & Rani (2022)
Published In :Int. Journal of Finance and Banking Research
Volume:Vol. 15, Issue 3
Methodology :Survey + regression analysis (N=200)

Hypothesis :Consumer trust improves with transparent data practices
Findings :Trust is highly influenced by visible data security efforts

4.Title:Security and Customer Loyalty
Authors : Bansal & Lal (2019)
Published In :Asian Journal of Management Studies
Volume:Vol. 11, Issue 4
Methodology :Structured questionnaire
Hypothesis :Strong data practices increase customer loyalty
Findings :Positive correlation between security and repeat use of online banking

5.Title:Legal Implications of the DPDP Act
Authors :Legal Implications of the DPDP Act
Published In :Sharma (2023)
Volume:Indian Journal of Law and Technology
Methodology :Vol. 18
Hypothesis :Doctrinal legal research
Findings :Internal and phishing attacks are rising, need for predictive AI systems

6.Title: Threat Landscape in Online Banking
Authors :Threat Landscape in Online Banking
Published In :Verma (2020)
Volume:Journal of Financial Crime
Methodology :Vol. 27, Issue 2
Hypothesis :Secondary data
+ threat analysis
Findings :Internal and phishing attacks are rising, need for predictive AI systems

7.Title:A Comparison of GDPR and Indian Laws
Authors :Patel & Mehta (2021)
Published In :Review of Law and Economics
Volume:Int. Vol. 61
Methodology :Comparative legal analysis
Hypothesis :GDPR more robust than Indian laws
Findings :Indian laws improving, but enforcement and consumer rights are weaker

ANALYSIS:

1. Demographics: 60% of respondents are male, representing a mix of ages and professions.
2. Familiarity: 61.1% are very familiar with banks like SBI, HDFC, and ICICI.
3. Data Collected: A whopping 85% of users reported that their banks gather personal information, including Aadhaar, PAN, phone location, and transaction history.
4. Consent Clarity: 68.7% agreed that consent is often bundled with other agreements and isn't clearly explained; many feel pressured to accept terms without fully understanding them.
5. Security Incidents: 14.6% of participants experienced issues like phishing, OTP fraud, or unauthorized access, raising concerns about banks' cybersecurity practices.
6. Trust in Banking Platforms: 55.9% expressed moderate trust in their bank's ability to protect personal data, while only 18.3% felt highly confident, indicating a clear need for better security assurances.
7. Limited User Rights: Just 25.4% believed they had control over their data (like the right to delete or limit its use). A significant 64.8% were unaware of any legal options or data protection measures available to them.
8. Policy Understanding: A staggering 72.6% had never heard of India's Digital Personal Data Protection Act, 2023, and only 9.2% were aware of their rights under it, such as the right to erasure, data portability, and consent withdrawal.

DISCUSSION:

The swift rise of digital financial services has completely transformed how consumers engage with banks, bringing in a level of convenience, speed, and accessibility that we've never seen before. But with these advancements come serious concerns about consumer data privacy and protection. This study aimed to explore how aware, trusting, and experienced consumers are when it comes to data protection practices in online banking, especially in India.

The results show that while a good number of consumers are using digital banking services, there's a significant disconnect between how much they use these services and their understanding of data privacy. Even though 58.2% of respondents said they were familiar with the idea of data privacy, only a small portion—less than a third—actually read or grasp the privacy policies of their banks. This points to the fact that while digital skills may be on the rise, understanding data privacy is still falling behind.

CONCLUSION:

Online banking is definitely the way of the future, but it can only thrive if we prioritize strong consumer data protection. The survey reveals that even though Indian banks have made strides in enhancing security measures, there are still challenges around awareness, technology implementation, and policy enforcement. To build a secure online banking environment, we need a balanced approach that includes stricter regulatory compliance, cutting-edge cybersecurity infrastructure, and robust customer awareness programs. Only then can we ensure lasting consumer trust in online banking.

REFERENCES:

1.Gupta, R., & Sharma, N. (2019). Online Banking Security in India. *Journal of Digital Finance*, 12
2.Rajput, A., & Chatterjee, S. (2020)
Cybersecurity Challenges in Indian Banking Sector: Focus on Consumer Data Privacy.
Journal of Banking Technology, 5(1), 33–47.
3.Patil, A., & Kulkarni, P. (2022).
Evaluating Data Privacy Awareness Among Online Banking Users in India.
South Asian Journal of Digital Banking, 11(4), 122–135
4..Sharma, P., & Mehta, D. (2020).
Data Protection Policies and Consumer Trust in E-Banking Services.
Indian Journal of Management and Banking, 14(3), 91–105.
5.Kumar, S., & Iqbal, T. (2019).
Impact of GDPR and India's Data Protection Bill on Online Banking Ecosystems.
6.Singh, R., & Ruj, S. (2020).
A Technical and Legal Look at India's Personal Data Protection Bill.
arXiv preprint.
7.Reserve Bank of India (RBI). (2020).
Report of the Working Group on Digital Lending – Including Lending through Online Platforms and Mobile Apps