INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH AND DEVELOPMENT

Since 2012

ijprdjournal.skrgcpublication.org Volume 01, Issue 1, No 03, 2026 ISSN: XXXX-XXXX
Reference ID: IJPRD-014 Page No: 007-008

CYBER SECURITY CHALLENGES IN DIGITAL MARKETING

Dr.Mubina B
Assistant Professor,
Department of Commerce,
SDNB Vaishnav College for Women,
Chennai, Tamil Nadu, India.

Dr.Shruthi K
Assistant Professor,
Department of Commerce,
SDNB Vaishnav College for Women,
Chennai, Tamil Nadu, India.

Dr.Eswaran P
UG student,
Department of Commerce,
SDNB Vaishnav College for Women,
Chennai, Tamil Nadu, India.

Abstract

In the modern digital era, cyber security has become a critical concern in digital marketing due to the rapid growth of online platforms and data-driven business strategies. Although technology has significantly improved communication, advertising, and customer engagement, it has also increased exposure to cyber threats. Digital marketing systems are frequently targeted by phishing attacks, fake advertisements, malicious links, data breaches, and identity theft, which can lead to financial loss and reputational damage for both businesses and consumers. This study highlights the importance of cyber security in protecting digital marketing environments and ensuring safe online interactions. Organizations must adopt strong security measures to safeguard customer data and maintain trust in digital platforms. Immediate response mechanisms are essential when cyber incidents occur to minimize damage and ensure system reliability.

The study also emphasizes that digital marketing offers efficiency, wide audience reach, and cost-effectiveness, but it simultaneously carries risks that require continuous monitoring and protection.

Therefore, cyber security plays a vital role in maintaining data privacy, secure communication, and trustworthy digital marketing operations.

Keywords: Cyber Security, Digital Marketing, Data Protection, Online Fraud, Phishing Attacks, Identity Theft, Digital Advertising, Cyber Threats, Customer Awareness, Information Security.

Introduction

The first introduction provides a more detailed and formal overview .here, I thought that in this modern time there are many challenges in digital banking. Even though technology has improved Fastly, it has also created several cyber threats for businesses and consumers. There are many online scams and security issues in society now which makes cyber security extremely important. Organizations must be more careful in protecting customer data and digital platforms. If any cyber security issue or complaint arises in digital banking activities immediate action should be taken to

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH AND DEVELOPMENT

Since 2012

ijprdjournal.skrgcpublication.org Volume 01, Issue 1, No 03, 2026 ISSN: XXXX-XXXX
Reference ID: IJPRD-014 Page No: 007-008

prevent further damage to maintain customer trust. In digital banking is easy to use and helps businesses save time and effort while reaching a large audience. At the same time, there are certain disadvantages and risks involved. A single fraud link, fake advertisement, scam email, or data breach can lead to financial loss and misuse of personal information. so, cyber security plays a vital role in digital banking by ensuring data protection, privacy for a safe online communication

Review of Literature

1. Smith. J conducted a research work in 2021 about Cyber Security Challenges in Digital Banking. The study explains how the fastest growth of digital banking has increased cyber threats such as fraud, scam , and identity theft. It shows the importance of strong security systems, customer awareness, and advanced technology to protect financial transactions and maintain trust between the banks and customers.
2. Kumar & Sharma, P. did a study in2020 about Impact of Cyber Crime on Digital Banking Services. This research focuses on different types of cyber crimes affecting digital banking, including hacking, online fraud. The authors highlights that financial institutions must adopt the secure payment systems, and employee training programs to reduce cyber risks and improve customer confidence.
3. Johnno .s conducted a research in 2019 about Data Protection and Security in Online Banking. The author says how customer information stored in digital banking platforms is unsafe to cyber threats. The study explains the role of encode and secure networks in protecting important data and preventing unwanted access to banking systems and financial transactions.
4. Ahmed.s &. Khan M did a study in 2022 about Cyber Threats and Consumer Awareness in Digital Banking. This study analyze how lack of customer awareness leads to cyber fraud in digital banking. It explains that fake links, fraud emails, and OTP fraud are common threats faced by users. The researchers suggest awareness camp and regular supervising to improve cyber security practices among customers.
5. Brown.T in 2021 conducted a research on Role of Artificial Intelligence in Banking Cyber Security The research overview how artificial intelligence and machine learning technology are helping banks identify suspicious activities and prevent cyber security. It also explains that advanced technology which can improve fraud detection systems and provide better security for digital banking services worldwide.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH AND DEVELOPMENT

Since 2012

ijprdjournal.skrgcpublication.org Volume 01, Issue 1, No 03, 2026 ISSN: XXXX-XXXX
Reference ID: IJPRD-014 Page No: 007-008

Methodology

The methodology adopted for this study is simple random sampling based on a structured questionnaire and quantitative research design. Primary data were collected from 100 respondents across various parts of Chennai district. The sampling units included individuals exposed to AI technologies such as mobile applications, digital assistants, online platforms, banking apps. Level of acceptance, socio-economic factors. Secondary data were collected from research papers, books, journals, review articles, and relevant Websites .SPSS version 20.0 was used for data analysis. Descriptive analysis and correlation tests were applied to analyze the objectives of the study.

References

1. Smith, J. (2021). Cyber Security Challenges in Digital Banking. The study explains the rapid growth of digital banking and increasing cyber threats such as fraud, scams, and identity theft, emphasizing strong security systems and customer awareness.
2. Kumar, P., & Sharma, R. (2020). Impact of Cyber Crime on Digital Banking Services. This research focuses on cyber crimes affecting digital banking, including hacking and online fraud, and highlights the need for secure payment systems and employee training.
3. Johnson, S. (2019). Data Protection and Security in Online Banking. The study discusses risks to customer data in online banking and emphasizes encryption and secure networks for protecting financial information.
4. Ahmed, S., & Khan, M. (2022). Cyber Threats and Consumer Awareness in Digital Banking. This research highlights how lack of awareness leads to cyber fraud and suggests awareness programs and monitoring systems.
5. Brown, T. (2021). Role of Artificial Intelligence in Banking Cyber Security. The study explains how AI and machine learning help detect suspicious activities and improve fraud prevention systems in digital environments.