JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ONLINE BANKING AND CYBER ATTACKS: THE RECENT SCENARIO IN INDIA

Dr.M. SUMATHI
Assistant Professor Of Commerce
*Dr. Umayal Ramanathan College for Women, Karaikudi

R.SUNDARALAKSHMI
M.Phil.(Commerce) Scholar
*Dr. Umayal Ramanathan College for Women, Karaikudi.

Abstract:

Internet banking or online banking has revolutionized an integral exertion of our ultramodern twenty-first century. Man developed colorful ways of communication for the conversation of evidence, ideas, and knowledge which is of great significance to him as a social being. The elaboration of e-banking technology makes the task veritably readily, banking deals come presto within a click. Operational and moveable banking make diurnal banking fast and accessible. The abuse of information technology in cyberspace is clinging up which gave birth to cybercrimes in the public and transnational situations. The chance of pitfalls and the challenges associated with it's increased. This exploration paper aims to review the current script of online banking and cyberattacks. In this paper, we concentrated on cybercrimes associated with available banking and original tricks and ways used by hackers.

Keywords: Info Technology, cybercrimes, cyber-attacks, mobile banking, effective banking.

INTRODUCTION

In the present script, online services have come to an added point in the banking sector. Guests to conduct fiscal deals on a secure website. Credit goes to the internet that handed ultimate ease to the guests at their doorstep. Online banking allows people to perform all the banking-related conditioning similar to plutocrat transfers, past transactional information, cash recessions, deposits, etc., with just one click of a mouse. Guests can fluently check their account balance every day just by visiting the website of their bank. This provides the place and time mileage to people handed if they've Internet access. With the paradigm shift of the Information Age, Computers have come to the instrument through which felonious acts are carried out as Technology-enabled crimes via the internet. Net crimes are high-tech crimes as the web connects people's biases bias encyclopedically. As technology grows, security on plutocrats is also a question mark the way in fraud discovery and banks should upgrade technology to combat cybercrimes. Banks calculate on digital networking for their ample business compass. This, in turn, aggravates the threat of banks and innocent guests to come victims of cybercrimes.

Review of Literature

Relinquishment of online banking services can be increased by the vacuity of quality internet connections like broadband (**Al-Somali et al., 2009**). But certain walls live that hamper which is from terrain to terrain.

According to the study of Laforet **and Li (2005)** perception of pitfalls as well as computer and technological chops are the main factors gumming online banking acceptance.

Goel, S. (2016). the E-the banking subdivision and overall tips to assist themselves from receiving a target of cybercrime.

Chevers, D.A. (2019). the continual growth of cybercrimes can hurt businesses and by extension the husbandry of countries. As a result, actions must be linked to overwhelming the problem.

Ezhilarasi, U. (2021) there's an appetite to probe the security issues in the prosecution of technologies in banks, and how to overcome similar challenges is the need of the hour. In this study, the experimenter attempts to study the cybercrime script and its impact on banks in Puducherry.

Azhar, S., Shahi, M., & Chhapola, V. (2020). Behind should take while dining dealing with online deals on to secure banking, and the arising ways in which have the eventuality to combat this issue of banking frauds. This study also gives sapience into the fraudulent instruments, the way they're used in banking frauds, and how this problem is dealt with by applying instrument translucency.

Objectives of the study

1. To study the colorful cybercrimes in theE-banking sector in India
2. To identify the current script of cybercrimes.
3. To dissect and use the preventative measures available to control fraud

Cyber Crimes Related E-Banking Sector

Hacking

Hacking isn't defined in the amended IT Act, 200032. But under Section 43 (a) read Information Technology (Amendment) Act, 2008 and under Section 379 & 406 of Indian Penal Code, 1860, a hacker can be penalized. However, the indicted is penalized under IT Act, for imprisonment, Ifa similar crime is proved also for a similar hacking offense. The hacking offense is considered a cognizable offense, it's also a bailable offense.

Credit Card Fraud

Online credit card frauds take place when guests use their credit card or disbenefit card for any online payment and another person. Proprietor when electronic deals aren't secured.

Cybercriminal Pitfalls At the most simplistic position, the cybercriminal pitfalls imaged in the narratives can be broken down into the following orders

• Intrusion for financial or another benefit
• Interception for spying
• Manipulation of information or networks
• Data destruction
• Abuse of processing power
• Fake particulars
• Elusion tools and ways

Current Script of Cybercrimes

India is trying to apply the Digital India design to the stylish of its capabilities. The success of Digital India designs minimal cyber security pitfalls. The figures for playing incidents were in 2012 and 2011. As per the cyber-crime data maintained by National Cyber Records Bureau, an aggregate of, and cases were registered under the Information Technology Act in 2011, 2012, and 2013, independently. An aggregate of 422, 601, and cases were registered under cyber-crime-related sections of the Indian Penal Code in 2011, 2012, and 2013, independently. There has been a periodic increase of further than 40 percent in cyber-crime cases registered in the country during the once two-three times.

Conclusion

Society should report these cases to the Digital Wrongdoing Branch rather than involving the branches for quick and strict conditioning. Systems should be started to apprehensive the public about the nonstop situations and forthcoming situations. Corrections should be rehearsed fully to stop these issues and discipline the assaulters. The council should keep track of the working system of huge information banks. The law perpetration should be strict and sometimes cover similar wrongdoings. In addition, the study will be suitable to determine which of the three independent variables has the topmost impact on the relinquishment of e-banking.

REFERENCES

1. Agrawal, S. (2016). Cyber Crime in Banking Sector*. UdgamVigyati, 3, 1-19.
2. Al-Somali, S.A., Gholami, R. and Clegg B., (2009), "An investigation into the acceptance of online banking in Saudi Arabia", Technovation, Vol. 29, pp. 130–141.
3. Azhar, S., Shahi, M., & Chhapola, V. (2020). E-Banking Frauds: The Current Scenario and Security Techniques. In Encyclopedia of Criminal Activities and the Deep Web (pp. 905-918). IGI Global.
4. Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. In CONF-IRM (p. 11).
5. Ezhilarasi, U. (2021) Cyber Crimes in Banking Sector-An Evaluation.
6. Goel, S. (2016). Cyber-Crime: A growing threat to the Indian banking sector. In 3rd Int. Conf. Recent Innovation. Sci. Technol. Management. Environment (pp. 13-20).
7. Kumar, S., Koley, S., &Kuamr, U. (2015). Present scenario of cybercrime in India and its preventions. IJSER, 6(4), 1972-1976.

8. Laforet, S. and Li, X., (2005), "Consumers' attitudes towards online and mobile banking in China" International Journal of Bank Marketing, Vol. 23 No. 5, pp. 362-380.
9. Zahid, N., Mujtaba, A., & Riaz, A. (2010). Consumer acceptance of online banking. European Journal of Economics, Finance and Administrative Sciences, 27(1), 2010.
10. https://www.legalserviceindia.com/legal/article-3073-cyber-frauds-in-the-indian-banking-industry.html
11. Source-*http://www.cert-in.org.in/*
12. https://lawbhoomi.com/cybercrimes-relating-to-unauthorised-access-a-critical-study/