IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, March 2024

Cyber Crime in Banking Sector Mumbai

Hritika M. Ankolekar
Research Scholar
The Byramjee Jeejeebhoy College of Commerce, Mumbai, Maharashtra, India

Abstract: *Cybercrime in the banking sector has emerged as a significant threat, posing severe financial and reputational risks to financial institutions and their customers. This paper explores the various forms of cybercrime prevalent in the banking sector, including phishing, malware attacks, data breaches, and identity theft. It examines the tactics used by cybercriminals to exploit vulnerabilities in banking systems and the potential impact on financial stability and consumer trust. Moreover, the paper discusses the strategies adopted by banks and regulators to combat cybercrime, including enhanced cybersecurity measures, regulatory frameworks, and public-private partnerships. By understanding the nature of cyber threats and implementing effective countermeasures, banks can better protect their assets and uphold the integrity of the financial system.*

Keywords: Cybercrime

I. INTRODUCTION

Cybercrime is any criminal activity that involves a computer, network or networked device.
While most cybercriminals use cybercrimes to generate a profit, some cybercrimes are carried out against computers or devices to directly damage or disable them. Others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.
A primary effect of cybercrime is financial. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information.

Types Of Cybercrime

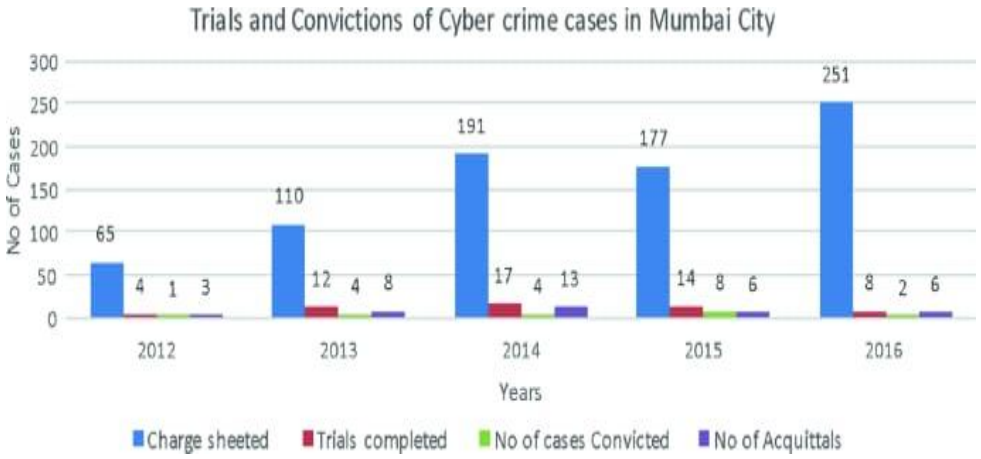
Cybercrime can be classified into various categories, including:
1. Hacking: Unauthorized access to computer systems or networks to steal sensitive information, disrupt operations, or cause damage.
2. Phishing: Sending fraudulent emails or messages, often disguised as legitimate entities, to trick individuals into revealing sensitive information.
3. Malware attacks: Distributing malicious software (e.g., viruses, ransomware) to infect computers and gain unauthorized access to data.
1. Online scams: Deceptive schemes designed to trick individuals into providing money, personal information, or sensitive data.
2. Financial fraud: Illegally obtaining money or assets through online transactions or fraudulent activities.

II. RESEARCH METHODOLOGY

The facts used is absolutely secondary in nature i.e., from assets published, printed media, magazines and journals. Objectives of the study:

- To examine cybercrimes and its implications at the Banking Sector
- To understand the seriousness of online cyber threats available to Internet banking enterprise.
- To understand the effects of cybercrime and its reasons.
- To degree the scope of protection and its implementation in Internet banking sectors
- To analyse and use the preventive measures available to manipulate frauds.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, March 2024



III. LITERATURE REVIEW

The internet is a medium that is becoming progressively important as it makes information available in a quick and easy manner. It has transformed communications and acts as a global network that allows people to communicate and interact without being limited by time, boarders and distance. However, the infrastructure is vulnerable to hackers who use the system to commit cyber crime. To accomplish this, they make use of innovative stealth techniques for their malicious purposes in the internet.

IV. CONCLUSION

Internet Banking is growing faster and getting vast. It is having more value than anything else for hacker or cyber criminals. It will never be 100% secure. 1 in a 4 people can likely be a victim of cyber attack. Financial sector will be main target for hackers. New technologies are coming, and hackers are getting smarter. Cyber security is important in online banking and its critical. 1 in a 4 people can likely be a victim of cyber attack. There is a big gap between banks and their customers regarding information about online banking and hacker and cyber criminals are taking advantage of this. Bank should inform customers how online transaction works. Bank should provide information in SMS what will this OTP (One Time password) will do. Bank should spread awareness about online banking and cyber fraud. People should not share their credentials with anyone. These simple measures can help people to protect their money and it will help in financial sector.

REFERENCES

[1]. https://www.techtarget.com/searchsecurity/definition/cybercrime
[2]. https://www.quora.com/What-is-cybercrime-1
[3]. https://ijarsct.co.in/Paper5468.pdf
[4]. https://www.bartleby.com/essay/Literature-Review-On-Cyber-Crime-PJP6L3WT26