A Study on Cyber Security Issues Affecting Online Banking and Online Transaction

Tejas Rao KG

Graduate Student, Bachelor of Commerce, CMR University, Bengaluru, Karnataka, India.

Abstract: Online banking and financial transactions over the internet are becoming more and more common in today’s digital age. But there are also new cyber security threats and challenges that come along with these luxuries. This study focuses on comprehending the weaknesses and difficulties that are directed at banking systems and consumer data and explores the challenges and risks associated with digital financial activity. The study closely goes through the available research and literature on cyber security in the banking industry in order to acquire ideas. It investigates typical cyber threats and their possible effects on the safety of banking systems and consumer data, including problems with confidentiality, integrity, and availability. This paper highlights how crucial security precautions like multi-factor authentication and encryption techniques are for boosting the safety of online banking platforms. Banks can improve system security and protect consumer data by putting these steps in place. The purpose of the findings of this research is to better understand the cyber security difficulties that the banking sector faces. The study also provides suggestions for enhancing the security of online banking and transactions.

Keywords: Cyber security, cyber threats, multi-factor authentication, banking systems

1. Introduction
The concept of lowering the danger of a cyber attack lies at the center of the entire cyber security system. The primary goal of cyber security is to keep all our electronic equipment, including computers, smart phones, and the online and workplace services that we utilize for both personal and professional purposes, safe from theft and harm. Sensitive data, personally identifiable information, protected health information, and information systems used by the government and business are all included. With the world turning completely digital in the twenty-first century, people find it convenient to utilize online banking rather than the old banking techniques. However, this also brings several risks, such as hacking, user account credit theft, loss of control, and account access.

Internet banking is the practice of doing financial transactions through the internet, such as creating a bank account and NEFT and other money transfers. Since its introduction, internet banking has gone through a period of adaptation and progress, but once again, all the variables worked in favorably, except for the fact that cybercrime was not under control. Every year, cyber security organizations provide fresh rules that must be followed. There are awareness campaigns carried out in schools and universities through debates and essay writing, but it is still a significant problem that millions of people throughout the world fall victim to every minute.

People all around the world have the misconception that cyber security is only a concern for information technology companies, but it also has an impact on the banking industry. It is of the utmost importance that banks take precautions to defend themselves from cyber attacks.

2. Objectives
- To raise awareness of global cybercrime
- To examine the value of cyber security
- To evaluate the relevance of preserving private data

3. Literature review
Dr. S. Nagaraju – (IJRT 2022) “A Research Study on Cyber Security Issues Affecting Online Banking and Online Transactions in India”

The study focuses on various aspects of digital security, such as data breaches, fraud, phishing attacks, and malware infections. The study also investigated the current preventative measures taken by banks and other financial organizations to safeguard client information and transactions. Through surveys and data analysis, the research study revealed the growing importance of improving the cyber security infrastructure and user awareness of the need to lower risks. Overall, the study provided insightful information about the cyber security environment of online banking and transactions in India and highlighted the need for proactive measures to maintain secure digital financial services.


The study's goal was to find out how the biggest weaknesses and dangers to the banking sector affect internet transactions. The study highlights several typical assaults that banks encounter, including phishing, malware, and identity theft. The study also looks into the strategies used by cybercriminals to exploit flaws in web-based financial frameworks.

Dr. Kamal Mohan Bansal - (IJogeti –online 2020) “Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis”

The study shows the challenges faced by online financial platforms and any potential risks associated with them. Various factors affecting the security of online banking transactions were examined in the paper. The study focused on the importance
of these cyber security concerns and their possible effects on people, financial institutions, and the economy as a whole. This study examined the methods and preventative calculations that can be used to lessen these network security risks.

4. Data analysis and interpretation

**TABLE 01**
Displaying the findings of the respondents' rates of seeking help or making a complaint after becoming the victim of fraud

<table>
<thead>
<tr>
<th>Have you ever sought assistance or filed a complaint about the fraud to which you fell victim?</th>
</tr>
</thead>
<tbody>
<tr>
<td>36 responses</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

**INTERPRETATION**
According to the responses gathered, 75% of the respondents didn’t ask for help or report the scam they were the victim of. Since the problem is better handled internally and does not warrant the effort and money of involving law enforcement. On the other hand, just 25% of the respondents went outside to look for assistance and filed a complaint.

**TABLE 02**
Respondents sharing their opinions on the security of online transactions and banking

<table>
<thead>
<tr>
<th>do you think that online banking and online transactions are safe and secure enough for widespread use?</th>
</tr>
</thead>
<tbody>
<tr>
<td>36 responses</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

**INTERPRETATION**
According to the replies gathered, 77.8% of the respondents concur that internet transactions are secure enough to be used widely. It is wise to use anti-virus software or a full-featured internet security solution to safeguard the system. 22.2% of respondents, however, disagree that internet transactions are secure.

**TABLE 03**
Seeking data from respondents about the resources they use in order to remain updated on current cyber security threats and the best techniques to secure their online accounts

<table>
<thead>
<tr>
<th>How do you stay informed about the latest cyber security threats and best practices for protecting your online accounts?</th>
</tr>
</thead>
<tbody>
<tr>
<td>36 responses</td>
</tr>
<tr>
<td>Getting updated by recent news</td>
</tr>
<tr>
<td>Vlogs and blogs</td>
</tr>
<tr>
<td>Social media</td>
</tr>
<tr>
<td>Own experience</td>
</tr>
</tbody>
</table>
**INTERPRETATION**

According to the replies gathered, 50% of the population of respondents, or half of the population, keeps up with the most recent cyber security concerns via social media, while 27.8% of respondents keep themselves informed by reading the daily news. While a small majority of respondents are well informed by their own experiences, 16.7% of the population is aware of the best practises for protecting online accounts through blogs and vlogs.

**TABLE 4**

<table>
<thead>
<tr>
<th>Obtaining respondents' feedback regarding the security of their personal data stored by banks or other financial institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>do you think your bank or financial institutions provide adequate security measures to protect your online transaction or personal information?</td>
</tr>
<tr>
<td>36 responses</td>
</tr>
</tbody>
</table>

- **50%** strongly agree
- **22.2%** agree
- **13.9%** neutral
- **13.9%** disagree
- **1.1%** strongly disagree

**INTERPRETATION**

According to the responses gathered, 50% of the respondents are undecided about whether banks or financial institutions offer adequate security measures to protect online transactions or personal information, while 22.2% of the respondents concur. However, 13.9% of the respondents firmly concur and accept this idea. Only a small portion of respondents, 8.3% and 5.6%, totally believe that banks and other institutions are responsible for protecting their online transactions and personal data. 13.9% of the respondents, however, strongly concur and back this idea. While only 8.3% and 5.6% of respondents, respectively, absolutely believe that banks or other institutions are responsible for protecting their online transactions or personal information.

**TABLE 05**

<table>
<thead>
<tr>
<th>Finding out the respondents' opinions on the safety of the widespread use of online transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>do you think that online banking and online transactions are safe and secure enough for widespread use?</td>
</tr>
<tr>
<td>36 responses</td>
</tr>
</tbody>
</table>

- **77.8%** Yes
- **22.2%** No

**INTERPRETATION**

As per the responses collected 77.8% of the respondents agree on the opinion that online banking and transactions are safe and secure enough for widespread use. On the other hand 22.2% of the respondents disagree on this.

**TABLE 06**

Inquiring the respondents if they use additional security measures before transacting online
Do you use any additional security measures, such as two-factor authentication or password managers? 
36 responses

- Yes: 19.4%
- No: 66.7%
- Maybe: 13.9%

INTERPRETATION
According to the replies gathered, 66.7% of the respondents employ additional security measures like password managers or two factor authentication. In contrast, 19.4% of respondents and 13.9% of respondents each hold a position that is mutually acceptable.

TABLE 07
Asking the respondents if they have faced any cyber security issues while using online banking or online transaction

<table>
<thead>
<tr>
<th>Have you experienced any cyber security issues while using online banking or making online transaction?</th>
<th>36 responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>47.2%</td>
</tr>
<tr>
<td>No</td>
<td>30.6%</td>
</tr>
<tr>
<td>Maybe</td>
<td>22.2%</td>
</tr>
</tbody>
</table>

INTERPRETATION
As per the responses collected 47.2% of the respondents did not experience any cyber security issues. Meanwhile 30.6% of the respondents experienced cyber security issues while using online banking or making transactions, followed by 22.2% of the respondents stand on neutral grounds.

5. Findings and Suggestions
Computers and other electronic systems are protected against harmful assaults using cyber security. The safeguarding of the client valuables is the key justification for having cyber security in electronic banking. Highly sensitive information will be protected after robust cyber security has been installed for digital banking. If it is discovered, a number of problems, including fraud, are possible. It has been discovered that many people do not seek help for scams they are victims of, which encourages scammers. As a result, it is advised to all victims to seek help and file a complaint in order to raise awareness, decrease fraudulent activities, and make online banking much safer.

6. Conclusion
One of the most crucial elements of the rapidly expanding digital world is cyber security. This study investigates the relationship between modern computer techniques and cyber security issues in the online banking sector. Cyber security is an issue for all businesses. Digital safety cannot be breached if you operate in the sector of digital banking. People are not accurate about cyber security; thus, many organizations are spending money on educational events to raise awareness. For companies that hold a lot of personal data and transaction lists, it is critical for banks to have the appropriate cyber security strategies and procedures in place.
7. REFERENCE
1. Dr. S. Nagaraju – (IJIRT 2022) “A Research Study on Cyber Security Issues Affecting Online Banking and Online Transactions in India”