# IMPACTS OF CYBER CRIME ON INTERNET BANKING: A STUDY

Ashish Sharma  
Research Scholar Department of Law Maharshi Dayanand University Rohtak  
ashish09bhardwaj@gmail.com

**ABSTRACT**

Internet banking, often called e-banking, is a service that make use of information and communication technology. Due to flexibility and convenience internet banking is growing more and more popular. Computer criminals attempts to obtain unauthorized access to the data of various sectors including financial and commercial sectors in order to engage in criminal activity. As a consequence, while using Internet banking and related services, users are always concerned for their security. Here security doesn’t mean physical security of the person rather it means security of financial information. The goal of this study is to determine which sectors are most vulnerable to cyber-attacks and to assure the development and modification of cyber security protocol.

**Key words**- Cyber crime, E-Banking, Financial Fraud, Internet, Technology

---

**INTRODUCTION**

The biggest issue that financial institutions face these days is the alarming increase in cybercrimes, and protecting online financial transactions is now become more important than ever before.

Cybercrime thus, become one of the most challenging problems of global e-banking sector. Global Findex database 2017\(^1\) indicates that since 2011, about 1.2 billion individuals have had bank accounts. According to research, the majority of Indians are migrating to a digital approach, with 51% of them choosing online banking channels, while 26% also utilize mobile banking services to access services. Cyber hazards have grown to be a significant topic of worry as a

---

result of the remarkable expansion of digitalization in banks. According to Gulshan Rai’s statement\(^2\), just 22% of cyber attacks that occurred in India targeted the banking industry. In the twenty-first century, cybercrime has become one of the deadliest retaliation tools anybody can employ to threaten or defraud someone.

Although it is true that computers have become a need for life, they have also created an atmosphere that encourages cybercrime. Given the rapidly changing environment and the considerable contribution of the IT industry, cybercrimes present a serious concern. In order to access computers and commit crimes, cybercrime is often carried out by offenders with technological expertise who can outwit and plan ahead of the law.

Majorly the systems and software used by banks have built-in weaknesses, and there are numerous internet entry points and out-of-date protection mechanisms that are extremely susceptible to sophisticated attack advancements by hackers. However, the most fundamental goal of financial institutions is to be required to be prepared for cyber security. A significant number of regulatory procedures and cyber security technologies have been developed over the years in response to the growing risks to the cyber infrastructure in its regulated businesses. As a result, there is a need to continuously assess the state of cyber security and new threats in light of the complexity and growing frequency of cyber security incidents. Monitoring of bankers’ progress in enhancing cyber security resilience and responsiveness is necessary.

It is necessary to take a comprehensive strategy in the battle against computer fraudsters and cyber terrorists by creating effective legislation and a sound legal framework to safeguard online financial transactions and other activities.

**REVIEW OF LITERATURE**

1. **CYBER-CRIMES: A Growing Threat to Indian Banking Sector**\(^3\) by Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru, (2018), they identified how to stop fraudulent operations and be able to take remedial action, it is necessary to discover, investigate, and evaluate the flaws in the Indian banking industry. This will improve the sector’s security measures.

   This Article was proved to be very much helpful for the understanding of various provisions related to the cyber space and the computers. It also helps to understand various provisions related to the I.T Act and also the punishments were described under this briefly with the help of various case laws.


---


\(^3\) International Journal of Engineering Technology Science and Research IJETSR www.ijetsr.comISSN 2394 – 3386 Volume 5, Issue 1 January 2018

\(^4\) Nappinai N.S., “Cybercrime Law in India has kept law pace with emerging trends? Anempirical Study” ,5, 2-6

Available online at: [https://jazindia.com](https://jazindia.com)
The above stated paper helps to understand the various concerns which are related to the online privacy and the personal data collection. It further tells about the various instances how the online privacy can be in threat. The paper played a major role in understanding the basic concept of the online privacy and the personal data protection. It also further helps to understand the ways that how can curb the cases of the violation of the online privacy and the personal data protection.

**CYBERCRIME**

Cybercrime is a term to direct towards crimes that are associated with cyberspace. As the Internet becomes an inseparable part of society, it has impacted culture and social structure in both positive and negative ways. The opportunities that the Internet provides across the world has made life easier. However, the disadvantage of easy access to every information has also placed privacy at risk. The technological advancement allows malicious organizations to have claws over much of the personal information of an individual through cyberspace. Such information can be misused and may give opportunity to criminals to harm the person in cyberspace as well as real space.

"Cybercrime", as mentioned in *Cyber Crime- Law and Practice*, "is a technology based crime committed by the technocrats." ²

**HOW CYBER CRIMES OPERATION WORKS**

The increasing use of card transactions and online bank accounts increases the potential of criminals to commit more and more cyber crimes. If you gain access to this financial information, you may steal not just covertly but also, possibly infinitely frequently, using an automated procedure driven by a virus. A number of techniques may be used to access credit card and bank account information, each requiring a different ratio of risk, cost, and expertise. Purchasing the "finished product" is the easiest option. We'll use an online bank account as an example in this situation. The product is information needed to obtain permission to access a bank account with a six-figure amount. This information may be obtained for a few dollars or few crypto currencies. Although it may seem like a little sum, the criminal who can offer it finds it to be extremely simple money given the labour and danger required. Additionally, keep in mind that this is a worldwide trade, and many cybercriminals of this caliber originate from developing nations in South America, Southeast Asia, or Eastern Europe. This transaction's likely marketplace will be a secret IRC (Internet Relay Chat) chatroom. The charge will probably be converted into e-gold or crypto currency or another type of virtual money. Different

---

participants in the criminal underworld carry out a variety of significant, specialized tasks. Not all cybercriminals operate at the front lines, and they certainly don't work solely for one another.

Therefore, why do banks are such a profitable target for cybercrime? The solution is straightforward: cybercriminals follow the money, and banks have more money than most other businesses. While bank systems and their clients are subject to a variety of dangers, one of the largest hazards and sometimes one of the toughest to spot is that posed by users who are dishonest, negligent, or compromised. These staff members, independent contractors, and partners are already inside the bank's security perimeter and are entitled to use its IT systems and sensitive data. Aside from that, phishing is frequently used to take over bank accounts. Other cybercrime methods also exist, but space does not provide a complete discussion of them.

**CYBER THREAT IN OTHER FINANCIAL SECTORS**

The advancement of any country relies on the monetary development, which thus is subject to the monetary area. The business analysts and policymakers to a great extent concur that monetary improvement contributes towards monetary establishments and markets, similar to venture and business banks, stock and security trades which thus lead to financial development. Furthermore, the monetary area assumes a vital part for society overall, serving organizations, states, families, people and metro foundations. The area carries out basic roles like empowering speculation and saving, giving insurance from takes a chance as well as supporting the making of new undertakings and occupations. To give these capabilities, it becomes fundamental that the area works in the general public in a steady and maintainable manner. Be that as it may, the encounters of ongoing many years have uncovered a scope of weaknesses in the monetary area. Digital dangers looked by the monetary area are like those looked by other basic framework areas i.e, assaults from gatherings or people with vindictive goal, similar to the fear outfits, wrongdoings, organizations and unfamiliar insight offices. In any case, the potential for financial additions alongside the monetary disturbances expands its engaging quality as an objective (Jan 2003). Likewise, the area has been an essential objective of digital goes after internationally principally because of the enormous worth of the data accessible. Albeit, the harm brought about by digital assault in this area could go from monetary misfortune, business interference, loss of notoriety and even obliteration of actual foundation through hacking of brilliant machines. All the more explicitly, the episodes connected with network protection can undermine monetary security through three channels i.e, disturbing the tasks of a monetary firm that offers basic types of assistance, harming the honesty of key information and decreasing trust in firms and markets. Plus, the digital assaults have broad monetary outcomes past the monetary, legitimate and reputational consequences for a singular firm.

Somewhat recently, the Indian monetary administrations area saw an outstanding development. Be that as it may, such a thrived development has not been without entanglements as the
Occurrences connected with extortion have likewise improved. It is assessed that the monetary misrepresentation offers more than $20 billion in direct misfortunes yearly. Albeit, the specialists suspect that the authentic figure is a lot higher as firms can't precisely quantify as well as recognize misfortunes because of misrepresentation. Moreover, most of banks in India offer both portable and web based financial administrations, and the majority of the exchanges are led through credit and charge cards, alongside electronic channels like ATMs. The reliance on web-based networks has made the monetary organizations in India progressively defenseless against complex digital assaults.

Consequently, a change in outlook has as of late been seen in assaults taking advantage of the thought processes, conduct, source and vectors. This uncovers that the traditional safeguard techniques utilized in the monetary area including the banks isn't satisfactory, bringing about serious monetary misfortunes. Hence, there exists a should really try to understand the inborn requirement for the monetary area banks to reinforce their stance connected with network safety directly following progressively modern quantum and nature of assaults. To summarize, the basic frameworks in India since 1990s like atomic offices, power lattices, safeguard organizations, monetary establishments and legislative informatics have been coordinated with PC and online organizations. This has improved on the errand of overseeing significant exercises speedily and from a distance. In any case, this rising computerization and digitalisation has additionally made them defenseless against malevolent demonstrations. Accordingly, it becomes fundamental for India to take on strategies and form organizations to safeguard the basic frameworks from the risks of digital assaults.

**TYPES OF INTERNET BANKING CRIMES**

**Identity Theft:** It is a kind of crime that has been committed by Cyber criminals by using someone else's identity/particulars, that includes their name, address, birth date, for fraudulent and illegal operations. By using such identity particulars, cyber criminals open new bank accounts, apply for loans, credit cards or for government benefits.

**Phishing:** In this kind of crime, cyber criminals contact the victims usually via email, text messages, or website links and pretends to be a genuine/trustworthy source in order to trick the victim and obtain sensitive information such as login id, password, bank account or credit/debit cards details, OTPs etc. In phishing attacks, attackers usually send an email or text posing to be a email or text from bank and asking to click on the given link.

**Vishing** : Vishing attack is similar to phishing attacks with a material difference that vishing attack is committed through the use of voice phishing. In this kind of scam, attacker usually contact a victim over the call and pretends to be a official of bank or company. Different kind of baiting techniques are used by the attackers such as creating fear, gaining of trust, curiosity or anxiety in order to convince a victim to share sensitive information.
Social engineering is the practice of manipulating others to carry out tasks or reveal private information. Computer fraudsters and cyber thieves frequently employ social engineering to get financial data and obtain illegal access to sensitive information.

Social networks: These days, people use various kinds of social networking sites such as Facebook, what’s app, twitter, snapchat, messenger, line, Telegram etc. Their whole life revolves around such social sites and has become a symbol of status show off. Although such sites and apps help people in connecting with each other but the criminals have find the techniques to misuse them too as a result Identity theft, defamation, hate speech, fake love scenarios, nudity and pornography become common.

Denial of service (DoS): DoS are attempts by online scammers to prevent users from accessing network resources. Because of the seriousness of these attacks, discrete distributed denial-of-service (DDoS) attacks may soon bring down not just a single website but also any intermediary service providers.

Mobile Phones and Electronic Devices: In today's digital era, using mobile phones and other electronic devices like computer tablets is becoming standard behavior. Security professionals foresee significant dangers from computer fraudsters and cybercriminals on the platforms for smartphones and tablets that are now accessible.

PREVENTIVE MEASURES TO CONTROL FRAUDS

Technology is evolving at a faster rate and so also the cyber crimes. Attackers have improved their ability to identify and collect vulnerabilities and exploiting security flaws to successfully take advantage of positions of power and disrupt the network. Nowadays, Banks are investing in the cyber-security technologies in order to defend their system from unwanted security breaches. The banking system may be secured against unwanted attacks with proper firewall setup and maintenance. There is a test to evaluate the network and infrastructure security of banks. It is required to take specific precautions, such as using the secret socket layer (SSL) protocol, to stop cyberattacks on banks' backend online programmes.

Any time a browser requests access to a site's data, it first obtains the SSL certificate, verifies that it is valid, was issued by a certified authority recognized by the browser, and is being used by the website for which it was issued. If all of these requirements are satisfied, the browser is then given access. Ineffective password management might make it simpler for attackers to access the server and network layers. Passwords need to be handled, kept secure, updated on a regular basis, properly secured, and encrypted. Using password encryption firewall settings must be used to protect networks. To secure the system core, many tiered protection frameworks should be offered. Firewalls and traffic content filters at the top network layer are required to stop the transmission of undefined and unauthorized data. Antivirus software should be used to direct the platform layer underneath. Old gear and software should be replaced with the most recent ones that have stronger security updates, and operating systems and other software should
be patched and upgraded on a regular basis. The backbone of back-office IT is the application layer, which has a large number of lines of source code. To secure the source codes, the necessary preventative system must be implemented. Developers must implement password encryption and minimize vulnerabilities connected to their programming.

In addition to the aforementioned, banks should concentrate on teaching staff members through self-awareness programmes, offering training on data protection regulations, and arming them with information on cyber security so that they are constantly on the lookout for any type of external intrusion. Extra caution should be exercised by users of internet banking who do daily transactions online. More than 60% of consumers are reported to be uninformed of the underlying information security concerns involved in banking operations and transactions, according to data gathered from studies. Additionally, about 55% of consumers are unable to exercise extra caution when using online banking services\(^6\). A few common preventive measures are outlined below as part of the user awareness programme that all bank workers must adhere to.

- Use strong passwords that are different from one another for network share logins.
- Instead of exposing remote desktops, use a Virtual Private Network (VPN) for all remote work (RDP).
- Working folders shouldn't include shared applications in exe format.
- When necessary, only download from a secure source with IT Security's consent.
- Controlling RDP access and turning it off when not in use.
- Maintaining constant browser updates and blocking add pop-up windows.
- Quickly confirming the legitimacy of the obtained surfing site. and prompt notification of the bank's IT security in the event of any suspicion.
- Always add vital websites to your favourites list to steer clear of scam sites.
- The sharing of personal information on any unidentified websites is prohibited.
- Improving email security to recognise dangerous attachments.

### AI TECHNOLOGY AND FRAUD PREVENTION

---


Available online at: https://jazindia.com
It's safe to say that AI has turned into a very popular buzzword in a number of commercial industries. There is no exception in the financial services sector. AI, which was first developed in the 1950s, has recently experienced a surge in popularity. Owing to a multitude of factors recently. Of course, adopting new security standards is one of them.

Promising technologies are being adopted by the sector as a whole, and many bank institutions have already started down that path. According to a Narrative Science survey, 32% of respondents from banks acknowledged employing AI technologies including speech recognition, predictive analytics, recommendation engines, and response. Once more, fraud detection is one of the most significant applications of artificial intelligence in the banking industry. Some banks are starting to use AI to combat cybercrime and deal with difficult problems in real time. The monitoring process has been considerably enhanced by AI over the past 10 years; it can now learn in a quick-paced environment and react to fraudsters' strategies as they emerge. Consider bank accounts. Certain usage habits can be recognized when an account's behavior is being watched. In this manner, any indication of unusual behavior is highlighted for evaluation. Therefore, the detection system may assess transactions in 0.3 seconds when a consumer attempts to make a purchase using a debit or credit card, identifying fraud or authorizing non-fraudulent transactions.

Such algorithms receive supervised training to identify probable fraud when a range of random samples are manually identified as authentic or fraudulent. The programme then gains knowledge from these manual classifications to independently assess the authenticity of upcoming actions. In a few years, the strategic use of artificial intelligence (AI) and machine learning will be a fundamental component of financial companies' security principles. AI can help banks save a lot of money by removing complicated fraud instances and defending their reputation.

FINDINGS AND SUGGESTIONS

Findings

- The reason why banks are always attacked is because they have all of the reserves in cash.
- Most of the time, fraud detection software is either old or takes a long time to utilize.
- Due to how simple it is to hack a customer's personal information, there is a significant danger to their security.
• There is no explicit law that addresses these crimes, particularly those involving the banking industry.

Suggestions

• Foremost necessary thing is to create awareness among the end users i.e. customers as well as the bank staff.

• Internet banking customers have to create secure passwords and unique user names for each of their accounts and websites.

• To keep track of such offences, law enforcement should be particularly strict and updated often.

• Fast track mobile courts should be available to settle these disputes, address public complaints, and foster public trust.

• Instead of only sending these situations to the banks, the public should report them to the Cyber Crime Branch in order to ensure swift and rigorous action.

CONCLUSION

Cyber crimes are endless and increase with the increasing Technology nowadays. The exponential growth of Cyber crime is dangerous and a big threat to banking sector and Financial Institutions. The dependence of the entire finance sector on technology depends on strict and strong security system. And making and maintaining a very dependent and reliable security protocol. Apart from these challenge Indian banks need to fight against the attitudinal mind set of the staff as well as the psychological mindset of the staff there is also need to review the infrastructure including software as well as hardware. Banks are the core backbone and leading Institution of any country and if there is any threat on them then no democracy or dictatorship can stand now time has come to secure the financial institutes as much as possible.

REFERENCES

1. http://www.cyberlawsindia.net/


6. www.conferenceworld.in

7. www.thehindubusinessline.com
