IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER CRIMES IN E-BANKING

RAMYA GAYATHRI BS

REVA UNIVERSITY BENGALURU(LLM STUDENT)

INTRODUCTION

In the modern world, privacy is the most important aspect, and everyone must take great care to protect it. With only one click on the Internet, we may send files and documents, as well as conduct online banking transactions swiftly and effectively.

Everyone is currently aware of how online transactions and banking work when using mobile applications and banking websites, but securing these transactions and our money is crucial. Cybercriminals or hackers occasionally utilize online transactions for their own gain. They can easily deceive victims and steal their money, and victims often suffer as a result. Most importantly, sometimes victims are unaware of how to manage problems due to a lack of cyber awareness.

Without cyber security, your data or money will be stolen in a matter of seconds without our knowledge. Because the banking industry is more valuable and cybercrime is rising there, it is really important. In today's technologically advanced and digitally connected society, security is currently the biggest issue. The majority of daily tasks, including shopping, office work, e-banking, and other activities, may be completed with the aid of the Internet. Everyone is familiar with mobile banking and online shopping, but many people are unaware of the security measures required while conducting any type of online business. Because of this lack of information about cyber security and hackers, cybercriminals profit from this situation. And the number of cybercrime incidents in the banking sector is rising rapidly every day. Because of their ignorance of security, victims of hackers or cybercriminals may occasionally fall for their deceit and not even recognize it until they receive notification from their bank that their account has been compromised.

World is a developing and advancing in its digitization. Securing online data or transactions during this time will become increasingly difficult. E-banking speeds up and simplifies labor, but it is not secure and never will be. And cybercrime is growing more quickly than we anticipate.

CYBER CRIMES THAT ARE RELATED TO E-BANKING

HACKING

An attempt to get around the security of a customer's banking site or account is known as hacking, which is illegal. The modified IT Act of 2000 does not define the crime of hacking. However, a hacker may be penalized under section 43(a) read with section 66 of the Information Technology (Amendment) Act, 2008 and under sections 379 & 406 of the Indian Penal Code, 1860.

A hack targeted Canara Bank's ATM servers in 2018. Twenty lakh rupees were cleared across several bank accounts. According to sources, fraudsters' access to more than 300 people's ATM information resulted in 50 victims overall. The personal information of debit cardholders was obtained by hackers using equipment known as skimmers. The number of transactions involving data that was stolen

SPYWARE

Spyware is the most used technique for collecting passwords for online banking. It is installed through phony "pop up" advertising that ask users to download software. Antivirus programs recognise and eliminate this type of software, usually by blocking its download and installation before it can infect the computer

VIRUS

An executable file can become corrupted by a virus, which makes it act weirdly as a result. It multiplies by embedding itself in executable files, including those used by operating systems and application applications. Running the executable file has the potential to transmit the infection. Worms, on the other hand, are software applications that have the ability to duplicate themselves; they don't alter or delete any files, instead choosing to expand and disseminate copies of themselves from the victim's computer to other computers.

COMPUTER CREDIT FRAUD

Online credit card fraud happens when a customer uses their credit card or debit card for any type of online payment and another person, with malicious intentions, uses such card details and password by hacking and misusing it for online purchases using the customers' hacked card details. It can also happen when a person commits fraud. Insecure electronic transactions give hackers the opportunity to misuse credit cards by impersonating cardholders.

DNS CACHE POISONING

In order to improve resolution response performance, DNS servers are installed on a company's network and used to cache previously received query results. DNS server poisoning attacks are started by taking advantage of a flaw in the DNS software. As a result, the server incorrectly confirms that DNS responses are coming from trustworthy sources. When a user submits the same request again, the server will eventually cache the incorrect items locally and serve them to the succeeding users. To deceive bank customers into providing their login credentials to a false version of a real website, an attacker may use a server controlled by criminals to send malware to victims of a banking website. Using a particular DNS server to forge an IP address and DNS entries

KEYLOGGING, OR KEYSTROKE LOGGING

Scammers utilise a method called key logging to record actual keystrokes and mouse clicks. Keyloggers are "Trojan" software packages that target the operating system and are "installed" through the use of a virus. These could be particularly dangerous because the con artist captures the user name, password, account number, along with any additional characters entered.

PHARMING

Farming and phishing are related to pharmaceutics. In phishing, an attacker hijacks a bank's URL so that whenever a customer checks in to the bank website, they are directed to another website that is phoney but looks exactly like the real website of the bank.Online pharmacy fraud and ATM skimming are also common.

A bank management trainee and the fiancée exchanged emails across the network of the company's computers. The Bank NSP Case is this. When they eventually split up, the young woman utilised various made-up email accounts, including "Indian bar associations," to send emails to the boy's international clients. She did this on the bank's computer. The boy's business lost a lot of clients, so it filed a lawsuit against the bank. The court decided to hold the bank liable because the emails were sent using the bank's technology.

WHAT ARE CYBERCRIME'S RESULTS

The expansion of financial services to the general people is a result of the growth of mobile networks and the development of information and technology (IT). However, technological advancement has raised the likelihood of becoming a target of cyberattacks while also improving the accessibility and cost of banking services.

Cybercriminals are now able to spy on companies and gain essential company data in addition to utilising sophisticated methods to steal money, which has an indirect effect on the bank's profitability. Additionally, hacking in the banking industry would violate customer privacy. Anyone, i.e., any hacker, is capable of using another person's identity to threaten them with engaging in criminal action and stealing their money.

NEEDS OF SECURITY IN E-COMMERCE

E-Commerce security is the rule that guarantees secure online transactions. It contains of procedures that protect those who conduct online transactions for the sale and purchase of products and services. And the cost of a breach, in terms of data loss and lost client trust, can be extremely damage for organisations of all sizes.

Owners of e-commerce companies are increasingly implementing security measures since they are acutely aware of these problems.By implementing the security basics of eCommerce security, which can win over the consumers trust such basics include:

a] privacy

The protection of privacy includes prohibiting any actions that could share consumer data with unauthorised parties. No one else should have access to a customer's personal information or account information except from the online seller they have chosen.

When merchants permit others to access such information, there has been a violation of confidentiality. A web-based company should implement the bare minimum of anti-virus, firewall, encryption, and other data protection measures so that Client bank and credit card information will be well-protected

b] Integrity:

It is another key idea in e-commerce security It entails making sure that any data users have shared online is kept untouched. According to the guiding concept, the internet firm uses the clients' information exactly as they provide it, without alteration. The buyer loses faith in the security and reliability of the online business when any portion of the data is altered c] Authentication:

Authentication is nothing but the verification of identity of both buyer and seller Both the buyer and the seller must be genuine according to the authentication concept in eCommerce security. They must be who they purport to be. The company must demonstrate that it is legitimate, deals only with real goods and services, and fulfils its commitments. For the seller to feel confident about the online transactions, the clients should also provide identification documentation. It is feasible to guarantee identification and authentication. Hiring a professional would be quite helpful if you are unable to do so. Client login credentials and payment card PINs are some of the common methods.

d] Non-repudiation:

Repudiation means denial.As the result,the legal principle of non-repudiation tells participants in a transaction not to deny their acts. The buyer and the business should complete the portion of the transaction they started. eCommerce can seem less secure because it takes place online without live video. eCommerce security is further enhanced by non-repudiation. It confirms that the communication that occurred between the two players indeed reached the recipients. Therefore, a party in that particular transaction cannot deny a signature, email, or purchase

CONCLUSION

The backbone of our economy is the financial sector. The growing incidence of cybercrime has had a negative impact on our economy. In order to prevent cyberattacks, it is important to make sure that the relevant laws are properly enforced. It is crucial to alert banks and customers to the risk and the need for safety measures. The many groups involved must coordinate their efforts to combat cybercrime.

The current scenario necessitates greater international cooperation among the nations in order to develop the tools and strategies necessary to effectively combat cyber crime.

Due to a lack of teaching in the subjects pertinent to the study of electronic and cybercrime, developing nations like India that are afflicted offer a serious problem. Furthermore, the banking industry now finds itself in a complex and thought-provoking situation as a result of global macroeconomic and geopolitical events. The banking industry is required to review its current practises in order to improve risk analysis and mitigation. Risk management techniques have been fueled by technology.

As a result, it is possible to regularly monitor banking transactions and activities, even though it may not be possible to totally eradicate cybercrime from the internet. Raising awareness among the populace is the only practical means of reducing crime.