INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD ISSN: 2455-0620 Volume - 7, Issue - 4, Apr – 2021
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value: 86.87 Impact Factor: 6.719
Received Date: 10/04/2021 Acceptance Date: 22/04/2021 Publication Date: 30/04/2021

An Insight Study of Cyber Security in Online Financial Transaction Environment

Deepak Jyoti
Assistant Professor Computer Science & IT
Shanti Devi Arya Mahila College, Dinanagar (Pb.)
Email: erdjyoti346@gmail.com

Abstract: *Online Financial Transaction Environment means online banking or internet banking or web banking or e-banking , in which financial transactions can be performed through the financial institution's website. Now a days, online banking playing an important role to carry out the financial activities execution for one or all. All online banking activities are based on the internet or private networks these days. They all perform these online activities through communication channels. If anyone using credit, debit card, online banking etc. to do financial transactions, then there is some risk of stealing your personal information or money. It means anyone doing online transactions, can be the victim of these threats. These online banking crimes have become very common in India. But as online services from banking are growing, simultaneously cybercrimes also started, which are very difficult to detect and cure. Security of personal data and transactions is very important which are carried over technology. This is not actually the fault of victim people, it is sometime due to not well educated, not trained or unaware about the current and upcoming crime. This paper studies online banking services by using information technology, protocols of Information technology in secure banking and awareness of cyber security by depicting the intensity of cyber-crimes committed in India.*

Key Words: *E-Banking, E-commerce, online, cyber security, IT.*

1. INTRODUCTION:

Information technology have made modern life more convenient. In present scenario, Banking industry is using information technology and communication channels for online banking activities. Twenty-four by seven services are available for bank customer. Customer can access his/her account details at anytime and anywhere. User can do finance management very easily. Money can be transfer immediately to any other beneficiaries as per need. At the time of shopping, there is no need to carry money with you. It can also transfer through any payment apps like PayPal, Google Pay, Paytm etc. Payment can also be done by swiping credit/ debit card. Banks and any other money transfer apps take transfer charges from customer. These charges are very less. Banks provides all these services online without taking any step inside the bank. But it also put your finances in high risk. Banks get hit by cyber attacks every day. The main concerns are related to security because of rapid growth of a technology; Internet banking – suggests that these concerns can be solved by many aspects .However, the threat of digitally stolen money is much more serious as compare to physically stolen. Information technology has a major impact in our life. We cannot think of a life without internet. Banks also started up introducing technological features in banking service to compete globally. A large enough capital pool is contributed by Indian government on technological financial services like Net Banking, E-Banking, E-Commerce to provide the security on financial transactions. Cyber crime is same as the robbers taking the safe away from home but through online. Now banks are becoming more alert at preventing breaches of security. They are implementing strong cutting-edge protocols in software to prevent cyber attacks from being successful. Only the few cyber attacks comes in highlighted news. These days' banks are facing a serious security issue. Every day a new type of hacking style of cyber criminal comes. Mostly banks take backup of database on servers . if these servers get hacked the all database of all customers are also hacked, then any bank customer can be the victim. Now the banks are trying to improve their systems exponentially for detecting and dealing with every latest crime style comes.

Moving into the online or digital market will certainly present multiple challenges. Banks with online facilities are facing stiff competition these days. Most of the competitors don't have the strong security features for keeping consumers and businesses information safe. These different customers are facing many threats every day. Consumers and businesses both are at risk of cyber security threats. Cyber criminals are hacking banks data through bank's insecure network and insecure customer account. These banks must update software tools regularly through which they are serving their multiple customer segments. This software package must be equipped with solutions for network monitoring, threat detection, identity and access management of customer, data security, and other types of defenses mechanisms. All customers have trust on banks. They keep their all sensitive and valuable thing in banks for safety. But banking online services are under high risk. Banks have a large range of security features in software to

manage cyber security solutions. Banks are providing services with security features like advanced authentication or threat monitoring, and charging from customers for providing these services.

So banks are investing a heavy amount for providing cyber security to protect their client's most valuable and sensitive information which is increasing the cost of doing such business in financial transaction services, but it also presents an opportunity for banks to generate a revenue from the invested amount on the cyber security solutions. As the banking industry is growing its more online services, simultaneously banks are also increasingly designing security solutions which can become a source of revenue for them. But cyber security is a major market where banks are in a unique position to deliver solutions. Banks have multiple customer segments like retail consumers, small businesses, and corporate who all are looking for help to protect them from hackers. Cyber security is security domain for banks to provide secure environment in the technology by investing billions of dollars in order to compete in the marketplace. Beside doing all these efforts, this threat is growing more complex and dangerous and banks need to respond to these security challenges with more efficient and effective solutions.

2. Online Banking Security Challenges and Precautions:

Pickpockets can target few people on roadside but internet frauds can target any person any time and anywhere through emails, phone calls, fake messages and fake websites. But you can protect yourself from such frauds by knowing about all types of frauds and their causes.

Phishing is a type of Internet scammers to obtain your personal information. The credential banking information and credit card details of any user are phished through email or instant messaging. Phishing receive communications material from your financial institution or banks. Usually financial institutes asks you to login your online banking account and verify. There are some cyber security issues. The fake email asks you to click on the link and takes you to a cloned website of your online banking site and you'll be asked to enter your credentials. Pharming is another way for hackers to get your personals details. Pharming is a type of online fraud with malicious software and fraudulent websites. Cyber criminals automatically install malicious software on your computer. The code automatically directs you towards fake websites without your knowledge. Pharming scams occurs when hackers install a malicious software on your PC without your knowledge, which redirects you to fake websites automatically even though you type correct URL. This malware hides the fake website URL and showing it in the legal website in browser. Then user asked to enter all online banking or account information, which hackers need to access for making criminal activity. Any bill payments can be quickly and easily done online. Bill Payment fraud occurs when someone gains unauthorized access to your online banking account number and personal access code and initiates fraudulent bill payments. The cybercrimial can access online account details through the installation of a key logger any other malicious software on your computer. The key logger is software which records your keystrokes on keypad and transmits that information to a fraudster. Similarly Interac e-Transfer is a financial transaction service offered by Canadian banks and other financial institutions, offered through Interac Corporation. There are numerous benefits for using this e-Transfer. When you have email and online banking access then you can send and receive Interac e-Transfers. However, if your computer is hacked then your email account and your banking credentials may be at risk. Online transactions frauds occurs when someone steals all your online banking login credentials and gains unauthorized access to your bank account. Once fraudster logged in your account sends online financial transactions from your bank account to another bank account or elsewhere. He can also change your settings also. If this happens to you, then report it to the bank to block your transactions. These emails may consists with following content:

- User can get warning messages about account closures from bank side and ask you to provide your all banking details immediately.
- Prize announced for you as special customer and ask for account details to send you amount
- Offers to register for a new eye catching services with bonanza gifts.
- They can offers pre-approved credit cards
- They can offer free antivirus programs,
- Mails for insurance company to ask your details.

Banks or financial institutes always alerts their customers by sending messages like "Bank will never ask your personal information and verify your banking details".

3. Precautions :

- Never give your any personal details in any email.
- Online messaging is not at all a secure communication. All messages gets stored on centralized server and if server gets hacked then every information given in messages will available to hacker.
- Any message or URL link received through unknown then don't open that message and respond.

- Any emails or any email with attachments received from any unknown sources should not open without scanning with reliable anti-virus software.
- The best way to protect yourself is to never use a link provided in an email to access your online banking because banks don't send those, all these scammers do.
- It will be more secure to type your financial institutional website link address directly into your browser and look for confirmation that you're browsing securely.
- The letter "s" in 'https' means you are browsing secure site. Any link with 'http' are unprotected URLs. Always look for the 'https' when using ecommerce sites.
- If you have any complaint about emails or other communication related to your online banking then call or visit your local branch immediately. you should complaint within twenty four hours.
- It is important to check your all types of accounts regularly. Account can be of credit card or a savings type, checking your regularly can alert about suspicious transaction
- If your bank offers mobile app then definitely use it because it is strongly more secure. Always download the app from your official website of bank. It should not download from play store because some play stores may have been hacked by hackers and they can upload fake apps that look nearly identical to the real ones.

Never use weak password because it move your online bank account extra vulnerable. Once a hacker get your password or crack your password, they will have full authorization to make any changes to your account. Password must be very strong, it must consists of alphabets, digits and special characters. A strong password for a banking account, an email or a social media account can avoid cracking of password. Use strong password which is not easy to guess. It must consists of combination of capital letters, numbers and special symbol which make it even more stronger.

Banks are providing next level of strong security level other than usernames and passwords. Biometrics verifications like fingerprint scans, face recognition, multi-biometric verification and other more secure techniques are used to identify their customers. In the near future, banks might even trying to use multiple biometrics measures like iris scans, facial recognition or voice prints. Most of people don't have any kind of password security features on their mobile devices. You must download banking app and use fingerprint or something like that biometric features to login. Use smartphone password or fingerprint for unlocking. Never share information to social sites which can be used to guess your passwords easily. Set alert notification for any bank account updation to avoid any fraud activity. People who are very active on social sites can be hacked very easily. Never sign-in online banking site on any public Wi-Fi. Bank transactions should always be done over a private network. Always sign out after the completion of your transactions, even if you are using your PC or own mobile device. If your bank provide security services of multi-factor authentication then utilize it, it can protect your finances. Because an account having two or multi factor authentication is much more difficult to hack. Hacker requires both account as well as the user's smartphone for hacking.

4. Protect your bank cards from fraud:

One of the most common ways is a scammer which will try to get access to your bank account at ATM machine. Fraudster install 'skimmer 'on the card reader at ATM machine. When you place card in the machine then skimmer captures data from your card and then by that scammed data is used to create a duplicate card. That duplicated card can be used to access your account. These Skimmers are difficult to detect. So when you place your card in the machine then you firstly need to actively check the machine properly for skimmer. Always check the ATM carefully for anything that looks different coloured plastic around the card reader slot etc. If you notice anything suspicious, immediately report to the concerned financial institution and use another machine. Card-related scams can also occur at shopping malls or restaurants other than ATM. Never give your card to swipe through any unknown person. Waiter or store attendant to whom you give your card to pay the bill and they may run it through a skimmer to get your card information details..

What happens if your bank account is hacked? Are you liable or is your bank? Data breaches are becoming increasingly frequently. If any loss occurs is on bank side then this fault is neither on the bank side nor with the customer side but it lies elsewhere in the system. The customer must report bank within twenty four hours about any fraudulent occurs from any unauthorized transaction. Bank will block your card for further transactions immediately for safety purpose. If you notice your ATM has scammed and transactions are going on ,then report to institute and contact the police. If any unknown transaction is noticed beyond seven working days, then the customer liability shall be final by the bank's Board-approved policy. The bank is required to credit the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of notification by the customer. Banks have made compulsory to link customers account to mobile number to register for SMS notification for any

transactions to make secure transactions. The banks are actually responsible for stolen funds as a result of cyber crime. This is all thanks to the guidelines established by the Federal Reserve to protect electronic funds transfers (ETFs).

5. CONCLUSION:

There is a need to set new regulations for online transactions to satisfy the customer and ensure security. Banking institutes must focus on managing the existing risks of recovery by following the international regulations to compete in the global market. In today's world of WiFi hotspots provided at coffee-cafe shop , then hackers can gain access to our accounts very easily. Browsing the web is fine, but don't enter personal information like your bank account login or even email password while on a publicly-accessed connection. These financial institutions should aware the customers about chances of frauds. News of previous cyber attacks and the threat of future ones is very scary. Often times, these institutions must have their advanced cyber security regulations to solve the problems of these threats. Those who are having feeling of data breaches considering a reason for not doing online transactions are over-reacting. There is fear in financial transactions because of hacking. But if your bank account is hacked, you shouldn't be scared to bank with online transactions because banking institutions has given multiple security verification steps while online transactions.

REFERENCES:

1. https://www.idc.com/getdoc.jsp?containerId=prUS43165817
2. https://www.reuters.com/article/us-usa-banks-technology-commercial-idUSKCN0WH232
3. https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#17c63152116d
4. https://home.kpmg.com/xx/en/home/insights/2018/02/reaping-the-security-advantage-talking-to-bank-ceos.html
5. https://www.bloombergquint.com/onweb/2018/05/07/goldman-sells-in-house-cyber security-software-to-tech-company#gs.ccXeFFA
6. https://www.capgemini.com/wp-content/uploads/2017/07/the_currency_of_trust_why_banks_and_insurers_must_make_customer_data_safer_and_more_secure.pdf
7. https://economictimes.indiatimes.com/news/et-explains/how-much-is-the-bank-liable-if-your-account-gets-hacked-heres-what-rbi-says/articleshow/65591511.cms