SECURITY AND PRIVACY ISSUE IN INTERNET BANKING

Dr.M.Parameshwari,
Asst.Professor of Commerce,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam.

Abstract: Banking is the Lifeblood of Financial system. Liberalization in Indian Banking since 1992, Increased global competition more private and foreign players have entered the Indian banking sector. At that time Information Technology (IT) has become an essential part to development of banking system. It helps to fulfill the Organisations and Customers requirements in an efficient manner to providing nonstop banking services. The nonstop services like ATMs, Internet Banking and Mobile Banking are helping the banks to reduce their customer service costs and their valuable time. The customers are no need to go to bank to pay any bills, check their account details and make fund transfer. The bank provides more online financial services to their customers. Customers can access their banking accounts from anywhere in the world. In India, ICICI bank was the first bank to offer online banking in 1996.at present majority of commercial banks are offering internet banking service to their customers. The rapid development of Information Technology (IT) in banking sector at the same time major issues accrue to Internet Security thefts, frauds, transactions etc. This paper presents security and privacy issues related to Internet banking. Various types of cyber attacks, fraud strategies, and prevention methods used by Internet banks, are also presented in this paper. This study discusses the security and privacy issue in Internet Banking.

Keywords: Internet banking, Information Technology (IT), Banking Services, Cyber attacks.

Introduction:

Finance is the life blood of trade, commerce and industry. Now-a-days, banking sector acts as the backbone of all business activities. Most of the countries developments are mainly depend upon the banking system. A bank is a financial institution which deals with deposits and advances and other related services. It receives money from those who want to save in the form of deposits and it lends money to those who need it. Banks act as bridge between the people who save and people who want to borrow that is, it receives money from those people who want to save as deposits and it lends money to those who want to borrow it. After the liberalization lot of the changes comes into the banking sector. Development of the Information Technology (IT) majority of the banks are used this facilities and to service their customers. This technology is greater helps to the customer and save their valuable time. Banks are introduced Internet banking, Mobile banking facilities to their customers. This facilities are very useful to the customer can access their account in our places. The customers can pay their all kind of bills, send or transfer money to various kind of multiple accounts, make deposits, withdrawals or payment with online checks, view history of transaction on their ongoing accounts, trade links and securities and all these activities can be done easily with just the click of the mouse and in the any where all over the world. But at the same time various problems also occur. Most of the customers are not known about the privacy policies even educated customers also not maintain their ATM Pin, Internet banking password themselves only. This is one type of customer related issues. Another side Internet banking a common target for hackers and other online criminals. however, Understanding the security issues relating to Internet banking can help to keep both the personal and business accounts safe from intruders.

Objectives:

- To evaluate the different types of security issues in banking sector.
- To assess the solution of the problems.

- **Different types of security issues in banking sector:**

Internet banking:

The Internet banking accounts are protected to the password of customers. Banks are insisting their customer to create strong password. The password should contain mixed – case letters, numbers, and symbols. But the customers are giving up the information voluntarily to the hacker in the way of receiving e –mail or call, presenting to be a representative of the bank .The hacker access to account information by using various technologies.

- **Phishing Attack:** Phishing is an attempt by fraudster to fish for banking details of customers. Phishing Attack usually is in the form of an e-mail that appears to be from customer banks. The e-mail usually encourages customer to click a link in it that takes him to a fraudulent log-on page designed to capture authentication details such as password and login ID, E-mail addresses can be obtained from publicity available sources or through randomly generated lists.
- **Keyloggers:** Keyloggers are malware programs that record keystrokes and other data, allowing a hacker to capture the password to the customer enter it. Many keyloggers and viruses use email to travel from computer to computer.
- **Spoofing:** Website spoofing is the act of creating a website, as a hoax, with the intention of performing fraudulent activities. To make spoof sites seem legitimate, phishers use the names, logos, graphics and even code of the actual website. The fake URL that appears in the address field at the top of the browser window and the padlock icon that appears at the bottom right corner.
- **Vishing:** It is a combination of Voice and Phishing that uses voice over Internet Protocol technology(VoIP)where in fraudsters feigning to represent real companies such as banks attempt to trick unsuspecting customers into providing their personal and financial details over the phone.

- **Solution of the Security Issues**

- The bank may offers two-factor authentication, adopting the technology is a great way to keep the customer's account information safe. Two-factor authentication requires a second code when logging into the account, either provided by an electronic token, or message sent to a registered Mobile phone or e-mail id. The extra layer of security renders the password useless to a hacker without the accompanying code.
- The customers must check their account balance often and make sure every transaction in their record is authorized. If unauthorized activity occur in to the account immediately report to the bank.
- Maintaining up-to-date antivirus suites on the computers can prevent these malicious programs from gaining a foothold, and setting up the work's firewall to monitor outgoing traffic can help to determine when an unexpected occurs. So adding anti-virus protection to the computer email server can help filter out these attacks.
- SWIFT(society for worldwide interbank financial telecommunication) since radical attack that occurred on 11th of September 2011.The main responsible of SWIFT is electronic fraud specially target for online banking.

Conclusion:

The Customers are using Internet banking, there is no technique to totally guarantee their safety. However customer should have good practices to face risks that have in banking transactions. By reviewing the bank's information about its online privacy policies and practices, customers can reduce risk of hacking and need to have good communication with the bank. Also customer care services can build the privacy policy taking direct actions in Internet banking environments to get most suitable development in privacy policy.

Reference:

1. 'Security features in Internet Banking', newagebanking.com/finsec/modernizing-digital-security-to-protect-banks-from-fraud/, Jan 16, 2017.

2. Elbek Musaev and Muhammed Yousoof (2015) "A Review on Internet Banking Security and Privacy Issues in Oman", ICIT 2015- The 7th International Conference on Information Technology.

3. Mr. Shakir Shaik and Dr. S.A. Sameera (2014) "Security Issues in E-Banking Services in Indian Scenario", Asian Journal of Management Sciences, Volume-02, Issue-03, pp.(28-30). ISSN:2348-0351.

4. Dr.Tejinderpal Singh (2013) Security and privacy issues in E-Banking an empirical study of customers, perceptions, Indian Institute of Banking and Finance (IIBF),30.

5. Dhillon, G. and Torkzadeh, G. (2006) Values-focused assessment of information system security in organizations. Information Systems Journal 16 (3): 293–314.