THE STUDY OF FRAUDS AND SAFETY IN E-BANKING

MISS. SARIKA DIGAMBERRAO GUDUP
(Research Scholar)
Yeshwant Mahavidyalaya, Nanded.
Email:- sarika_gudup@rediffmail.com.

ABSTRACT

Now a day's, bank transactions are carried out on a large scale which is very complicated and time consuming. It is highly impossible for banks to perform those transactions manually like in traditional day's bank. So there arises the need of IT to handle lengthy and complex transactions in the banks. IT has made banking procedures easy, convenient, fast and professional, which is one of the greatest landmarks in banking history.

E-Banking is more of science than art, as it is scientific in using different electronic devices such as computers, telephone, and mobile, internet etc. It helps in bringing technology in the hands of clients and making them operate and transact their own. Today's young generation is well versed with the use of internet and is expected to be the future online customers. So computerization of banks entire transactions are expected in the future.

Keywords:- *E-Banking, Frauds, Safety.*

INTRODUCTION OF E-BANKING

Now a day's information technology plays a vital role in banking sector. Day by day increasing change in technology world, it leads to improve e-banking services of various banks. Traditional branch model of bank is now changing into new form of e-banking services like kiosk marketing machine, coin vending machines of SBI. It provides various advantages to customer of various banks.

Now-a-days people are educated more than olden days, today human lives becomes machine oriented and they don't have enough time to visit bank branch than ever before. E-Banking means providing banking products and services through electronic delivery channels like ATM, Internet banking, Telephone banking and other electronic delivery channels. SBI has over 4500 ATM centre in India approximately. Automated Teller Machine-ATM is electronic computerized telecommunication device that allows a customer to directly use a secured method of communication to access their bank accounts or make cash withdrawals and other services. Internet banking highly useful to the customer one who have computer with internet connection, they need not visit bank branch for their business transactions. Simply they can transact anywhere, anytime if they have internet connection. By dialing the tele-banking number customer can get various facilities like cheque book request, balance inquiry etc.

INTRODUCTION OF E-BANKING FRAUD

Although there is no single accepted definition of fraud The Legal Practitioner, 2013, it relates to wrongful or criminal deception that results in financial or personal gains. Bank Fraud is the use of deliberate misrepresentation which usually requires some technical expertise in order to fraudulently obtain money or other assets from a bank wise Geek, 2013. Research to understand why internal staff opts to engage in such activities exists. Benjamin, 2011 found that perceived inequality and perceived job insecurity had significant effect on employee fraudulent intent. Such findings help highlight that beyond technology, there are other factors capable of impacting fraud that comes into play.

Phishing is one of the mechanisms that fraudsters use to obtain customers personal details leading to its use for fraudulent activities. Amtul 2011 states that such challenges presented by phishing results in companies loosing thousands of dollars, and emphasizes the need for biometrics to help checkmate such activities. In addition, statistics show that 35.9% of the financial sector is the target for phishing. A Javelin Identity Theft Report 2010 started that there was a 12% and 12.5% increase in identity theft victims and fraud respectively. This not only highlights the fact that fraud and identity theft is on the rise, but that current security measures in place are insufficient.

INTERNET BANKING AND RELATED FRAUDS

Around 65% of the total fraud cases reported by banks were technology-related frauds (covering frauds committed through, at an internet banking channel, ATMs and other payment channels like credit, debit & prepaid cards) whereas advance-related fraud accounted for a major proportion of involved in fraud.

1. **Triangulation cloning:** Customers enter their card details on fraudulent shopping sites. These details are then misused.
2. **Hacking:** Hackers or fraudsters obtain unauthorized access to the card management platform of banking system. Counterfeit cards are then issued for the purpose of money laundering.
3. **Online fraud:** Card information is stolen at the time of an online transaction. Fraudsters then use the card information to make online purchases or assume an individual's identity.
4. **Lost or stolen card:** It refers to the use of a card lost by a legitimate account holder for unauthorized and illegal purposes.
5. **Debit card skimming:** A machine or camera is installed at an ATM in order to pick up card information and PIN numbers when customers use their cards.
6. **ATM fraud:** A fraudster acquires a customer's card, PIN and withdraws money from the machine.
7. **Social Engineering:** A thief can convince an employee that he is supposed to be let into the office building, or he can convince someone over the phone or via e-mail that he's supposed to receive certain information.
8. **Dumpster diving:** Employees who aren't careful when throwing away papers containing sensitive information may make secret data available to those who check the company's trash.
9. **False pretenses:** Someone with the intent to steal corporate information can get a job with a cleaning company or other vendor specifically to gain legitimate access to the office building.
10. **Computer viruses:** With every click on the internet, a company's systems are open to the risk of being infected with nefarious software that is set up to harvest information from the company servers.

INTRODUCTION OF E-BANKING SAFETY

Information security not only deals with information in various channels like spoken, written, printed, electronic or any other medium but also information handling in terms of creation, viewing, transportation, storage or destruction. This is in contrast to IT security which is mainly concerned with security of information within the boundaries of the network infrastructure technology domain. From an information security perspective, the nature and type of compromise is not as material as the fact that security has been breached. To achieve effective information security governance, bank management must establish and maintain a framework to guide the development and maintenance of comprehensive information security programmers.

TIPS FOR SAFE ONLINE BANKING

Keep your computer up-to-date with antivirus software, operating system patches, firewalls etc and ensure your browser is set to the highest level of security. More advice for Windows PC users can be found here or if you use an Apple Mac go here. Be wary of unsolicited emails or phone calls asking you for PINs or passwords your bank or the police would never ask for these in full. Always type your bank's address into your web browser never follows a link in an email and then enters personal details. A locked padlock or unbroken key symbol should always appear in your browser window when banking online. The 'http' at the beginning of the website address will change to 'https' when a secure connection is made. When making a payment, always double check that you have entered the correct account number and sort code. Never leave your computer unattended when logged in and log off as soon as you're finished, especially on any public computer. Check your statements regularly if you notice anything strange, contact your bank immediately.

Be wary of any unexpected or suspicious looking 'pop-up' windows that appear during your online banking session. Stop and think about the process you normally go through to make a payment to someone be suspicious if it differs from the last time you used it. Fraudsters sometimes try to trick people into making a real payment by claiming "it's just a test". If you want to get started with banking online, contact your bank directly. Most banks offer online demos of how to use their internet banking service. Many banks also offer free anti-virus software and browser security products.

OBJECTIVES OF THE STUDY

1. To find out the E-Banking frauds under the study area.
2. To know the awareness amongst E-Banking users regarding E-Banking safety measures.
3. To study the role of RBI towards prevention of E-Banking frauds
4. To analyses the risk factors and safety factors in E-Banking services.
5. To find out and suggest the remedial measures to prevent E-Banking frauds.
6. To know the various types of E-Banking users.

HYPOTHESIS OF THE STUDY

1. There is no any significance difference regarding awareness of E-Banking between traditional users and new users.
2. There is no any association between Occupation and awareness of E-Banking users.
3. There is no any association between Age and awareness of E-Banking users.
4. There is no any association between Sex and awareness of E-Banking users.
5. There is no significant difference in the users' perception towards security and privacy satisfaction regarding use of E-Banking services.

RESEARCH METHODOLOGY OF THE STUDY

For the completion of present research work the primary data and secondary data will be collected through Questionnaire and Banks reports, journals, Internet, etc. In this research study the sample will be selected areas customers having internet banking, ATM & credit cards of selected banks from Nanded District.

IMPORTANCE OF THE STUDY

Though there is automation and computerization, bank is still technological oriented, as it is service-providing institution. In such organizations it is necessary to provide an excellent service for learning online banking for efficient functioning of the organization and achieve goals of both the organization and individual. In a fast developing economy like India, banks have come to be known as an instrument of social and economic change.

CONCLUSION

The study of E-Banking services and Frauds was carried out using primary sources as well as secondary sources of information. Conclusions have been drawn on the various segregations on the basis of these analytical tools. These conclusions have provided the base on which the researcher was able to meet the objectives of the study. The rationale behind the study was verified on the basis of these conclusions as well the final conclusions that were drawn from the various segregations have enabled the researcher to pin point the exact level of awareness amongst E-Banking users about E-Banking services and the potential risks attached to them while availing them suggestions are given for creating awareness about E-Banking frauds and adopting proper safety and security system for banking industry. Efforts have been made to present some useful and interesting conclusions pertaining to present studies.

REFERENCES

1. http://www.icicibank.com/online-safe-banking/phishing-mail2.html.
2. © 2013, IJARCSSE All Rights Reserved.
3. Electronic Banking Consumer Security Awareness - Philippine National Bank.
4. Internet-Banking-Awareness-Guide-Retail-v2015.
5. Banking safely online.
6. In the use of all over study Books, Journals, Websites, News, and Reports.