International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

November-2015 Volume 2, Issue-6

Email: editor@ijermt.org

www.ijermt.org

ONLINE BANKING FRAUD RISK AWARENESS

Dr. Asha Sharma

Associate Professor, Department Of Commerce

Government College, Sri Ganganagar

Abstract

The purpose of this research is to investigate the knowledge of online banking fraud within the banking industry in India as a safeguard for financial customers. The research is founded on both the idea of routine activity and the theory of criminology. A qualitative content analysis research approach was utilized for the study of the text content data through the consistent nomenclature process of coding and classifying themes or patterns in order to present a careful consideration of online banking fraud awareness in the banking sector. This was accomplished by using the consistent nomenclature process of coding and classifying themes or patterns. The data reveal that many India banks have a very limited level of awareness regarding online fraud to the general population through their websites. On their respective websites, the majority of financial institutions publish to the general public less than half of the internet banking fraud knowledge that has been found. Even though some banks include information about online fraud on their internet banking applications, there is considerable doubt about whether or not this information is accurate and effective. This suggests that the majority of consumers of financial institutions engage in internet banking activities without having sufficient understanding on possible hazards and assaults posed by the internet. As a direct consequence of this, there is a significant risk that customers of financial institutions may become victims of fraud using internet banking.

keywords:*Banking, Fraud , Online*

INTRODUCTION

E-banking, often known as Internet banking, refers to any institution (banks) that enables borderless financial services at any time, from any location, and through any banking method. In layman's terms, this means that any user who possesses a personal computer and an internet connection (browser) may get connected to his bank's website in order to carry out any of the I.T system's functions. This is possible since banking services are now provided by means of a computer-controlled system. The users will have to interact directly with the consumers using this technology. It is not necessary for the consumers to physically visit the bank's location. A bank that offers online banking would often have a centralized database that can be accessed over the web. The menu provides access to all of the online banking options that the financial institution makes available. Any service may be chosen, and the manner in which the interaction continues will be determined by the specific nature of the service. Internet banking is responsible for the majority of the basic banking tasks that are carried out these days. Information technology is required for all virtual banking functions. This particular financial institution strives to provide the highest quality of core banking services possible through a variety of electronic channels, including mobile banking, telephone banking, debit cards, credit cards, smart cards, automated teller machines (ATMs), electronic funds transfer (EFT) systems, check transaction payment channels, and, most importantly, the internet. Because of internet banking, customers seldom go to branches, and one client in particular avoids using main branch banking altogether. E-banking is quickly emerging as a viable alternative to the conventional paradigm of banking that is based on physical bank branches. The term "intranet" refers to the internal network that is responsible for providing connectivity to the main office as well as connecting the numerous branches of the company. These networks are exclusive to the organizations for whom they were designed in the first place. As a result of developments in information technology, the majority of financial institutions in India have transitioned to core banking systems and shifted their reliance for conducting business on payment cards (both debit and credit cards) as well as electronic channels such as automated teller machines, internet banking, and mobile banking. It contributes to the growth of criminal organizations that commit frauds online, such as internet banking scams. Customers have not been the only ones pursued by fraudsters into this sector. However, the majority of banks' responses to frauds in these areas have room for additional development. This is necessary in order to avoid placing the whole burden of responsibility on the consumer. In addition, there is a lack of transparency among banks on the process of reporting these incidents as frauds. It is necessary for every banking institution to have a comprehensive framework for the governance of fraud, with a special emphasis on preventing frauds that are based on electronic channels. The purpose of this paper is to attempt to highlight the difficulties associated with effectively combating the problem of electronic fraud and to make recommendations for a framework that can be adopted across institutions. A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank. This definition of banking fraud can be found here.

OBJECTIVE OF STUDY:

1. To bring awareness to the many different types of e-banking scams perpetrated by con artists
2. To investigate the factors that contribute to the occurrence of bank fraud.

E-BANKING FRAUD

Despite the fact that there is not a single definition of fraud that is universally acknowledged, According to The Legal Practitioner (2013), it refers to the practice of engaging in unlawful or illegal deceit for the purpose of obtaining financial or personal benefit. In order to illegally gain money or other assets from a bank, one must engage in bank fraud, which is the purposeful falsification of financial information, which often takes some level of technical competence. Geek, 2013. There has been research done to try to understand why employees on the inside choose to participate in such activities. Benjamin's research from 2011 indicated that employees' perceptions of inequality and job instability had a substantial influence on their willingness to do fraudulent acts. These findings help bring to light the fact that, in addition to technology, there are other elements that can have an influence on fraud that are at play. Phishing is one of the methods that con artists employ to get the personal information of their victims, leading to the use of such information in fraudulent actions. According to Amtul 2011, such difficulties, such as those presented by phishing, result in businesses losing thousands of dollars. Amtul 2011 also underlines the necessity for biometrics to assist checkmate such actions. In addition, according to the figures, 35.9% of the businesses in the financial industry are victims of phishing. According to the Javelin Identity Theft Report for 2010, there was a 12% rise in the number of people whose identities were stolen, and there was a 12.5% increase in the number of people who committed fraud. This underlines not just the reality that fraudulent activity and identity theft are on the rise, but also the fact that the security mechanisms that are already in place are insufficient.

INTERNET BANKING AND RELATED FRAUDS

Around sixty-five percent of the total fraud cases that banks reported were technology-related frauds (covering frauds committed through internet banking channels, ATMs, and other payment channels like credit, debit, and prepaid cards), whereas advance-related fraud accounted for a significant portion of those who were involved in fraudulent activity.

1. Cloning by triangulation: Customers submit their credit card information on shopping websites that are fake. After then, these particulars are misapplied.
2. Hacking: This is when criminals or hackers get unauthorized access to the card management platform of a financial institution. After then, fraudulent credit cards are distributed with the intention of launder[ing] money.
3. Credit card information is taken during the course of an online purchase and used for fraudulent purposes. Criminals commit identity theft by using stolen credit card information to make online transactions or to assume the identity of another person.
4. Card lost or stolen: This term refers to the usage of a card that was taken from a valid account holder for the purpose of doing unauthorized and criminal acts using the card.
5. Debit card skimming is the installation of a device or camera within an automated teller machine (ATM) with the purpose of stealing card information and PIN numbers from consumers when they use their cards.
6. Atm fraud occurs when a con artist fraudulently obtains a customer's card and PIN and uses them to steal money from an ATM.
7. Social engineering: A thief can convince an employee that he is meant to be admitted into the office building, or he can convince someone over the phone or via e-mail that he is supposed to get particular information. Both of these methods are examples of how a thief might steal information.
8. Employees who are careless while discarding papers that contain sensitive information may inadvertently make confidential data accessible to those who inspect the garbage at the organization.
9. Under false pretenses: A person who has the intention of stealing business information might seek a position with a cleaning company or another vendor particularly to gain lawful access to the office building in order to take the information.
10. Computer viruses: Every time a user makes a click on a website that is hosted on the internet, a business runs the danger of having its computer systems infected with malicious software that is designed to steal information from the company's servers.

NEED FOR E-BANKING

Through the use of online banking, any query or transaction may be performed, at any time of day or night, over the internet, rather than having to physically go to the branch in order to withdraw cash or deposit a check. The use of online banking also contributes to the safety of financial transactions. It alleviates the anxiety associated with constantly being required to carry cash. The availability of online banking services is quickly transitioning from a "nice to have" to a "need to have" amenity. Because it is the most cost-effective method of offering banking services to clients, internet banking is increasingly being seen as the standard rather than the exception. Banks have always been at the forefront of utilizing technology to improve the quality of their products and the effectiveness of their operations.

TYPES OF INTERNET BANKING OR E-BANKING- Examiners are able to evaluate the hazards associated with using online banking by first gaining an understanding of the various forms of online banking. The following is a rundown of the three primary varieties of online banking that are now in use in the industry.

Informational-

The most fundamental aspect of internet banking is the informational level. On a server, the bank maintains all of the relevant marketing information on the services and products offered by the bank. In this case, the danger is not particularly high because there is no path between the server and the bank's internal network that is provided by the informational systems. This level of Internet banking may be offered by the banks themselves or may be contracted out to a third party. Even if the risk to a bank is quite minimal, there is still a possibility that the server or website might be corrupted. Therefore, the right controls need to be set up in order to prevent unauthorized changes from being made to the server or website of the bank.

Communicative-

This category of Internet banking systems is beneficial to the interaction that takes place between the client and the banking system. The contact could be restricted to e-mail, inquiries about accounts, applications for loans, or static file modifications (name and address changes). The danger associated with this setup is greater than the risk associated with informational systems since the servers in question may have access to the bank's internal networks. Any effort by an unauthorized party to gain access to the bank's internal computer networks and networks must be prevented, monitored, and reported to management in accordance with the specifications of the controls that have been established. In this scenario, virus control also becomes an issue of much greater importance.

Transactional-

Customers have the ability to carry out transactions thanks to the transactional level of Internet banking. This is the design with the most risk, as there is generally a path between the server and the bank or outsourcer's internal network. Therefore, the controls for this architecture need to be the most stringent. Accessing accounts, paying bills, moving payments, and other activities can all fall under the category of customer transactions.

FRAUDS-

Tricks used to gain dishonest advantage over another person; usually financial in nature is known as Fraud.

Online banking fraud is divided into three categories; each poses a unique threat to customers and institutions. They are:

- **Identity Theft** – The third form of fraudulent activity involving internet banking is the one that may be characterized the most broadly. Customers are most concerned about having their identities stolen. As these examples show, identity theft can be as straightforward as possible or as intricate as possible. - (a) A client receives a phone call from a collection agency informing her that she has a credit card debt of $5,000. The consumer discovers after conducting some investigation that her identity was stolen and that the perpetrator created many credit card and checking accounts at various institutions, passed fraudulent checks, accessed her online account, and moved the money out via bill pay. b) A client's entire funds were withdrawn because another employee at her doctor's office had a name that was similar to hers and was able to gain access to the customer's private information. Once the thief in possession of the stolen identity had obtained the information, they emptied the victim's finances by moving their money into a new account and then making withdrawals from that account.

Theft of one's identity can make life very challenging for the victim of the crime. It might take several months, or possibly several years, to repair the harm that it could do. If the thief has obtained sufficient information to answer the questions requested by the financial institution in a satisfactory manner, then the thief will be able to utilize the information to perpetrate fraud against the financial institution. Because the degree of scrutiny and the kinds of questions that are asked might influence whether or not an identity theft is successful, it is essential that those questions be formulated in such a way that only the real person can know the answers to them.

• **Friendly Fraud** – This particular type of deception is often referred to as "civil fraud" or "family fraud."When someone commits fraud by exploiting information that belongs to a trusted friend or family member, this is referred to as "friends and family fraud." Despite the fact that consumers are told by their financial institutions, other organizations, and the media that they should not disclose their sensitive data with other individuals, a significant number of customers do in fact share their information with their immediate friends and family. A rising number of incidents of identity theft suggest that intimate friends or family members of the victim would pretend to be that person in order to steal from them. The investigation of these matters takes a significant amount of time, but they may pose a reduced threat to the organization if they are returned to the client for resolution in a civil rather than a criminal context. When a person finds out that a close friend or member of their family has lied to them, it may have a terrible effect on them, and these situations can be particularly challenging for the people who have been victimized. The following are some examples of fraud committed by friends and neighbors: - a client of the financial institution dials the toll-free number provided by the call center to report that he is unable to access his account online. While the person from the contact center is speaking with the client, the representative is able to observe that someone is accessing the customer's account while they are online. The representative asks the client if anyone else might know his password, and the customer responds that he has told his daughter it is the same password as the one on his ATM card, which he gave to his daughter so that she could withdraw money. The representative then asks if anybody else might know his password. It has come to light that the daughter recently uprooted herself, did not leave on amicable terms, and absconded with all of her father's money. b) A customer phones the call center to check about her account, and it is revealed that her soon-to-be ex-husband moved all of the monies out of her individual account and into the joint account using the customer's online user ID. After that, he proceeded to the location where the transaction took place and withdrew the money from the joint account. The wife never sees her husband or her money again.

The most effective way to protect oneself against this kind of deception is to impress upon one's clients the significance of maintaining the strictest possible confidentiality regarding their passwords. It is the responsibility of the client to invite anybody they feel comfortable entrusting with their money to join the account if they want that individual to have access to the customer's money. If the customer does not trust the other person enough to do that but still wants to donate money to someone, the customer should withdraw the money themselves and give it to the recipient in person.

Internal Fraud – One more way for an employee to steal is provided by this form of fraudulent activity, which adds to the total number of possible ways. If workers of a financial institution have access to client data, and that data is the same information that is required to acquire online access to customer accounts, then it is simple for employees to perpetrate fraud against customers. Because of this, financial institutions should demand a password or PIN before allowing customers to do online banking, and they should retain the password or PIN in an encrypted manner. Altering account numbers and other client information while restricting staff access to the whole numbers is still another possibility. Internal fraud has the potential to be the most expensive kind of the three forms of fraud that may occur in financial organizations.

FRAUD RISK MANGEMENT:

There is a pressing requirement for an appropriate and unified standard of fraud governance. The banks themselves are the ones who should be in charge of fraud risk management and fraud investigation. Banks in India have altered their focus to their core banking operations and have migrated their transactions and payments to electronic channels such as ATMs, internet banking, and other similar services. Criminals that commit fraud have also taken an active part as customers in the global financial system that is based on computerized transactions. The reaction of the banks on the fraud revealed a need for more enhancements to quickly overcome the theft that occurred through e-banking. The following are some methods that may be used to manage the risk of fraud.

- A powerful "Transaction Monitoring Team" is an essential component that every financial institution must have and keep up to date. The transaction monitoring team's job is to keep an eye on all of the transactions that are taking place and determine whether or not any suspicious transactions are occurring in accordance with the banking standards. If they discovered any questionable transactions, then the account holder should be held accountable for any appropriate steps that are taken.
- A powerful "Fraud and Prevention team" is something that every single financial institution ought to have and make sure to keep up. The Fraud and Prevention Unit is responsible for tracing out fraudulent behavior and stopping it from occurring before it is actually carried out.
- Customers of a financial institution may use a specialized email address provided by the institution to report any fraudulent behavior they may observe. The aforementioned email addresses can be used to contact a specialized staff that will respond to any questions or issues raised by customers. Phone banking officers and branch personnel both need training on how to respond to questions and concerns raised by clients regarding fraudulent activity.
- Banks should consider the possibility of establishing a fraud helpline for their consumers as well as their workers. This would provide customers and staff the ability to report possible scams and seek advice on how to avoid falling victim to it. Banks can open up yet another channel for the early reporting and identification of fraudulent activity if they behave in this manner.
- Increasing both the staff's and the consumers' knowledge of fraudulent activity. The foundation of effective fraud management is education on how to both avoid and uncover fraudulent activity. It is necessary for financial institutions to use a variety of steps in order to raise awareness among both their employees and their consumers.
- The safety of the banking industry's physical infrastructure is the responsibility of a staff that is present at each and every financial institution. This group should do routine security audits at a variety of

offices in order to look for any deviations or gaps in security. It is the duty of this group to make certain that the physical assets of the bank and any data that has been duplicated onto magnetic or optical media are not removed from the premises of the bank without proper authorization.

- Banks may provide clients with unique email IDs that they can use to report any fraudulent behavior that the customer may observe. The aforementioned email addresses can be used to contact a specialized staff that will respond to any questions or issues raised by customers. Phone banking officers and branch personnel both need training on how to respond to questions and concerns raised by clients regarding fraudulent activity.
- Raising awareness among workers and providing them with training on the many forms of fraud, as well as how to identify them and how to avoid falling victim to them. It is feasible with the implementation of the appropriate methodology and training program.

Conclusion

According to the facts presented above, this study comes to the conclusion that online banking fraud awareness disclosure is at an extremely low level across many banks in India. On their own websites, the majority of the banks published fewer than fifty percent of the aforementioned online banking fraud knowledge. This suggests that the majority of consumers of financial institutions engage in internet banking activities without having sufficient understanding on possible hazards and assaults posed by the internet. As a direct consequence of this, there is a significant risk of falling victim to fraudulent activity using internet banking. Both primary and secondary sources of information were utilized over the course of the research project that was conducted on fraudulent activities and electronic banking services. On the basis of these different analytical techniques, a number of conclusions have been formed about the various classifications. The researcher was able to accomplish all of the goals of the study because to the foundation that was supplied by these results. Fraud presents ever-growing difficulties for financial institutions. These difficulties are only expected to grow. Criminals are always coming up with new fraud schemes in an effort to keep one step ahead of those who are attempting to battle such techniques. These fraud schemes include malware, trojans, phishing, vishing, whaling, SMS sishing, and hacking.

References

[1] Abend, V., Peretti, B., Bach, A., Barry, K. & Donahue, D. (2008). Cyber Security for the Banking and Finance Sector, Homeland Security, pp. 1-17.

[2] Angelakopoulos, G. & Mihiotis, A. (2011). E-banking: Challenges and opportunities in the Greek banking sector, Electronic Commerce Research, Volume 11, Issue 3, pp. 297-319.

[3] Ahmad, W. (2008). Is credit card fraud a real crime? Does it really cripple the E-commerce sector of E-business? Proceedings - International Conference on Management of e-Commerce and e-Government, ICMeCG, pp. 364-370.

[4] Alsheyyab, M.M.A. & Singh, D. (2013). Effect of trust on E-banking user's satisfaction: A review.Research Journal of Applied Sciences, Engineering and Technology, Volume 5, Issue 4, pp. 1397-1406.

[5] Baker, C.R. (1999). An analysis of fraud on the Internet, Internet Research, Volume 9, Issue 5, pp. 348-360.

[6] Brink, H., Walt, C., Rensburg, G. (2012). Fundamentals of Research Methodology for Healthcare Professionals. Juta & Company, South Africa.

[7] Chiemeke, S.C., Evwiekpaefe, A.E. & Chete, F.O. (2006). The Adoption of Internet Banking in Nigeria: An Empirical Investigation, Journal of Internet Banking & Commerce, Volume 11, Issue 3, p. 4.

[8] Personal talk to those banking personnel who are working in the“Transaction Monitoring Team” and “Fraud and Prevention team”

[9] B.P.Gupta, V.K.Vashistha, H.R.Swami, Banking and Finance, Ramesh Book Depot, Jaipur-New Delhi (2008).