International Journal of Engineering Technology and Management Sciences

Website: ijetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005
ISSN: 2581-4621

IMPACTS OF CYBER CRIME ON INTERNET BANKING

Dr. Vijayalakshmi P[1], Dr.V.Priyadarshini[2], Dr. Umamaheswari K[3]

[1] *Associate Professor, Sri Krishna College of Engineering and Technology, Coimbatore*
[2]*Associate Professor, Kathir College of Engineering, Coimbatore*
[3]*Assistant Professor, Lead College of Management, Palakkad*

[1]vijayalakshmimenon@gmail.com
[2] priya.management@gmail.com
[3]uma@lead.ac.in

***Abstract*—Internet banking or e-banking refers to the facility through information and communication technology. Internet banking is increasingly becoming popular because of both convenience and flexibility. Computer fraudsters are always trying to gain illegal access to the information of financial and business sectors for fraudulent activities. The customers of Internet banking always fear for their financial data when dealing with Internet banking and its services. There is a need to create awareness among Internet banking customer on how to avoid the available threats. The research in this paper critically analyzes and discusses the effects of cyber threats when dealing with online banking services. It is concluded that by the research that there is a need to increase safety measures in available cybercrimes when dealing with Internet banking and sensitive financial data.**

***Keywords*— Cyber-Crime, Financial Fraud, Motives, Identity Theft**

I. INTRODUCTION

The rapid growth in cybercrimes is the main concern for financial institutions in 21st century and the need to protect the cyber space is becoming more critical than ever before. Cybercrime is one of the burning issues in today's Internet banking industry in the world.

Cybercrime according to Douglas and Loader (2000) can be defined computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties. For appropriate measurements to be implemented, organizations must understand the effects of cybercrimes. Financial organizations need to be aware of Internet threats and must take into concern all those measure that can help in improving the awareness of individuals in regard of safety and to maintainable financial business environment. The effects of cybercrimes are more than the financial integrity of financial institutions and other organizations. For appropriate measurements to be implemented, organizations must understand the effects of cybercrimes.

The rapid growth of Information Technology and mobile networks has led to the development of Information society in the modern world. Although this development provides and facilitate computer users to collect information with their fingertips but there are issues that must be considered. The fear of losing personal information or becoming a victim of Internet banking services is still there in the modern society of information technology. Security developers are using many tactics to provide secure financial platforms. However, computer impostors and criminals are few steps forward.

This needs a broad approach to fight against cyber criminals and computer impostors by developing satisfactory legislations and appropriate legal framework to protected Internet financial transactions and additional activities.

II. REVIEW OF LITERATURE

Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru, (2018), they have identify study and analyze the loopholes existing in the Indian Banking Sector in order to curb the fraudulent activities and to be able to take corrective actions, thereby enhancing the security measures of this sector.

Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas (2017), discussed that effect of cyber threats in Internet banking services and had strengthen customer awareness when dealing with Internet banking services. By their way of survey it is important to understand and identify the security issues and Internet banking customers must be aware about these techniques and methods used by computer fraudsters.

Seema Goel (2016), revealed that technical aspects of various types of cybercrimes concerning the banking and financial sector and their related impacts. Additionally, she identifies the threat vectors supporting these cybercrimes and develop measures to aid in the combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security.

R. P. Manjula & Dr. R. Shunmughan (2016), analyze about the cyber space and the customer's perception about cybercrime. More awareness programs can be conducted

Website: ijetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005
ISSN: 2581-4621

for the customers so that the cybercrime can be reduced in future period of time.

A.R. Raghavan and Latha Parthiban (2014), they examined the different types of cybercrimes which plague the banking sector and the motives of the cyber criminals behind such acts. The financial loss in the banking sector is huge across the globe both in terms of combating the cyber-attacks and on development of systems, so that such attacks need to be prevented in the future.

Ajeet Singh Poonia (2014), Cybercrime has high potential and thus creates high impact when it is done. It is easy to commit without any physical existence required as it is global in nature due to this it has become a challenge and risk to the crime fighter and vice versa.

Soni R.R. and Soni Neena (2013), they showed a bigger share of private and foreign banks in frauds related to Internet banking, ATM, cards and other digital banking. Banking cyber frauds in the country are the result of introductory phase of banking technology like ATM, Internet banking, mobile banking, EFT etc. which need time for people, market and technology to get matured. Regulatory framework also gets stronger by experience.

Wada and Odulaja (2012), discussed that Cybercrime policy issues and provide insight into how cybercrime effects on E-banking from a Nigerian perspective. Social theories were used to explain causation with a view of guiding policy makers on behavioral issues that should be considered when formulating policies to address Cybercriminals activities in Nigeria.

Jaishankar K., (2008), he developed a theory called 'Space Transition Theory' in order to explain the causation of crimes in the cyberspace. He felt the requirement for a separate theory of cybercrimes because the general theoretical explanations were found to be inadequate as an overall explanation for the phenomenon of cybercrimes.

Divya Singhal and V. Padhmanabhan (2008), Internet banking is becoming is increasingly becoming popular because of both convenience and flexibility. The current paper explores the major factors responsible for internet banking based on respondent's perception on various internet applications.

Siaw I, Yu A (2004), identifies who are able to leverage competitive benefits from the internet are confronted with significant business potential. The impact of internet in banking industry and internet banking as a source of competitive advantage has becoming challenging issues for both business managers and academics.

Joseph et al. (1999) examined the impact of internet on the delivery of banking services. They found six fundamental dimensions of e-banking service quality such as convenience and accuracy, feedback and complaint management, efficiency, queue management, accessibility and customization.

III. RESEARCH METHODOLOGY

The data used is completely secondary in nature i.e., from sources published, printed media, magazines and journals.

Objectives of the study

- To study cybercrimes and its implications on the Banking Sector
- To understand the seriousness of online cyber threats available to Internet banking industry.
- To understand the impacts of cybercrime and its motives.
- To measure the scope of security and its implementation in Internet banking sectors.
- To analyze and use the preventive measures available to control frauds.

IV. OVERVIEW OF INTERNET BANKING IN INDIA

Internet banking refers to the use of Internet as a remote delivery channel for banking services such as opening a deposit account or transferring funds at different accounts etc. There is evolution in development of internet banking. Jun and Cai (2001) suggested that some dimensions such as responsiveness, reliability and access are critical for both traditional and internet banks.

At the basic level, Internet banking contains the setting up of a web page by a bank to give information about its product and services. At an advance level, it involves provision of facilities such as accessing accounts, funds transfer, allowing integrated sales of other process and access to other monetary services such as investment and insurance. The services through Internet banking are e-tax payment; access the account to check balance, online trading of shares, online remittance of money, electronic bill payment system, railway reservation, transfer of funds from one customer's account to other, application of loan, etc.

Jansen, J. (2015), examined the model is extended with additional variables, making it suitable for the Internet banking context. The coping perspective, which is central to the Protection Motivation Theory, seems to be valuable to study behavior in information systems

There are three functional levels of Internet banking which are informational, communicative and transactional. Under informational level, it has been identified that banks have the marketing information about the bank's products and services on a standalone server. Communicative level of Internet banking allows some interaction between the bank's systems and the customer. Transactional level Internet banking permits bank clients to electronically transfer funds to/from their accounts, pay bills and conduct other banking transactions online.

Website: ijetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005
ISSN: 2581-4621

Rexha, N., Kingshott, R. P. & Shang Aw, A. S. (2003), revealed that cumulative effects of customer satisfaction were found to have a positive impact on trust directed towards the bank, and this greatly impacted on the propensity to use electronic banking.

V. CYBER CRIME IN INTERNET BANKING

Some of the crimes in Internet banking sector are:

Identity Theft: Using someone else identity such as name, date of birth, and address for fraudulent activities is one of the common tactics adopted by cyber criminals when dealing with electronic businesses particularly Internet banking services. Information obtained through identity theft by cyber criminals can later be used for many commitments such as opening new bank accounts; obtaining credit card or loans and receiving state benefits.

Phishing: Phishing are strategies adopted by cyber criminals and impostors to make victims disclose their personal and other secret financial information. For phishing, there are many tactics which are used by cyber fraudsters but the most important tactics is sending a phishing email to Internet banking customers by imagining that a genuine company/organization is offering electronic services.

Vishing: Vishing using voice is a way of using fake call center using VOIP, Voice over IP, and technique by computer fraudsters to acquire Internet banking customer's details and their financial data. To achieve the purpose an email system is used by fraudsters asking Internet banking customers to confirm their banking details and other information as process of security routine check at the phone number provided in the phishing email.

Malware: Malware (Viruses, Worms, Trojans and other threats) is the most important threat available from cyber criminals to gain unauthorized access to user's accounts to steal their financial data and other sensitive information. The rapid growth in mobile devices such as Smartphone and Tablet PCs leads to more development of the malicious software of Malware. Hacking &Cracking: Through hacking and cracking computer impostors can break into computer and computer networks to steal financial information which can later be used for unauthorized purpose. Different malicious software could be used for the purpose of hacking by computer fraudsters such as Trojan virus. Bossler, A. M., & Holt, T. J. (2009), they uses routine activities framework to explore data loss caused by malware infection. Similar to research on traditional forms of victimization, computer deviance was related with computer victimization.

Automating Online Banking Fraud: Cybercriminals and computer fraudsters have currently taken things a step further with the help of Automatic Transfer Systems (ATSs). A new system has been started for an Automating Online Banking Fraud system using in conjunction with Spy Eye and Zeusmalware variants as part of Web Inject files which is a transcript file with lot of JavaScript and HTML Codes.

Social Engineering: Social Engineering is the art of employing people into performing actions or exposing confidential information. The social science discipline of social engineering is commonly used by computer fraudsters and cyber criminals to attain financial data to gain unauthorized access to sensitive information.

Social Networks: Social Networks are the mutual platforms available for cyber impostors to access information shared by the account holders. The accessed information by cyber fraudsters can later be used for unauthorized purposes. These social networks platforms such as Facebook and Twitters allows user to send an instant message and during the process users could be redirected to some other website by providing a link by the fraudsters.

Denial of Services (DoS) Attack: Denials of Service (Dos) attacks are challenges by cyber fraudsters to make network resource unavailable to its users. The nature of these attacks is so serious that individual distributed denial-of-service (DDoS) attacks could soon take down not just one site, but any intervening service providers.

Electronic Gadgets and Mobile Phones: The use of smart-phones and other electronic gadgets such as Computer Tabs becoming common practice in today's electronic age. Security experts are predicting serious threats from cyber criminals and computer fraudsters on the available platforms of smart-phones and computer tablets.

Electronic Media Platforms: People are using more sophisticated browser enabled platforms in their homes now. These include media streaming devices and internet based or smart televisions offered by many manufacturers. An example of Google TV is near too. Accessing internet via these platforms also create security concern for consumers. The platforms can easily allow cyber criminals and fraudsters to manipulate variety of physical devices through controlled applications.

VI. IMPACTS OF CYBER CRIME ON THE BANKING SECTOR

The cases related to cybercrimes have grown ruthlessly due to the upsurge in mobile devices with internet connectivity. Smartphones are nowadays used for numerous online activities like internet banking, Online shopping, paying utility bills and are constantly in the eyes of the criminals to get access to private information.

Among the several motivations for committing a cybercrime, Financial Gain remains the constant winner for the past many years overtaking other motives including revenge, extortion and political causes. Alarmingly, simple phishing attacks enjoy a success rate

Website: ijetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005
ISSN: 2581-4621

of 45% due to lack of awareness regarding the common safeguards to protect against the shrewd cyber criminals.

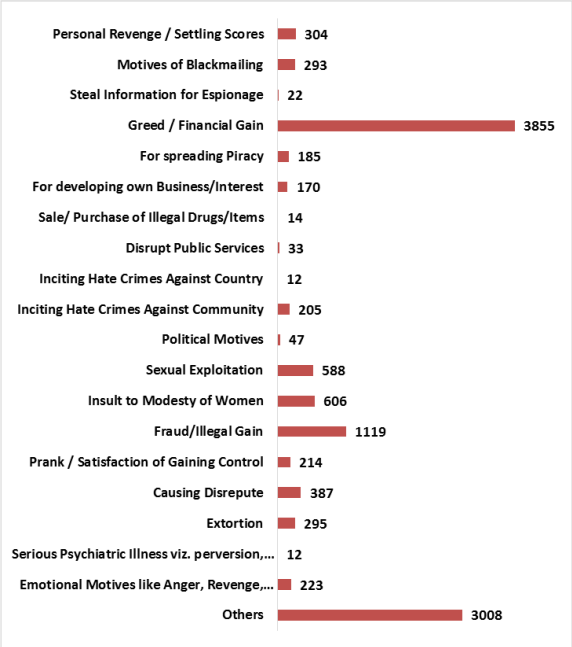

Fig. Cyber Crime by Motives

The span of cybercrime can be projected from the figures of 3855 cybercrimes committed for financial gain (NTRO) and 534 phishing incidents (CERT-In) in year 2020.

There are 27,482 cases of cybercrime were reported from January to June 2018. These incidents only correspond to the reported incidents and do not comprise the incidents that pass on unreported and/or ignored.

Security Measures

Internet banking users should know common security measures to prevent cyber-attacks and to secure their financial data.

Secure the Device: The safety of the device used for Internet banking access is serious at initial stage. These devices contain computer systems, mobile and other gadgets used for the access of Internet banking.

Protect your Personal Data: Data security is important. Confidential and personal data should not be disclosed to all people. When providing information, one needs to consider the purpose and take extra measures to avoid some social engineering or other strategies used by computer fraudsters and criminals. Internet banking users should understand how to encrypt the data used for financial organizations such as banks and tax returns.

Use Strong Passwords: The usages of strong passwords are continuously recommended for Internet banking users. Many tools can be used by computer fraudsters to deduct or crack the passwords of Internet banking users. It is further recommended that passwords should not be written down anywhere. Combinations of different alphabets, number and special characters should be used for a strong password.

Be Secure when Online: The identity of individuals must be protected when dealing online. All social media profiles must be set to private. Security setting of social media accounts should be checked regularly. Private and sensitive information should not be disclosed through the use of social media.

Upgrade System and Software: It is suggested that Internet users must renovate their systems and software to avoid security breaches.

VII. FINDINGS AND SUGGESTIONS

Findings

- Majority of the cybercrimes in this sector have resulted out of hacking and identity theft.
- Banks are being targeted over and over again because all the reserves in the form of cash are held with the banks.
- The software can be used for detecting frauds in maximum cases is either outdated or very time consuming.
- The number of cases would be resolved by the cyber cell has remained consistently low for the last four years, with only 20 per cent success rate.

Suggestions

- Internet banking users should use strong passwords and different user name combinations for different sites and accounts.
- The law enforcement should be very rigid, and updated from time to time to keep a track of such crimes.
- There should be fast track mobile courts to solve these cases, to meet the grievances and build confidence among the public.
- The government should also keep a track on the operating network activities with the help of Big Data Banks.
- Punishments and penalties must be exercised systematically in order to minimize the impact of these issues and penalize the attackers.

Website: ijetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005
ISSN: 2581-4621

- Awareness Programs should be initiated in order to inform the public about the ongoing scenario and upcoming threats.
- The public must information about these cases to the Cyber Crime Branch in the matters related rather than just referring it to the banks, so as to ensure fast and strict actions.

VIII. CONCLUSION

This research is to understand and identify the security issues when dealing with Internet banking services. The criminals of this advanced age endeavor to commit these new crimes with the support of computers through Internet by abusing cyber space. Cybercrime is becoming a greater threat as a result. Cybercrime comprises its own set of unique attractive features that have gradually started outweighing the traditional crimes. The extent of anonymity, global victim reach and swift results are amongst the few that cybercriminals find most attractive. Unaware consumers are easily deceived due to lack of insight into the latest attack methodologies and identified preventive measures. Engagement of expert in cyber security professionals is a step further to develop quicker and better cybercrime investigation results. As estimated by NASSCOM's Cyber security Task Force, India needs 1 million trained cyber security professionals by 2025.

References

[1] .Liaqat Ali, Faisal Ali, Priyanka Surendran, Bindhya Thomas (2017), The effects of cyber threats on consumer behavior and e-banking services,7(5), 70-76.

[2] Seema Goel (2016), Cybercrime: A Growing threats to Indian banking sector, 5(12), 552- 558.

[3] Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru, (2018), Cybercrime: A Growing threats to Indian banking sector, 5 (1), 926-933.

[4] Siaw I, Yu A (2004), An analysis of the impact of the internet on competition in the banking industry, using porter's five forces model. International Journal of Management 21: 514-522.

[5] Wada & Odulaja (2012), Assessing Cybercrime and its Impact on E-Banking In Nigeria Using Social Theories, 4 (3), 69-82.

[6] Soni R.R. and Soni Neena (2013), An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks, 2(7), 22-27.

[7] A.R. Raghavan and Latha Parthiban (2014), The effect of cybercrime on a Bank's finances, 2 (2), 173-178.

[8] R. P. Manjula & Dr. R. Shunmughan (2016), A study on customer preference towards cybercrime with banking industry, 2 (1), 597-603.

[9] Jansson, K. & Von Solms, R. (2013), Phishing for phishing awareness. Behavior & Information Technology, 32(6), 584–593.

[10] Ajeet Singh Poonia (2014), Cybercrime, challenges and its classification, International journal of Emerging Trends and Technology in Computer Science, 3(6).120-127.

[11] Divya Singhal and V. Padhmanabhan (2008), A Study on Customer Perception towards Internet Banking: Identifying Major Contributing Factor, 5 (1), 101-111.

[12] Douglas Thomas and Brian Loader (2001), Cybercrime: law enforcement, security and surveillance in the information age, 30 (1), 149-188.

[13] M. Jun, and S. H. Cai, (2001), The Key Determinants of Internet Banking Service Quality: A Content Analysis," International Journal of Bank Marketing, 19 (7), 276-291.

[14] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q.,Warkentin, M. & Baskerville, R. (2013), Future directions for behavioral information security research. Computers & Security, 32, 90–101.

[15] Jansen, J. (2015), Studying safe Online banking behavior: A protection motivation theory approach. Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance, 120–130.

[16] Ngo, F. T. & Paternoster, R. (2011), Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773–793.

[17] Hansman, S. & Hunt, R. (2005), A taxonomy of network and computer attacks. Computers & Security, 24, Elsevier Ltd., 31-43.

[18] Hwang, J., Yeh, T. & Li, J. (2003), Securing on-line credit card payments without disclosing privacy information. Computer Standards & Interfaces, 25, Elsevier Science B. V., 119–129.

[19] Khattak, N. A. &Kashif-Ur-Rehman (2010), Customer satisfaction and awareness of Islamic banking system in Pakistan. African Journal of Business Management, 4(5), 662-671.

[20] Rexha, N., Kingshott, R. P. & Shang Aw, A. S. (2003), The impact of the relational plan on adopting of electronic banking. Journal of Services Marketing, 17(1), 53-67.