Vol. 9. No. 3. 2022

©Copyright by CRDEEP Journals. All Rights Reserved.

DOI: 10.13140/RG.2.2.33218.25282

Contents available at: http://www.crdeepjournal.org

Global Journal of Current Research (ISSN: 2320-2920) CIF: 3.269

A Quarterly Peer Reviewed Journal

Global Journal of Current Research

Review Paper

Cyber Threats in E-Banking & its Effect on Consumers' Behaviour: An Analytical Study

Binayee Mishra

Lecturer in Commerce, U.N. (Autonomous) College of Science & Technology, Adaspur, Cuttack, India.

ARTICLE INFORMATION

Corresponding Author:
Binayee Mishra

Article history:
Received: 30-06-022
Revised: 10-07-2022
Accepted: 17-07-2022
Published: 18-07-2022

Key words:
E-Banking, Cybercrimes, Cyber Security, E-Commerce, Cyber Threats

ABSTRACT

Over the past three decades after globalization and financial sector liberalization banking industry has grown rapidly with financial institutions providing online banking services and encouraging customers to do online banking transactions such as money transfer, access information about the account or otherwise as well as payment of monthly bills. During all this time Internet crimes and thefts is bringing on forefront issues of cyber security all over world. Again in Developing countries cyber security threats in banking sector are becoming more pronounced and serious due to lack of financial literacy and awareness among customers. Internet banking has become one of the fastest and easiest way of banking. The threat of cyber security attacks set a great challenge for the Internet banking and electronic commerce (E-commerce) industries. In this backdrop the present article determine the types of cyber threats experienced by e-banking consumers; identify the effects of cyber threats on customer's behavior in e-Banking services and proffer control measures to curb cyber threats. Here 220 users of online banking have considered through a structured questionnaire from students of different colleges in Odisha. The study concludes that Online banking users should know common security measures to prevent cyber-attacks and to secure their financial data.

Introduction

Cyber threats increases by the ongoing digitalization. More and more organizations rely on digital networks for their business operations. This increases the risk for organizations and their customers of becoming victims of cybercrime. Over the past few years there were several cyber-attacks in the banking sector and on various components of online banking. Those attacks varied from stealing money to disabling online payment systems such as online banking through websites, mobile apps and iDeal. Cyber-attacks in the banking sector are mainly fraud related, because of the financial gain and have many forms .The impact of cybercrime has generated a significant risk exposure for individuals (personal harm) and organizations (reputational harm). It includes exposure to financial losses, regulatory issues, data breach liabilities, damage to brand and reputation, and loss of client and public confidence (Verma, Hussain and Kushwah, 2012). Cybercriminals can significantly threaten the finances and reputations of banks and other (financial) organizations. Moreover, it affects the relationship between the image of the organization and the trust that customers and other stakeholders have in the organization. Consequent negative publicity can create some serious issues for organizations when they become victims of cybercrime.

The objectives of this study are:

1. To determine the types of cyber threats experienced by e-banking consumers.
2. To identify the effects of cyber threats on customer's behavior in e-Banking Services
3. To proffer control measures to curb cyber threats.

Materials and methods

Methods of data collection: The study is based upon both primary and secondary data.

Primary data :

A survey was conducted with a target population of three i.e puri,khurda and cuttack districts in Odisha which comprises students of different educational institutions. Convenience sampling was used for survey. The final questionnaire was administered personally from 220 users of online banking in Odisha. The survey was done in the month of January 2020.

Secondary data:

Besides primary data, secondary data is also used for the purpose of research. The secondary data has been collected from various articles, working papers and websites of different banks.

Questionnaire Design:

A questionnaire consists of 50 questions was administered for customers to know their perception towards cyber-attack . The questionnaire was tested in the P.G department of commerce, U. N. College Cuttack and based upon the feedback appropriate changes were made to improve the questionnaire to make it more respondents friendly. The data was collected from 18 years old and above of online banking customers. A sample size of 220(n=220) is taken into account for the purpose of study.

Types of Cyber Threat

To increase the awareness of available cyber threats among online banking users, it is important that users should understand the available crimes. These cybercrimes are discussed in the further sections of this research.

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 online banking services. Information obtained through identity theft by cyber criminals can later be used for many purposes such as opening new bank accounts; obtaining credit card or loans and receiving state benefits. Identity theft is one of the world’s fastest growing crimes and the Kingdom of Bahrain is one of the victims of identity thefts crimes.

Phishing: Phishing are tactics adopted by cyber criminals and fraudsters 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 online banking customers by pretending that a legitimate company/organization is offering electronic services. A ‘spoofing site’, computer fraudsters designed website similar to the legitimate websites of financial institutions, can also be used for the purpose of phishing activities and stealing financial information of the online banking customers. The protection of online banking data is becoming difficult in today’s age of mobile applications as it was found that researchers at Web sense Security Labs have stumbled upon a password-stealing Trojan that uses sophisticated DNS redirection techniques to dodge server shutdowns and hijack online banking data. Phishing via mobile, computer applications and social media sites are the common platforms which are regularly used by computer fraudsters. It was reported by AFCC, Anti-Fraud Command Center, and that the total number of phishing attacks cost $4.5 billion of loss in the year 2014.

Vishing: Vishsing or phishing using voice is a method of using fake call center using VOIP, Voice over IP, technique by computer fraudsters to acquire online banking customer’s details and their financial data. To achieve the purpose an email system is used by fraudsters asking online 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 significant 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. Malware applications are used over the last few years by computer fraudsters to perpetrate hundreds of thousands of frauds against online consumers in business sectors particularly in online banking to draw off large amounts of money. Mobile Phone Malware is important to be considered here as some of the growing mobile platforms such as Android are the most targeted by malware authors and there is growing need to develop robust defenses against these sophisticated malware applications targeting online banking services and other financial institutions.

Hacking and Cracking: Through hacking and cracking computer fraudsters 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.

Automating Online Banking Fraud: Cybercriminals and computer fraudsters have now 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 ZeuS malware variants as part of Web Inject files which is a text file with lot of JavaScript and HTML Codes.

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

Social Networks: Social Networks are the common platforms available for cyber fraudsters 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 attempts 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. The costs of DoS attacks to critical infrastructure organizations can be significant. A respondent to the 2005 Australian Computer Crime and Security Survey reported a single-incident loss of $8 million arising from a DoS attack. Online banking services must consider the seriousness of these attacks and cyber threats to its business growth and therefore serious measures should be taken to improve the level of security and to maintain sustained business growth. There is constant need to improve the layers of security to the applications of online banking services and to minimize the available threats coming from cyber space.

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. The increase in customer accessing online banking services and application through mobile devices and the available threats must be considered seriously by the financial organizations and online banking services to make sure that they are skilled to operate their services on as many of these new platforms as possible.

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 there 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. Consumer education and awareness is becoming more important on how to best utilize and access these electronic media platforms.

Results

On the basis of data collected from users of online banking, we have analyzed the available information in following manner.

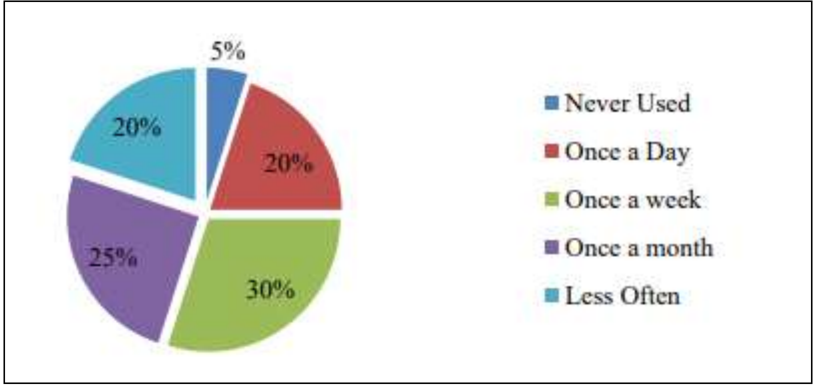

Fig 1-Frequency Measurement

The above Fig. 1 and its analysis clearly shows that only 20% of the participants use online banking services every day and 30% use online banking services once a week. The analysis proves that participants do online banking, except 5%. The 25% respondents confirmed that they are using online banking services once a month while 20% confirmed that they are less often using these services.

Fig. 2 (below) analysis proves the level of awareness of the respondents in regard to online banking services and available cyber threats. As shown, 40% respondents are aware of the computer hacking, 5% are aware of phishing while other 5% confirmed that they got awareness about vishing (phishing over VOIP). Out of 220 respondents, 15% confirmed their awareness about identify theft and 5% confirmed about DoS attacks. 2% respondents confirmed their awareness about social engineering. However, it is important to note that 23% respondents are aware about all the crimes and cyber threats mentioned in the survey. On the other hand, it shows that around 77% online banking users got limited awareness about available cybercrimes and threats.

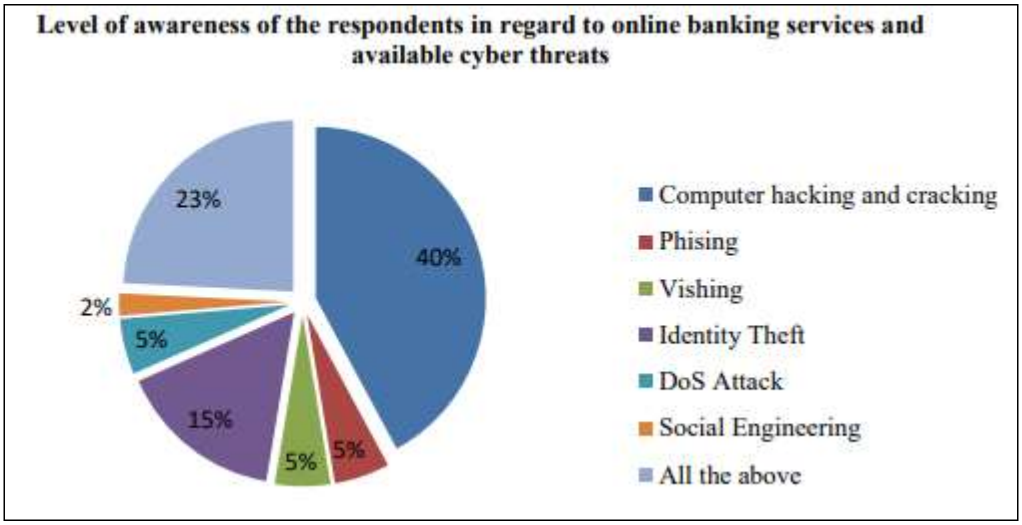

Fig 2: Awareness Measurement

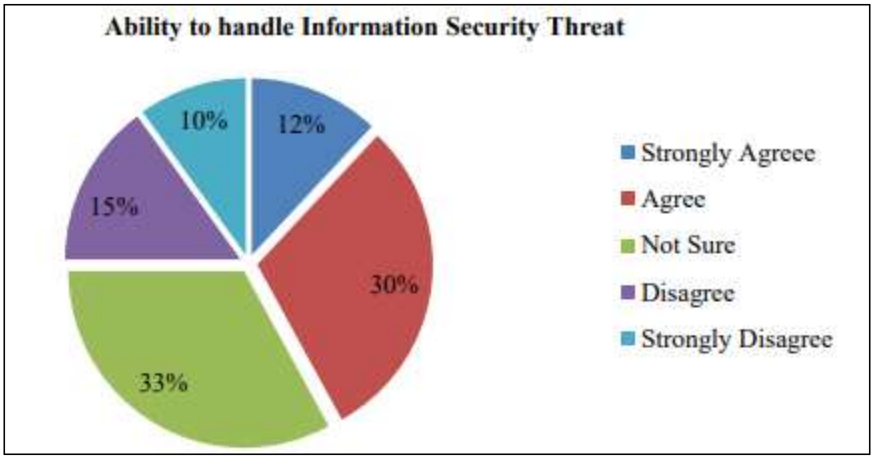

Fig 3: Ability of Handling Threat Measurement

The analysis of above Fig. 3 confirmed that only 42% respondents are able to identify information security threats and further they got the ability to handle with such threats. However, 33% survey respondents are not sure that they can manage the available threats. 25% respondents as per the above analysis cannot identify such threats and also do not have the ability to handle such threats.

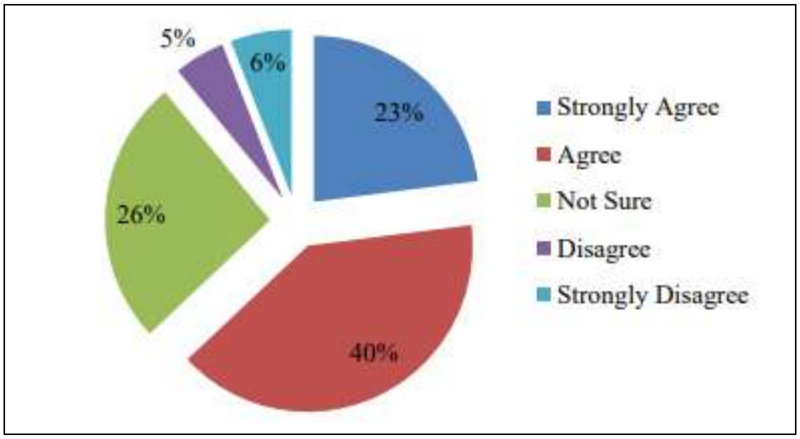

Fig 4. Individual's role in Information Security Risk

The analysis of the above Fig. 4 shows that 63% respondents of the survey are agreed or strongly agreed that the role of every single individual is important in reducing information security risks. The other 26% respondents are not sure while 11% do not agree with this.

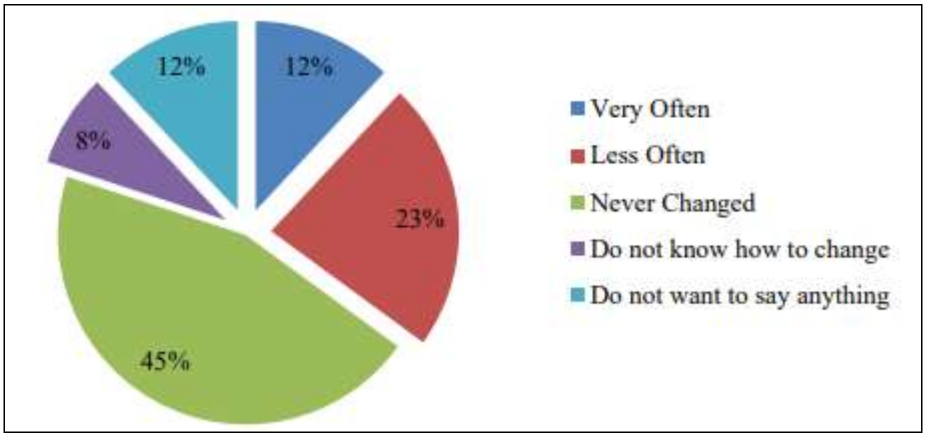

Fig 5. Frequency of changing Passwords

The analysis of above Fig. 5 proves that only 12% respondents regularly change their password to keep their online banking secure from online threats. 23% respondents hardly change their passwords while 45% never changed their passwords since using online banking. The other 8% users are not even aware how to change their passwords of online banking accounts.

Discussion

The conducted survey of this research based on 220 responses made it possible to draw the conclusion of this research. It is important to understand and identify the security issues when dealing with online banking services. The confidence level of the online banking users is measured. When dealing with online banking and other services, it is critical that users must be aware about existing threats coming from computer fraudsters and criminals. Computer fraudsters use different techniques and methods such as computer hacking, phishing, vishing, identify theft, denial of services, social engineering and many more to steal the financial data of end users. It is therefore important that online banking customers must be aware about these techniques and methods used by computer fraudsters. However, only 23% respondents of the survey confirmed that they are aware about all the threats mentioned in the survey of this research. This proves that almost 77% online customers got limited or no awareness about the threats available to individual and banking industry. This further opens doors for computer criminals and fraudsters to access unauthorized customer's information and to utilize them for their illegal activities and objectives. The online banking users need to take extra care when dealing with banking services. However, more than 63% users are unable to identify and handle the existing information security threats. Also, about 65% users do not take any extra care when dealing with online banking services.

Conclusion

Over the last few years, cybercrimes have become more intense, sophisticated and potentially debilitating for individuals, organizations and nations. Law enforcement agencies are finding it difficult to check and prevent the crimes in the cyber space because the perpetrators of these crimes are faceless and incur very low cost to execute a cybercrime whereas the cost of prevention is extremely high. Targets have increased exponentially due to the increasing reliance of people on the internet. Cybercrimes which were restricted to computer hacking till some time ago, have diversified into data theft, ransom-ware, child pornography, attacks on Critical Information Infrastructure (CII) and so on. India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of cyber security and cyber hygiene. As per CERT-IN, one cybercrime was reported every 10 minutes in India during 2017. These statistics are quite alarming and therefore, merit focused and collective attention from Law Enforcement Agencies (LEA's).However, Online banking users should know common security measures to prevent cyber-attacks and to secure their financial data.

Recommendations

Based on the data findings and discussion above, this research recommends the followings;

1. The use of secure application software must be introduced or should be increased to increase the layers of online banking security system.
2. More sophisticated and robust systems must be developed to monitor the activities of computer fraudsters and hackers to make sure that they do not gain any unauthorized access to the financial information of online banking customers. This will alternatively help the business transactions to be accomplished in secure environment.

3. The confidence level of the online banking users must be developed by educating them about the tools and techniques used when dealing with online banking services.
4. The awareness about available online threats must be developed among those users who deal with online banking services and the banking industry must take positive initiatives to achieve this objective.
5. Online banking users should use strong passwords and different user name combinations for different sites and accounts.
6. E-banking customers should be educated more about the importance of secure online banking environment.

References

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.

DeCuir-Gunby, J.T., Marshall, P.L. & McCulloch, A. (2011). Developing and using a codebook for the analysis of interview data: an example from a professional development research project. Field Methods, 23(2), 136 – 155.

Hunton, P. (2009). The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. Computer Law & Security Review, 25(6), 528 - 535.

Jang, Y.J. & Lim, B.Y. (2012). Harmonization among National Cyber Security and Cybercrime Response Organizations: New Challenges of Cybercrime.

Lagazio, M., Sherif, N. & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 1 - 32.

Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS Quarterly, 33(1), 71 – 90.

Manzoor, A. (2014). Protecting Customers Online: Response from Pakistani Banks. International Journal of Science and Applied Information Technology, 3(1), 1 – 7

Martin, N. & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security, 30, 803 – 814.

Saini, H., Rao, Y.S. & Panda, T.C. (2012). Cyber-Crimes and their impacts: a review. International Journal of Engineering Research, 2(2), 202 – 209.

Verma, M., Hussain, S.A. & Kuswah, S.S. (2012). Cyber Law: Approach To Prevent Cyber Crime. IJRREST: International Journal of Research Review in Engineering Science and Technology, 1(3), 123 – 129.