IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, January 2023

A Critical Analysis of Cyber Phishing and its Impact on Banking Sector

Atul Yadav
Shri G.P.M. Degree College of Science and Commerce, Andheri, Mumbai, Maharashtra

Abstract: *The fast development of network communication leads to the expansion of iinformation technology which n turn leads to the influence of access control system n T sectors and banking sectors which sails n to the sea of Network security the most essential scenario n our daily life. So we are n a position to keep the company workers/customers knowledge base up-to-date on any new dangers that they should be cautious about. There are many technologies available to counteract intrusion, but currently no method s absolutely secured. This paper focused on the electronic crime with brief examinations of two cases studies. The study also presented a number of suggestions to assist n tackling policing strategies for further development. The most dangerous frauds that causes n day to day banking activity s phishing, a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity n an electronic communication. According to the latest research, 93 percent of phishing attack specifically involving attempts to rob customers of financial services companies. The aim of this paper s to discuss the various ways by which the phishing affects the internet banking and also discuss the implementation of safety security measures adopted by the users.*

Keywords: Cybercrime, cyber phishing, banking sector, information technology, credit card theft..

I. NTRODUCTION

Computer crimes are criminal activities, which involve the use of iinformation technology to gain an illegal or an unauthorized access to a computer system with intent of damaging, deleting or altering computer data. Computer crimes also include the activities such as electronic frauds, misuse of devices, identity theft and data as well as system interference. The usage of internet services in India s growing rapidly. t has given rise to new opportunities n every field we can think of – be t entertainment, business, sports or education. There are many pros and cons of some new types of technology which are been invented or discovered. Similarly the new & profound technology .e. using of NTERNET Service, has also got some pros & cons. Banking s one of the most risk years as far as privacy s concerned. There are number of ways n which violation of privacy can take place n the banking sector. Phishing s typically carried out by email spoofing or instant messaging n which users are asked to click on the link usually for securing their accounts[3]

These cons are named CYBER CRIME, the major disadvantages, illegal activity committed on the nternet by certain iindividuals because of certain loopholes. The internet, along with ts advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for llegal activities like e-mail espionage, credit card fraud, spams, and software piracy and so on, which nvade our privacy and offend our senses. Criminal activities n the cyberspace are on the rise. The most dangerous frauds that causes n day to day banking activities s phishing, a criminal activity using social engineering techniques. Phishers attempts to fraudulently acquires sensitive information's, such as usernames, passwords and credit cards details, by masquerading a trustworthy entity n an electronici communication.[4]

Aim of the Study

- To understand about the cyber crime
- To analyses and use the preventive measures available to control frauds
- To know the reason for cyber phishing
- To study about the cybercrime and its impact on banking sector

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, January 2023

Cyber Phishing

In this type of crimes or fraud the attackers tries to gain information such as login information or account‟s information by masquerading as a reputable individual or entity n various communication channels or n email. Some other cybercrimes against individuals includes Net extortion, Hacking, ndecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc.

The potential harm of such a malefaction to an individual person can scarcely be bigger.

Cyber extortion and ransomware are also on the rise, although actual loss numbers are less easy to come by as a great many of these attracts go unreportedi(up to 85% of National cyber crimes are not reported).

Cyber Phishing

In this type of crimes or fraud the attackers tries to gain information such as login information or account's information by masquerading as a reputable individual or entity n various communication channels or n email. Some other cybercrimes against individuals includes Net extortion, Hacking, ndecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc. The potential harm of such a malefaction to an individual person can scarcely be bigger. Cyber extortion and ransomware are also on the rise, although actual loss numbers are less easy to come by as a great many of these attracts go unreportedi(up to 85% of National cybercrimes are not reported).

Types and its impact on Banking Sector

Neither crime nor cyber-crime has been defined n PC or information Technology Act, 2000 (hereinafter referred as T Act), but only provides punishment for certain offences. The word „cyber‟ s synonymous with computer, computer systems and computer network. Thus, t can be said that cyber-crime occurs when any llegal activity s committed using a computer or computer resource or computer network.

They are cyber-deceptions, cyber-violence, cyber-pornography and cyber-trespass. The frauds n e-banking sector are covered under cyber-deception. Cyber-deception s further defined as an mmoral activity which includes theft, credit card fraud, and ntellectual property violations. Mostly frauds are committed because of two goals, one, to gain access to the user‟s account and steal his personal information and transfer funds from one account to another. Second s to undermine the mage of the bank and block the bank server because so that the customer s unable to access his account.

The term internet fraud refers to any type of fraud scheme that uses one or more components of the internet- such as chat rooms, e-mail, message boards, or websites-to existing fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to broadcast the proceeds of fraud to financial institutions or to other connected with the scheme.

The term internet fraud refers to any type of fraud scheme that uses one or more components of the internet- such as chat rooms, e-mail, message boards, or websites-to existing fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to broadcast the proceeds of fraud to financial institutions or to other connected with the scheme.

Hacking

Hacking s a crime, which means an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers. The Hacking s not defined n the amended T Act, 200032. But under Section 43(a) read with section 66 of information Technology (Amendment) Act, 2008 and under Section 379 & 406 of Indian Penal Code, 1860, a hacker can be punished. Before the 2008 Amendment Act, Hacking was punishable under Section 66 of the T Act with up to three years of imprisonment or fine which may extend up to two lakh rupees, or both. f such crime s proved then for such hacking offence the accused s punished under T Act, for mprisonment, which may extend to three years or with fine, which may be extended to five lakh rupees or both. Hacking offence s considered as a cognizable offence, t s also a bailable offence.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, January 2023

Credit Card Fraud

There are many online credit card fraud are made when a customer use their credit card or debit card for any online payment, a person who had a mala fide ntention use such cards detail and password by hacking and make misuse of t for online purchase for which the customers card used or hacked s suffered for such kind of attract or action of a fraud made by and evil. The hacker can misuse the credit card by mpersonating the credit card owner when electronic transactions are not secured.

The adjudicating officers, Chennai had directed CICI bank to pay compensation to the customers for an unauthorized withdrawal from a customer‟s bank account. The bank pleaded t as a phishing attack and asserted that the customer had disclosed confidential information and thereby fallen prey to a phishing fraud.

The adjudicating officers, Chennai had directed CICI bank to pay compensation to the customers for an unauthorized withdrawal from a customer's bank account. The bank pleaded t as a phishing attack and asserted that the customer had disclosed confidential information and thereby fallen prey to a phishing fraud.

II. CONCLUSION AND SUGGESTION

The present conceptual framework has provided a bird‟s eye view of ongoing efforts to prevent and control highly technological and computer based crimes, and highlighting general trends and developments within and without the Indian banking sector. This study has described deeply a number of common electronic crimes, dentified n the specific areas of Indian banking sector.

The study has provided an overview to the concept of E-banking by discussing deeply various cyber-crimes, dentified specifically n the banking sector. The Banking system s the lifeblood and backbone of the economy. information Technology has become the backbone of the banking system. t provides a tremendous support to the ever increasing challenges and banking requirements.

Presently, banks cannot think of introducing financial product without the presence of information Technology. However information Technology has an adverse impact too on our banking sector where crimes like, phishing, hacking, forgery, cheating etc. are committed. There s a necessity to prevent cyber-crime by ensuring authentication, dentification and verification techniques when a person enters into any kind of banking transaction n electronic medium. The growth in cyber-crime and complexity of its investigation procedure requires appropriate measures to be adopted. t s imperative to increase the cooperation between the stakeholders to tackle cyber-crime. Many organization have developed anti-phishing solutions, the usage of these security tools may be encouraged through regulation. In addition, small organization should be supported by states n making their electronic transactions secure.

Indian banking sector cannot avoid banking activities carried out through electronic medium as the study suggest that there has been an ncrease n the number of payments n e-banking. However, the change n the banking ndustry must be such which suits the ndian market. Banks are required to be updated and ahead with the latest developments n the T Act, 2000 and the rules, regulations, notifications and orders ssued therein pertaining to bank transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic funditransfer etc. as part of overall operational risk management process. t s the need of the hour to ncrease cooperation between the countries, over the tools and techniques, which will help them effectively, counter global electronic crime. n developing countries, like ndia, cyber and electronic crime poses a serious problem because there s a lack of training on the subjects related to nvestigation of electronic and cybercrimes. Lastly, t can be concluded that to eliminate and eradicate cybercrime from the cyberspace s not a seemingly possible task but t s possible to have a regular check on banking activities and transactions. The only propitious step s to create awareness among people about their rights and duties and to further making the mplementation of the laws more firm and stringent to check crime.

REFERENCES

[1] Krebs, brian. “phishing scemes scars victims”, washingtonpost.com, nov 18, 2004

[2] Hannan.M& Blunde;;. B (2004). “electronic crime- t not only the big end of town that should be worried”’ we-B centre & edith cowan university, PP 1-9.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, January 2023

[3] Privacy and banking : Do ndian banking standard provides enough privacy protection? The nternet and society available at www.cisinida.org
[4] Perumal, subramoniam Arumuga, mpact of cyber crime on virtual banking (ovt 24,2008) available at www.ssrn.com
[5] Muthukumaran.B (2008), "cyber crime scenario n ndia", criminal investigation department Review, January, pp. 17-23.
[6] www.cyberlawsindia.com
[7] Kumar. A (2002) "cyber crime- crime without punishment", available at unpanl.un.org.
[8] cyber extortion risk report 2015, NYA nternational, oct 2015