National Conference on Latest Innovations and Future Trends in Management
ISSN: 2349-6002

A Study on Cyber Security Issue Affecting Banking And Online Transactions

M Sravika
MBA II Year, Sridevi Women's Engineering Collage

Abstract **- In the era of globalization Internet banking or online banking has revolutionized integral activity of our modern twenty first century. The man developed various ways for communication to the exchange of information, ideas and knowledge which is of great importance to him as a social being. The evolution of e-banking technology makes the task very easy, banking transactions becomes very fast within a click. Online and mobile banking make daily banking fast and convenient. The misuse of information technology in the cyber space is clutching up which gave birth to cyber crimes at the national and international level. The percentage of risks and the challenges associated with it is increased. However online and mobile banking is never 100 per cent safe. The purpose of this research paper is to review cyber attacks. In this paper we focused on cyber crimes related to online banking and new tricks and techniques used by hackers. The study totally based on the secondary data. The findings of this research paper shows that the IT usage and cybercrime related to online banking in India are on the rise. Majority of the cybercrimes have been committed by young people in the age group 18-30and are male gender. Our law enforcement agencies need to be adequately equipped to overcome and prevent the cyber crime. Finally researcher has given some suggestions for the prevention and safety use of online banking services.**

Index Terms **– Information Technology, cyber crimes, cyber attacks, mobile banking, online banking, National Crime Record Bureau, hacking.**

I.INTRODUCTION

Information technology has played very important role in the field of banking. Online banking or e-banking is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society.

Banking in India in modern sense originated in the last decades of the 18th century. Since that time the banking sector applying different ways to provide facilities to a common man regarding to money. The banking sector is totally changed after the arrival of Internet especially in terms of security because now money is in our hand on a single click. User has number of choices to manage his money with different kind of methods.

E-banking implies provision of banking products and services through electronic delivery channels. It is method of banking in which the customer conducts transactions electronically via the Internet. It is also known as electronic funds transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by check or cash.

The high connectivity to the world from any place has developed many crimes and these increased offences. Cyber Crimes Attack is also called Computer Network Attack is an attack from one computer to another computer using a network deliberately to alter, disrupts, deny, degrade or destroy or damage the data hosted in the attacked system or network. The interrupter interrupts by producing a malicious code which is directed against a computer processing code or logic. These attacks are made in a way to steal the relevant information without leaving back any traces of intrusion.

Financial crime, also referred as white-collar crime, covers a wide range of criminal offences which are generally international in nature. Cyber attacks generally refer to criminal activity conducted via the Internet. These crimes affect private individuals, companies, organizations and even nations, and have a negative impact on the entire economic and social system through the considerable loss of money incurred. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses

on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure. The loss or misuse of information assets is the most significant consequence of a cyber attack.

OBJECTIVES

1. To study the categories of cyber crimes in banking sector.
2. To analyze the challenges of cyber security in digital banking
3. To analyze Present Security Systems for Online Banking
4. To analyze solution for the threat of Cyber security in digital banking

A.CATEGORIES OF CYBER CRIMES IN BANKING SECTORS

1.Viruses and worms

Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.

2. Spam emails

Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver— potentially creating a wide range of problems if they are not filtered appropriately.

3. Trojan

A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk

4. Denial-of-service (DoS)

DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.

5. Malware

Malware is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a botnet a network of computers controlled remotely by hackers, known as herders to spread spam or viruses.

6.Scareware

Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses

7.Phishing

Phishing attacks are designed to steal a person's login and password. For instance, the phisher can access the victims bank accounts or assume control of their social network.

8.Fiscal fraud

By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits

9.State cyber attacks

Experts believe that some government agencies may also be using cyber attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an invisible attack on Iran's secret nuclear program. The virus was aimed at disabling Iran's uranium enrichment centrifuges.

8. Carders

Stealing bank or credit card details is another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops.

B.CHALLENGES OF CYBER SECURITY IN DIGITAL BANKING

Some of the factors have posed a serious challenge to the Cyber security in digital banking.

1.Lack of Awareness

Awareness among the people regarding the Cybersecurity has been quite low, and not many firms

invest in training and improving the overall Cybersecurity awareness among the people.

2. Inadequate Budgets and Lack of Management

Cybersecurity is accorded low priority; therefore, they are most of the time neglected in the budgets. Top management focus also remains low on Cybersecurity, and support for such projects is given low priority. This may be because they misjudge the impact of these threats.

3. Weak Identity and Access Management

Identity and access management has been the fundamental element of Cybersecurity and especially in these times when the hackers have the upper hand; it may require only one hacked credential to enter into an enterprise network. There has been a slight improvement in this regard, but still, a lot of work remains to be done in this area.

4. Rise of Ransomware

The recent events of malware attacks bring our focus to rising menace of ransomware. Cybercriminals are starting to use methods that avoid them to be detected by endpoint protection code that focuses on executable files.

5. Mobile devices and Apps

Most of the banking institutions have adopted mobile phones as a medium to conduct business. As the base increases each day, it also becomes the ideal choice for exploiters. Mobile phones have become an attractive target for hackers as we see a rise in mobile phone transactions.

6. social media

Adoption of social media has led to hackers to exploit even more. Less aware customers put out their data for anyone to see which is exploited by the attackers.

C. PRESENT SECURITY SYSTEMS FOR ONLINE BANKING :

1. User id & Transaction Password:

Firstly, New York introduces online banking using user id and text password in the early 1980s. To access online banking facilities, a customer have to register himself with a unique id and password for user verification . The new User id must be 6 to 19 characters and the password must be 8 to 17 characters and must contain at least 2 alpha and 2 numeric characters. Customer can set security data to email address, Security Queries, Authentication Pass Phrase & Computer Registration. Now, user can access and take full benefits of internet banking services

2. OTP:

One-Time Password (OTP) Service Using Mobile Phone Applied to Personal Internet Banking was implemented first time in japan, 2007. This is an authentication service that makes use of an OTP in addition to the conventional ID and password for personal identification. User can use this OTP for better security during online transaction by downloading special password-generation software to their mobile phone. User can perform authentication by entering an OTP displayed by the mobile phone application in addition to their normal ID and password. The one-time passwords are specific to each user, and a new password is generated every minute. Even if the password is obtained by a third party fraudulently, it cannot be used outside its lifetime

3. QRP: code –

QRP that is Quick Response Protocol, is a secure authentication system that uses a two-factor authentication by combining a password and a camera equipped mobile phone, where mobile phone is acting as a authentication token. It is very secure and also very easy to use for encrypted data. It is very secure protocol for use on untrusted computers.

4. Biometric:

Biometric is specifically used for secure ATM transaction. In such a transaction, the use of a biometric mechanism such as iris/retinal scan, hand geometry or fingerprint scan can greatly improve overall security. All customers need to do is register their biometric information at a bank's branch. Then they will be able to withdraw money from ATM by just providing their biometric password and providing their date of birth and Pin number. Currently there are 80,000 biometric enabled ATMs in japan used by more than 15 million users

5. OTP and QR code:

To eliminate threat of phishing and to confirm user identity the system with the combination of OTP and QR code was developed. QR-code can be scanned by user mobile device which overcome the weakness of traditional password-based system. This improves more security by using one time password (OTP)

which hides inside QR code. shows the flow of this type of authentication system

6. Grid Authority Card:

Grid authority Card is a card that helps in preventing the fraud at the initial stage itself such that the fraud could not take part. In this system, the customer submit his/her credit card credential along with the respective Grid Characters on the grid card associated with the credit card. Grid card contains the alphabets associated with the numeric numbers printed on it. These grid codes are generated randomly by the user interface application through which the customer is connecting to the Payment Gateway via secure internet connection. Without the Grid Card, no one can do the online payments in case of credit card theft or lost. It helps in get rid of online frauds. The sample of ICICI grid card is as shown in the figure

7. E-Token:

E-Secure Token provides an additional security feature when logging on to Internet Banking. The E-Secure Token provides a "One-Time-PIN" (OTP), which should be used to access the Internet Banking sites, together with username and password. Each OTP is only valid for one session; therefore, the E-Secure Token should be used to generate an OTP with every login. To obtain login OTP user have to switch on his E-Secure Token using the On/Off Button. Then he have to enter his 4 digit secret pin. User's E-Secure Token LCD screen message will then display his login OTP. Security Question: Based on research for multifactor authentication (MFA) and fraud risk mitigation, the verification process was strengthened for Internet Banking users by reducing the number of opportunities to correctly answer security challenge questions. Previously, users selected three security challenge questions to be present during MFA and had up to five prospects to correctly answer those questions. Specifically, a user was presented the first security challenge question and had two opportunities to answer properly. If the user didn't provide the correct

D. SOLUTIONS TO THE TREAT OF CYBER SECURITY IN DIGITAL BANKING :

1. Make certain you have the up-to-date security updates:

From time to time, flaws are discovered from the Programs running on your computer. These flaws can be misused by any black hate community member to gain access to workstations. As such, publishers will issue updates to correct these flaws.

2. Install effective anti-virus software:

You may already using anti-virus software, but the software should be updated regularly to provide complete system protection. There are various effective plans to select from, but the most common profitable products contain Symantec, McAfee, Trend Micro, Sophos and F-Secure. It is also credible to use free anti-virus shield from Microsoft Security Essentials, Grisofts AVG, Avast and Clam Win. However, be aware to visit the genuine site as there are number of forged products claiming to safeguard your system.

3. Use a personal firewall:

It is a minor program that assistances to protect your workstation and its contents from unknowns on the internet. When mounted and properly and configured, it stops unauthorized traffic to and from your workstation. There are many effective plans to choose from. Common viable examples include Check Point Zone Alarm (free) and Windows Firewall, Norton Personal Firewall and McAfee Personal Firewall.

4. Use an anti-spyware program:

This is actually used to define programs that run on your workstation which monitor and record the way you surf the internet and the sites you visit. It can also be downloaded deprived of your permission or awareness and used to see personal data that you have entered online, counting passwords, telephone numbers, identity card numbers and credit card numbers. Anti-spyware programs currently available include Ad Aware, Microsoft Defender (free), Spyware Blaster, Spy Sweeper, Microsoft Defender (free), Spyware Blaster and Sunbelt Software Security Spy.

5. Block spam e-mail:

Spam e-mails are specially used for phishing attacks, tempting you to click on links that can directly download malware to your computer or direct you to a fake website. That's why, for security purpose it is better to remove any e-mail form an unrecognized source as soon as possible. A spam filter is there which can separate spam e-mail in separate spam folder, so that you can easily identify it. Removing unwanted

spam without reading will protect your system from phishing attack.

6. Be aware to potential fraud:

Be alert that there are some fake websites designed to pretend you and gather your private data. Sometimes links to such websites are enclosed in e-mail messages asserting to come from financial institutions or further trustworthy organizations. Never monitor a link enclosed in an e-mail, even if it seems to come from your bank.

7. Keep your passwords secure:

Keep your password to yourself only, Make them hard to guess, differ them: Try to use unlike passwords for different services, Change your passwords frequently and never write them down.

8. Be cautious where you go online:

Avoid using Banking or any other internet facilities that necessitate passwords at internet cafe's, libraries or any other public sites to avoid the risk of information being copied and abused later you leave.

9. Always log off:

Always remember to log off from banking site and close your browser after completion of your online banking. This will remove all traces of your stopover from the workstation's memory.

10. Password-protect your computer:

Never forget to give a strong administrative and master password to your computer. This will avoid other customers from using it if it is stolen or left unattended.

11. Don't use administrator mode:

Don't use administrative mode because anyone who gain access to it will then have nearly boundless rights to see downloaded software or stored information. It's far superior to make a user account and log in with that for everyday usage

CONCLUSION

Cyber security in digital banking is something that cannot be compromised with. With the growth in the digitalization in the banking industry, it has become more prone to attacks from cybercriminals. Therefore there needs to be a foolproof Cyber security that doesn't compromise with the safety of customer's and financial institution's data and money. From an operational perspective, this study indicates that Internet banking allows customer to conduct transaction any time and thus it reduces the number of physical visit to a bank and it has reduced the cost per transaction. But, technologically, implementing web-based banking system is challenging to the customer. Hence Cautious planning is a prerequisite and full assistance are to be realized. In our study we have found that different technologies have played an important role to control the risk factors through Authentication system.

REFERENCE

[1] Sven Kiljan, Harald Vranken, Koen Simoensd, Danny De Cocke, Marko van Eekelena, "Technical report: security of online bankingsystems" Open University, Netherlands, February 10, 2014

[2] http://en.wikipedia.org/wiki/Online_banking

[3] Rajpreet Kaur Jassal1 , Dr. Ravinder Kumar Sehgal, "Comparative Study of Online Banking Security System of various Banks in India "International Journal of Engineering, Business and Enterprise Applications (IJEBEA) 6(1), September-November., 2013, pp. 90-96

[4] http://en.wikipedia.org/wiki/Internet_safety

[5] https://www.hsbc.com/internet-banking/types-of-online-attack

[6] "Online Banking Quick Reference User Guide" Community Banks of Colorado, N.A. Rev. 05/12

[7] "One-Time Password Service Using Mobile Phone Applied to Personal Internet Banking for the First Time in Japan" NTT data corporation, June 18, 2007

[8] Sonawane Shamal1, Khandave Monika, Nemade Neha, "Secure Authentication for Online Banking Using QR Code" International Journal of Emerging Technology and Advanced Engineering(IJETAE), Volume 4, Issue 3, March 2014

[9] Abhishek Gandhi, Bhagwat Salunke, Snehal Ithape, Varsha Gawade, Prof. Swapnil Chaudhari, "Advanced Online Banking Authenticatio System Using One Time Passwords Embedded in Q-R Code" International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 5 (2), 2014.

[10] Nayani Sateesh, "An Approach For Grid Based Authentication Mechanism To Counter Cyber

Frauds With Reference To Credit Card Payments" Global Journal of Computer Science and Technology(GJCST), Volume 11 Issue 1 Version 1.0 February 2011

[11] Abhishekh Kumar Sinha, "Financial transaction get personalized and secure with biometrics"

[12] "E-secure manual", Bank Windhoek

[13] "Enroll and manage Security Questions for Multifactor Authentication