International Journal of Scientific Research in Computer Science and Engineering **Review Paper**
Volume-5, Issue-1, pp.41-44, February (2017) **E-ISSN:** 2320-7639

Security Issues on Online Transaction of Digital Banking

Wakil Ghori

Indore Indira School of Career Studies, Indore (MP), India

Available online at: www.isroset.org

Received 21st Dec 2016, Revised 5th Jan 2017, Accepted 01th Feb 2017, Online 28th Feb 2017

***Abstract*— Digital banking system has a broad range of benefits that add value to customer's fulfillment in term of superior service quality, and at the same time it enables banks to add a competitive benefit over other financial competitors. Presently, Digital banking customers only require a smart gadget with access to the Internet to use digital banking services. Customers can access their digital banking accounts from anywhere in the world. However, more attention towards digital banking security is required and needed against fake behavior because the lack of control over security policies makes digital banking still untrusted for many customers till now. This paper presents challenges and security issues related to digital banking. Various types of cyber attacks, fraud strategies, and prevention methods used by digital banks, are also presented in this paper. This research work studies security and safety issues of online banking.**

***Keywords*— Digital Banking, Hacking, Rootkits, Phishing, encryption, OTP, QR code**

I. INTRODUCTION

At the basic level, Internet banking can mean the setting up of a web page by a bank to give information about its products and services. At an advanced level, it involves provision of facilities such as accessing accounts, transferring funds, and buying financial products or services online as well as new banking services, such as electronic bill presentment and payment, which allow the customers to pay and receive the bills on a bank's website[1].

Now, Digital banking is not a new phenomenon anymore as more and more financial institutions and banks worldwide adopting this system[2]. The most outstanding feature to online digital banking is its convenience. People are always too busy to spend their precious time standing in line at banks queue. Online banking provides them the ability to carry out banking transactions in the comfort of their homes or offices digitally. People can do banking transactions sitting at home, at office, or lying on their bed midnight as this can be done through computers or mobiles. There no time boundation to do banking operation and no need to move to bank premises in order to open new bank account, check account balance and make funds transfer. Today banks with Digital banking experience provide more complicated online financial services, due to that digital security and privacy issues are of high concern. So banks should provide more safe and secure digital banking services.

The Information Technology revolution has brought stunning in the business environment. Perhaps no other institutions or organization has been influenced by advances in technology as banking and financial institutions[3]. As a result the banking sector cause a totally new looks in today scenario. Electronic funds Transfer, Electronic clearings System, Automated Teller Machine (ATM), Tele-banking, Mobile banking and Net banking are widely in use.

Digital Banking is one of the gifts of technology to human beings. E-Banking is a fast spreading service that allows customers to use computer and mobile to access account transactions from a remote location. Digital banking is also extremely beneficial to the banks as they do not have to acquire large office area or hire additional staff to deal with customer demands. Internet digital banking is also extremely beneficial for the environment since it reduces paper usage for one. The popularity of online banking is good news not only for us and financial institutions but also for cyber criminals, who keep eye on online banking customers[4]. Security is the major disadvantage with digital banking. Although all the security features and encryption software placed with your account, there will always be hackers who are smart enough to get into your account and misuse it, take money. Identity theft is one of the main drawbacks of online banking.

Rest of the paper is organized as follows: In section II, the information related security threats in Online digital banking is given. Section III includes the information on security tips for safe online digital banking. In Section IV, we have mentioned the points to improve the internet security. In Section V, we have given the short summarization of the related work. In Section VI we have proposed some suggestions and recommendations. Section VII concludes the paper with future scope.

II. ONLINE DIGITAL BANKING SECURITY THREATS

The Commercial Banks have been facing lot of problems due to Online Banking Crimes. Some of them are enumerated below.

- Malicious Software
- Virus/Worm (Programmes that self replicate or are sent over the internet by emails and can damage your PC)
- Trojans (Programmes that compromise computer security by intercepting password without known to user)
- Man-in-the-Middle (MITM) Attacks
- Phishing (Using a false name, website and address for fraudulent purpose)
- SMSishing (SMS phishing)
- Vishing
- Keylogger
- Rootkits (malicious software giving unauthorized administrator level access without the real administrator noticing)
- Unauthorized Access (Hacking)
- Credit Card Fraud
- Cross-Site Scripting
- Password Guessing
- Website Spoofing
- Pharming (Redirect the users to a fraudulent purpose)
- Unencrypted Transmission of Data

III. IMPORTANT SECURITY TIPS FOR SAFE ONLINE DIGITAL BANKING

- There are a number of steps we can take for an extra layer of protection to keep us safe online.
- Protect your computer and mobile devices with up-to-date security software and install regular security and software updates.
- Only use official Mobile Banking apps and only download apps from an official app store.
- Never log in to Online Banking through a link in an email.
- Create password (or PIN) that is hard to guess. Change your PIN or password immediately if you think someone may have discovered it.
- Don't give anyone your security details and never write them down or store them on your mobile in a way that might be recognized by someone else.
- Never give your Personal Identification Number (or password) and full security details to anyone who call you, and never reveal them in an email or text message.
- Be cautious of opening attachments or links in emails that you were not expecting or are unsure about.
- Banks or Financial Institutions never call you and ask you to transfer money, so ignore such calls.
- If your phone is lost or stolen, call your bank so they can disable your Mobile Banking apps as a precaution.
- Access your bank website only by typing the URL in the address bar of your browser.

IV. HAVING THE FOLLOWING WILL IMPROVE INTERNET SECURITY

- Install newer version of Operating System with latest security features.
- Update Antivirus definition.
- Always use latest version of web Browsers.
- Firewall is enabled.
- Antivirus signatures applied.
- Scan your computer regularly with Antivirus to ensure that the system is Virus/Trojan free.
- Change your Internet Banking password at periodical intervals.
- Always check the last log-in date and time in the post login page.
- Avoid accessing Internet banking accounts from public places such as cyber cafes or shared PCs.
- Use OTP (One Time Password) from sensitive digital transaction.

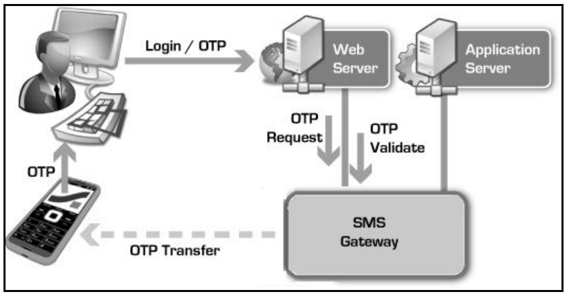

Figure 1 Sample Image of OTP generation process

- Use QR code (Quick Response Code) for fund transfer

Figure 2 Sample Image of QR code-Scanning

V. RELETED WORK

- Online banking has become increasingly important to the profitability of financial institutions as well as adding convenience for their customers. As the number of customers using online banking increases, online banking systems are becoming more desirable targets for criminals to attack. To maintain their customers' trust and confidence in the security of their online bank accounts, financial institutions must identify how attackers compromise accounts and develop methods to protect them. The unique aspect about security in banking industry is that the security posture of a bank does not depend solely on the safeguards and practices implemented by the bank, it is equally dependent on the awareness of the users using the banking channel and the quality of end-user terminals.[5]
- Emeka Nwogu and McChester Odoh, in their paper "Security Issues Analysis on Online Banking Implementations in Nigeria", have given With the help of Internet banking, many transactions can be executed by the account holder. When small transactions like balance inquiry, record of recent transaction, etc. are to be processed, the Internet banking facility proves to be very handy. The concept of Internet banking has thus become a revolution in the field of banking and finance[6].
- Tejendra Pal Sing Brar mention in his paper that - Electronic Banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The use of Electronic Banking has brought many concerns from different perspectives: government, businesses, banks, individuals and technology[7].
- Panida Subsorn and Sunsern Limwiriyakul, introduce their paper with words "Most industries have deployed internet technologies as unessential part of their business operations. The banking industry is one of the industries that has adopted internet technologies for their business operations and in their plans, policies and strategies to be more accessible, convenient, competitive and economical as an industry. The aim of these strategies was to provide internet banking customers the facilities to access and manage their bank accounts easily and globally. Nevertheless, there are inherent information security threats and risks associated with the use of internet banking systems that can be variously classified as low, medium and high. In particular the confidentiality, privacy and security of internet banking transactions and personal information are the major concerns for both the banking industry and internet banking customers"[8].

VI. SUGGESTION AND RECOMMENDATION

The following suggestions are recommended for enhancing digital banking services of banks to the customers

- Banks should take essential steps to make awareness among people about the advantages of digital banking services available in the banks.
- Many bank customers have not availed of the internet banking services because they do not trust the internet channel presuming it as complicated. So banks should train the customers to get acquainted with the system.
- Internet banking is convenient and easy to use, but customers are afraid of adopting these services because they think that using these services is complicated. So, bank personnel should provide on-site training to the bank customers who intend to use online banking services.
- Banks should regularly improve their internal security mechanism to provide privacy and security to the customer's transactions.

V. CONCLUSION AND FUTURE SCOPE

Security is the most significant issue in digital banking. There are many ways to have a secure communication via computer and mobile networks today. It may occur in form of risk in case of unauthorized access of information of bank account. Many customers are still not comfortable with online system, especially from the security point of view. In addition to this, financial institutions and banks also face the domestic problems like employee frauds. Many customers hesitate to deal with an online banking system as they are not sure of products and services quality which they will receive from banks. Banking system may also face problems due to wrong choice of technology, insufficient Control and inappropriate system. Wrong selection of technology may cause financial loss, so it is always recommended to follow the security measures as suggested.

With the expansion of the security technology and mechanism of the Internet banking, as well as the continuous improvement of the security solutions of the Internet banking systems, the Internet banking is becoming more and more secure, and there will be a board market of digital banking with secure services.

REFERENCES

[1] Rajpreet Kaur Jassal and Ravinder Kumar Sehgal, "Online Banking Security Flaws: A Study", International Journal of Advanced Research in Computer Science and Software Engineering, Volume-03, Issue-08, ISSN-2277 128X , August 2013.

[2] Elbek Musaev and Muhammed Yousoof, "A Review on Internet Banking Security and Privacy Issues in Oman", ICIT 2015- The 7th International Conference on Information Technology, January 2015.

[3] Mr. Shakir Shaik and Dr. S.A. Sameera, "Security Issues in E-Banking Services in Indian Scenario", Asian Journal of Management Sciences, Volume-02, Issue-03, pp.(28-30). ISSN: 2348-0351, March 29, 2014.

[4] 'Security features in Internet Banking', newagebanking.com/finsec/modernizing-digital-security-to-protect-banks-from-fraud/, Jan 16, 2017

[5] Kenneth Edge, "The Use of Attack and Protection Trees to Analyze Security for an Online Banking System", HICSS 2007-40th Annual Hawaii International Conference on System Science, Online ISSN: 1530-1605

[6] Emeka Nwogu and McChester Odoh, "Security Issues Analysis on Online Banking Implementations in Nigeria", International Journal of Computer Science and Telecommunications, Volume-06, Issue-01, ISSN 2047-3338, January 2015,

[7] Tejinder Pal Singh Brar, Dr. Dhiraj Sharma, Dr. Sawtantar Singh Khurmi, "Vulnerabilities in e-banking: A study of various security aspects in e-banking", International Journal of Computing & Business Research, ISSN (Online): 2229-6166

[8] Panida Subsorn and Sunsern Limwiriyakul, "An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia: A Customer Perspective", IJCSI International Journal of Computer Science Issues, Vol. 09, Issue 02, ISSN (Online): 1694-0814, March 2012.

AUTHORS PROFILE

Wakil Ghori received Bachelor of Computer Science (Honours) Degree in 2000 and Master of Computer Management (MCM) in 2003 from Devi Ahilya University, Indore (MP). He pursed MCA from Institute of Advanced Studie in Education (Deemed University), Rajasthan in 2003. He was worked as Assistant Professor in Govt. Holkar Science College from 2004-2006 and also worked in Renaissance College of Commerce and Management from 2006-2012. He is presently working as an Assistant Professor at Indore Indira School of Career Studies, Indore (MP) since 2012 till date. His areas of interest are Computer Programming, Digital Electronic, DBMS, Computer Networking.

Email:wakilghori47@gmail.com