IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Security Measures for E-Banking Transactions

Mrs. M. AMBIGA[1], Mrs. C. MEENA[2]

Assistant Professor, Department of Computer Science, Parvathys Arts and Science College, Dindigul, Tamilnadu, India

Assistant Professor, Department of Computer Science, Parvathys Arts and Science College, Dindigul, Tamilnadu, India

ABSTRACT : This paper attempts to make awareness among customers towards internet banking. With online banking, cyber criminals simply need to ascertain certain personal information to break into a person's account and steal their money. So, security is still a major issue for online banking transactions. In order to predict the banking data from the hackers, the customers have to be aware of precaution measures. The significance of the study of this paper is to give valuable suggestions to improve awareness and satisfaction towards E-banking and services.

KEYWORDS: Skimmers, Scams, Jailbroaken

I.INTRODUCTION

Internet banking refers to the banking services provided by the banks over the internet. The online services offered might differ from bank to bank, and from country to country. The common **online services** offered by banks are the t**ransactional activities** like funds transfer, bill pay, loan applications and transactions and n**on-transactional activities** like request for cheque book, stop payment, online statements, updating your contact information.

Internet banking is performed through a computer system or similar devices that can connect to the banking site via the internet and it can be also be accessed through mobile phones using a Wi-Fi or 3G connection. The popular software are Apex, ASPECT Microfinance Software, Finacle, Key Bank, Olympic, TCS BaNcs etc., used to design the banking transaction system. We have various banking strategies such as home banking, Telebanking, Internet Banking, Mobile Banking tec.,[6].

How the Online banking system works

Online banking is carried out in four main phases illustrated here

.

1.The computer's user runs on the installed operating system.
2. After the web-browser opened, users can access the bank's website and then enters the personal identifying number (PIN) and the password by using the keyboard.
3. The data input is encrypted by SSL (secure socket layer) and transmitted to the bank's server.
4. The bank's server decrypts the transmitted information and processes of the user's authentication.

Pros and Cons of Internet Banking

Online banking has increased in popularity over the past few years due to various reasons. Now, people don't need to walk down to the banks to get the transactions done. They can manage almost everything right from their computers, laptops or smart phones. Moreover, internet technology never sleeps, the bank may have fixed working hours, but internet works 24×7 and from anywhere. Whether a person is out of city or even out of country, his/her transactions will take place the way he/she wants. It takes just a few seconds, almost like a blink of eye, our transactions are processed. It takes just a few seconds, almost like a blink of eye, your transactions are processed.

As far as our security is concerned, it is one of the most significant challenges for online banking transactions. Online bankers are one of the most favorite (sometimes easiest) targets of hackers. Bankers, in case of lacking internet connection can find themselves unable to transact. Those who lack awareness about the safety measures of online banking are easy target for hackers and intruders. Moreover, as compared to traditional banking method, online banking lacks security as your card details can be stolen.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Technology has both pros and cons, and online banking is no exception. Safer you make use of it, better and easier your life becomes. Summing it up, there may be more pros and cons of online banking, but these are some important ones.

Security Issues in Online Banking Transactions

Currently there is a clear need for efficient security procedures by banks which offer online access to their systems. Several new security technologies and procedures which aim at providing authenticated secure communication against the number of malware that exploit online banking system vulnerabilities. In general, it is first necessary to understand and determine the existing attack methods and vulnerabilities on which they are based. Hence, the attack strategies and techniques can be divided into three main vectors that can be used against online banking systems, such as:

Firstly, a credential stealing attack (CSA), is where fraudsters try to gather users' credentials, either with the use of a malicious software or through phishing.

Secondly, a channel breaking attack (CBA), involves intercepting the communication between the client side and the banking server, by masquerading as the server to the client and vice versa.

Thirdly, a content manipulation also called man-in-the browser (MiTB) attack, it takes place in the application layer between the user and the browser. The adversary is granted with privileges to read, write, change and delete browser's data whilst the user is unaware about it.

It is well-known that attacks against online banking systems are mostly cases dangerous. Therefore, the online banking systems should be imposed an effective security procedures capable of identifying users (finger print, reading iris data) and authorize a variety of transactions, thus mitigating fraud.

Security Precautions

In order to make their bank account safe, one should follow certain security precautions. Customer should never share personal information like PIN number, passwords etc. with anyone, including employees of the bank. Customers are also advised not to provide sensitive account-related information over unsecured e-mails or over the phone. It is also important to ensure that the logged in session is properly signed out. Banking Sector provides some the following suggestions to be made by the customers to make things much harder for criminals and to significantly lower your safety risks. Always use a pin or gesture code to lock mobile devices, Only use official routes to communicate with financial institutions, Be aware of connection services, be careful what you download, read the fine print, Set up your phone to encrypt data, Download anti-virus software and enable firewall protection for your cell phone, never respond to email messages from your bank that request personal information. Be skeptical about text messages. Sign Off When Done, etc.,

Bank Account Safety Tips for Preventing Fraud[4]

Keep your PIN and passwords secret, Use a strong password for online banking, Change passwords periodically, Do not give out account info over the phone, Do not give out account info through email, Don't click links embedded in emails, Use anti-virus protection software, firewalls and spyware blockers, Don't use public computers for online banking, Check for secure connections, Report lost cards immediately, Be aware of your surroundings at ATMs, Watch out for skimmers, Take your receipt. Shred documents and old checks. Minimize check writing, Write checks in permanent blue ink, Do not leave blank space on your check, Make sure checks can't be seen through envelopes, Use secure mailboxes only.

The various services covered under E-Banking are[3];

Automated Teller Machines (ATM)

Credit Cards, Debit Cards, Electronic Funds Transfer (EFT) System, Mobile Banking, Internet Banking, Tele-banking, Home banking, Demat facility and Cheques Truncation Payment System,

Automated Teller Machine (ATM)

An ATM is a computerized Tele-communication device which enables the customers to perform several banking operations such as withdrawals of cash, request of mini-statement etc.

Credit Cards

A credit card is a small plastic card issued to users as a system of payment

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Debit Card

A debit card (also known as a bank card or check card) is a plastic card that provides the cardholder electronic access to his or her bank account/s at a financial institution.

Electronic Transfer of Funds

Bank customers can buy goods and services without caring cash by using credit or debit cards. The Customer swipes the card by using the card reader device to make the transactions.

Tele-Banking

A customer can do non-cash business related banking over the phone anywhere and at any time.

Home Banking

The customers can perform a no. of transactions from their home or office.

Internet Banking

Internet banking means any user or customer with personal computer and browser can get connected to his banks website and perform any service possible through electronic delivery channel. All the services listed in the menu of bank website will be available.

Demate Banking

It is nothing but de-materialization.. The customer who wants to invest in stock market or in share and stock needs to maintain this account with the commercial banks.

Cheques Truncation Payment system (CTPS)

Truncation is the process of stopping the flow of the physical cheque issued by a drawer to the drawee branch.

Mobile Banking: It is another important service provided by the banks recently. The customers can utilize it with the help of a cell phone. The bank will install particular software and provide a password to enable a customer to utilize this service.

Mobile Banking is said to be more secure and risk-free than online Internet Banking. The ways which I mentioned in this paper can assist you at a great extent to make awareness against threats as well as to make the banking mobile apps safer.

II.VARIOUS WAYS TO STRENGTHEN MOBILE BANKING SECURITY[1]

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

1. Introduce device fingerprinting

To determine the integrity of the device and helps to confirm a user identity by using the unique set of signals obtained from the device. Such signals usually include IP address, location, screen size, browser, time of day, device type, etc.

2. Implement SIEM solutions

Mobile banking protection with a SIEM system allows identifying a large number of risks, anomalies and malicious behavior, such as jailbroken or rooted device, device is connected to an insecure Wi-Fi network, device is running an emulator, access from foreign countries, high velocity of recent logins, escalation in bad login attempts and other unusual circumstances, etc.,

3. Add multi-factor authentication

To increase mobile banking security, banks should add an additional layer of defense, such as generated one-time passwords or biometric authentication. While static biometrics analyzes peoples' physiological characteristics, such as fingerprints, iris, retina, etc., behavioral biometrics deals with a person's voice, typing rhythm, scroll speed, swipe patterns, and other traits revealing the unique ways people interact with their devices.

4. Offer real-time text and email alerts

By adding security alerts to your mobile banking functionality, Such alerts allow a bank to notify consumers:

1. When big purchases happen
2. When a customer's profile or password changes
3. When an ATM withdrawal exceeds a certain amount
4. When a customer's account balance drops below a specific amount
5. When any debit card purchase occurs, etc.

5. Proactively educate your customers

Banks that offer mobile banking apps to their customers should also educate them how to protect themselves from any fraudulent activity.

III. CONCLUSION

The providers of online banking services should be more responsive to security requirements, and makes the online transaction have a layered protection against security threats. The necessity for a strong authentication solution became inevitable in banking services because of the growing pace of the transition technology adoption along with the unfortunate rise in fraud and security breaches. Two factors may be considered to provide more security than the existing one in ATM Machine is fingerprint (Biometrics) and capturing iris along with ATM PIN (Permanent Account Number) are important to increase security and reduce the stealing of customer data. When implemented, these factors are almost impossible for fraudsters to mimic.

Banks should take the security considerations as part of their service offerings in future, to take precautions for a more secured online banking experience by the customers.

REFERENCES

1. https://www.google.com/search?ei=_HJ_XILhEYme_Qb4-p-YCg&q=5+ways+to+strengthen+mobile+banking+security&oq=5+ways+to+strengthen+mobile+banking+securit2
2. http://www.ijcst.com/ijmbs/research1
3. http://dailytools.in/BankingKnowledge/EBanking
4. https://www.epnb.com/blog/20-bank-account-safety-tips-for-preventing-fraud/
5. https://lieu.house.gov/media-center/in-the-news/bank-info-security-bank-account-hackers-used-ss7-intercept-security-codes
6. https://www.softwaresuggest.com/accounting-software

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details