Net Banking and Banking Frauds

Shashikala K

Assistant Professor

Department of Commerce

Govt. First Grade College, Bantwal

Dakshina Kannada Dist

Abstract

Banking system plays an important role in the financial and economic development of the country The definition of banking as per Banking Companies Regulation Act says that banking is accepting for the purpose of lending or investment of money from the public, repayable on demand and withdrawable by cheque, draft ,order or otherwise. Under traditional banking there was a personal relationship between the banker and customer. Customers are supposed to go the bank premises and get done their banking activities Now there is a shift from traditional banking system to digital banking wherein banking activities are done through internet. With the Indian Government's vision of a cashless economy and rapid development in improving internet availability throughout the nation, the country recorded over 25.5 billion real-time payment transactions (highest in the world) exceeded China by 60 %.Digital banking is the technique of doing banking transactions electronically without having personal contact with the banker. It is also called as internet banking, online banking etc. The scheme of demonetization introduced in the country in 2016 paved the way for development of cashless and paperless transactions ,this cashless economy contributed to the development of digital or net banking. The digital banking frauds have been the issue of concern over the years. Fraudsters are inventing newer techniques to cheat the customers. This paper examines the various types of banking frauds associated with digital or net banking and how to prevent it.

Key words: traditional banking. Cashless economy, online banking, banking frauds, demonitisation

Introduction

Net Banking, also known as online banking or Internet Banking, is an electronic payment system. It allows us to conduct many different types of transactions through the internet from the comfort of our home. Internet Banking, also known as net-banking or online banking, is an electronic payment system that enables the customer of a bank or a financial institution to make financial or non-financial transactions online via the internet. This service gives online access to almost every banking service, traditionally available through a local branch including fund transfers, deposits, and online bill payments to the customers.

Internet banking can be accessed by any individual who has registered for online banking at the bank, having an active bank account or any financial institution. After registering for online banking facilities, a customer

need not visit the bank every time he/she wants to avail a banking service. It is not just convenient but also a secure method of banking . Net banking portals are secured by unique User/Customer IDs and passwords.

Here are some key events in the history of internet banking :

- December 1980: United American Bank launched the first home banking service, which allowed customers to check their account information securely.

- 1981: Four major banks in New York (Citibank, Chase Manhattan, Chemical Bank, and Manufacturers Hanover) launched their own home banking services.

- 1983: CCF Bank (now part of HSBC) launched France's first videotext banking service.

- 1984: Online banking was launched in the United Kingdom, but it didn't become popular until the 1990s.

- 1995: Wells Fargo became the first U.S. bank to add account services to its website.

- 1996: Presidential became the first U.S. bank to open bank accounts over the internet.

- 1996: OP Financial Group, a cooperative bank, became the second online bank in the world and the first in Europe.

- 1997: Sumitomo Bank launched Japan's first online banking service. he concept of a cashless economy was first discussed in the 1990s with the rise of electronic banking [1]. However, the use of non-cash transactions for daily life settlements became widespread in the 2010s with the advent of digital payment methods such as PayPal, Apple Pay and electronic bills [1]. Some notable milestones in the journey to a cashless society include [2] [1]:

- 2012: Debit cards accounted for 35% of monthly card spends in India.

- 2016: United States User Consumer Survey Study reported that 75% of respondents preferred a credit or debit card as their payment method.

- 2016: Only about 2% of the value transacted in Sweden was via cash.

- 2017: Debit cards accounted for 50% of India's monthly card spends.

- 2018: India launched the Bharat Interface for Money (BHIM) which allowed for instant bank transfers via a mobile app.

Demonetization in India started on :

- January 12, 1946: The British government removed the Rs 500, Rs 1,000 and Rs 10,000 notes from circulation to combat black-market activities.

- January 16, 1978: The Indian government removed the Rs 1,000, Rs 5,000 and Rs 10,000 notes from circulation to combat black money.

- November 8, 2016: The Indian government demonetized the Rs 500 and Rs 1,000 notes and introduced the Rs 2,000 note to combat counterfeit money and black money.

All these developments in India lead to the development of internet or net banking in India.

Special Features of Internet Banking

Here are some of the best features of internet banking:

*Provides access to financial as well as non-financial banking services

*Facility to check bank balance any time

*Make bill payments and fund transfer to other accounts

*Keep a check on mortgages, loans, savings a/c linked to the bank account

*Safe and secure mode of banking

*Protected with unique ID and password

*Customers can apply for the issuance of a chequebook

*Buy general insurance

*Set-up or cancel automatic recurring payments and standing orders

*Keep a check on investments linked to the bank account

Advantages of internet banking

Given below are some advantages/benefits of Internet Banking available for all the users-

24×7 Availability: Internet banking, unlike usual banking hours, is not time-bound. It is available 24×7 throughout the year. Most of the services available online are not time-restricted. Users can check their bank balance, account statements and make fund transfers anytime instantly.

Convenience of initiating financial transactions: Internet banking is largely preferred because of the convenience that it provides while fund transfer and bill payments. Registered users can use almost all the banking services without having to visit the bank and standing in queues. Financial transactions such as paying bills and transferring funds between accounts can easily be performed anytime as per the convenience of the user.

Proper Track of Transactions: Acknowledgement slips are provided by the bank after transactions which have a high possibility of getting misplaced. However, with internet banking, it becomes very easy to track the history of all the transactions initiated by the user. Transactions and fund transfers made online are organised in the 'Transaction History' section along with other details such as payee's name, bank account number, the amount paid, the date and time of payment, and remarks.

Quick and Secure: Net banking users can transfer funds between accounts instantly, especially if the two accounts are held at the same bank. Funds can be transferred via NEFT, RTGS or IMPS as per the user's convenience. One can also make bill payments, EMI payments, loan and tax payments easily. Moreover, the transactions, as well as the account, are secured with a password and unique User-ID.

Non-financial Transactions: Besides fund transfer, internet banking allows the users to avail non-financial services such as balance check, account statement check, application for issuance of cheque book etc.

Types of Fund Transfers using Internet Banking

There are three types of fund transfers which can be made using net-banking. Let us understand more-

NEFT

National Electronic Fund Transfer (NEFT) is a payment system which allows one-to-one fund transfer. Using NEFT, individuals and corporates can transfer funds electronically from any bank branch to any individual or corporate with an account with any other bank branch in the country NEFT service is available 24×7 on internet banking. But, it is a time-restricted service at the bank branch Usually, NEFT transfer is successfully completed within 30 minutes. Nonetheless, the time can even stretch to 2-3 hours or might be completed in just 10 minutes

RTGS

Real-Time Gross Settlement (RTGS) is a continuous settlement of funds individually on an order by order basis. This payment system ensures that the receiver's account gets credited with the funds almost immediately and not after a certain duration, as is the case with other payment modes like NEFT ,RTGS transactions are tracked by the RBI, thereby successful transfers are irreversible. This method is majorly used for large value transfers

The minimum amount to be remitted through RTGS is 2 lakh. There is no cap on the maximum amount for transfer via RTGS .Like NEFT, RTGS is also available online 24×7

IMPS

Immediate Payment System (IMPS) is another payment method that transfers funds in real-time. IMPS is used to transfer funds instantly within banks across India via mobile, internet and ATM, which is not only safe but also economical both in financial and non-financial perspectives IMPS is an inexpensive mode of fund transfer. Other fund transfer mediums such as NEFT and RTGS charge significantly higher than IMPS. It does not require details like account number, IFSC code, etc. Funds can be transferred via IMPS just with the mobile number of the beneficiaries.

Internet banking involves the use of technology, so there is always techno frauds associated with it. Internet Banking Fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet Banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing.

Net banking frauds: The following are the various types of frauds associated with net banking:

1.SIM Swap:

Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.

How do fraudsters operate?

Step – 1

Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means.

Step - 2

They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.

Step 3

The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

Step – 4

Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

How to protect yourself from fraud:

If your mobile no. has stopped working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the Scam.

Register for SMS and Email Alerts to stay informed about the activities in your bank account.

Regularly check your bank statements and transaction history for any irregularities.

2. Vishing:

Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

How do fraudsters operate?

Step – 1

The fraudster poses as an employee from the bank or a Government / Financial institution and ask customers for their personal information.

Step – 2

They cite varied reasons as to why they need this information. For e.g. reactivation of account, encashing of reward points, sending a new card, linking the Account with Aadhar, etc.

Step – 3

These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.

How to protect yourself from fraud:

Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email.

If in doubt, call on the Phone Banking number of your Bank.

3.Smishing :

Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How do fraudsters operate?

Step – 1

Fraudsters send SMS intimating customers of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials.

Step – 2

Unaware, the customers follow instructions to visit a website, call a phone number or download malicious content.

Step – 3

Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on customer's account, causing them financial loss.

How to protect ourself from fraud:

We should never share our personal information or financial information via SMS, call or email.

Do not follow the instructions as mentioned in SMS sent from un-trusted source, delete such SMS instantly.

4. Phishing :

Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (voice phishing) and SMS (Smishing).

How do fraudsters operate?

Fraudsters pose as Bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information.

Information so acquired is then used to conduct fraudulent transactions on the customer's account.

How to identify fake Phishing website:

Verify the URL of the webpage. The 's' at the end of 'https://' stands for 'secure' - meaning the page is secured with an encryption. Most fake web addresses start with 'http://'. Beware of such websites!

Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website.

Establish the authenticity of the website by verifying its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window.
How to protect yourself from Phishing:

Always check the web address carefully.

For logging in, always type the website address in your web browser address bar.

Always check for the Padlock icon at the upper or bottom right corner of the webpage to be 'On'.

Install the latest anti-virus/anti spyware/firewall/security patches on your computer or mobile phones.

Always use non-admin user ID for routine work on your computer.

DO NOT click on any suspicious link in your email.

DO NOT provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Visa or MasterCard etc.

DO NOT open unexpected email attachments or instant message download links.

DO NOT access Net Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

5. Money Mule:

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.

How do fraudsters operate?

Step – 1

Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange of attractive commissions.

Step – 2

The fraudsters then transfer the illegal money into the money mule's account.

Step – 3

The money mule is then directed to transfer the money to another money mule's account – starting a chain that ultimately results in the money getting transferred to the fraudster's account.

Step – 4

When such frauds are reported, the money mule becomes the target of police investigations.

How to protect yourself from fraud:

Do not respond to emails asking for your bank account details.

For any overseas job offer, first confirm the identity and contact details of the employing company.

Do not get carried away by attractive offers/commissions or consent to receive unauthorized money.

6. Trojan :

A Trojan is a harmful piece of software that users are typically tricked into loading and executing on their computers. After it is installed and activated, Trojan attacks the computer leading to deletion of files, data theft, or activation/spread of viruses. Trojans can also create back doors to give access to hackers.

How do fraudsters operate?

Step – 1

Fraudsters use spamming techniques to send e-mails to numerous unsuspecting people.

Step – 2

Customers who open or download the attachment in these emails get their computers infected.

Step -3

When the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters.

Step – 4

These details will then be used to conduct fraudulent transactions on the customer's account.

How to protect yourself from fraud:

Never open e-mails or download attachments from unknown senders. Simply delete such emails.

Installing antivirus helps. It scans every file you download and protects you from malicious files.

Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities.

Install patches from software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defence against Trojan.

Download and use the latest version of your browser.

If your computer gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. If necessary, get your computer serviced.

To overcome the dangers of above frauds, the following preventive measures can be taken:

Secured Net-Banking Tips

• Keep your Customer ID and password confidential and do not disclose it to anybody.

• Change your password as soon as you receive it by logging into your Net Banking account. Memorize your password, do not write it down anywhere.

• Avoid accessing internet banking from shared computer networks such as cyber cafes or public Wifi network like hotel/airport etc.

• Do not click on links in the emails or sites other than the genuine net banking site of your Bank to access your Net Banking webpage.

• Always visit the Bank's Net Banking site through Bank's home page by typing the bank's website address on to the browser's address bar.

• Always verify the authenticity of the Bank's Net Banking webpage by checking its URL and the PAD Lock symbol at the bottom corner of the browser.

• Disable "Auto Complete" feature on your browser.

• Uncheck "User names and passwords on forms", click on "Clear Passwords"

• Click "OK"

• Use virtual keyboard feature while logging into your internet banking account.

• Do cross check your last login information available on Net Banking upon every login to ascertain your last login and monitor any unauthorized logins.

• Always type in your confidential account information. Do not copy paste it.

• Monitor your transactions regularly. Use Bank's Alerts service and bring any fraudulent transaction to the notice of the bank.

• Always logout when you exit Net Banking. Do not directly close the browser.

Secured and safe ATM Banking

• Memorize your PIN. Do not write it down anywhere, and certainly never on the card itself.

• Do not share your PIN or card with anyone including Bank employees, not even your friends or family. Change your PIN regularly.

• Stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN. Beware of strangers around the ATM who try to engage you in any conversation.

• Do not take help from strangers for using the ATM card or handling your cash

• Do not conduct any transaction if you find any unusual device connected to your ATM machine.

• Press the 'Cancel' key and wait for the welcome screen before moving away from the ATM. Remember to take your card and transaction slip with you.

• If you get a transaction slip, shred it immediately after use if not needed.

• If your ATM card is lost or stolen, report it to your bank immediately

• When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.

• Register your mobile number with the Bank to get alerts for your transactions

• If your card gets stuck in the ATM, or if cash is not dispensed after you keying in a transaction, call your bank immediately

• If you have any complaint about your ATM/Debit/Credit card transaction at an ATM, you must take it up with the bank

Secured Phone Banking

• While talking to the Phone Banking officer, never disclose the following

o 4 digit ATM/IVR PIN

o OTP

o Net Banking password

o CVV (Card Verification Value)

• Ensure that no one sees you entering you PIN (personal identification number).

• Avoid giving verification details to the Phone Banking officer while in public places.

• The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.

Secured Online Shopping tips

• Always shop or make payments through trusted/reputed websites.

• Do not click on links in emails. Always type the URL in the address bar of the browser.

• Before entering your private details, always check the URL of the site you are on!

• If you are a frequent online shopper, signup for Verify by Visa and Master Card secure code program.

• Check your account statements regularly and bring any fraudulent transaction to the notice of the bank.

• Check for PAD LOCK symbol on the webpage before starting to transact.

• Do not click on links in emails or on referral websites to visit the online shopping site. Always type the URL in the address bar.

Do not enter your confidential account information such as Credit Card Numbers, Expiry Date, CVV values, etc in your phone or any books.

Conclusion

As the economy is moving towards formalisation, digital foot prints are becoming strong all over the places .However, this trend comes with usual problems associated with it. Legal and ethical issues are the serious issues to be addressed. In present scenario, Indian banking sector cannot avoid banking activities carried out through electronic medium but Cyber- crime and frauds are more serious offence than the real -life crimes, in order to overcome this problem, the victims should report these cases to the nearest police station and cyber fraud council in banks. In order to stop these issues, the legislature should keep a track on the working system of banks and law implementation should strict to monitor such wrongdoings and moreover banks should educate the customers regarding the awareness of cyber-crimes often. Customers who use net banking must safeguard their net banking passwords. Now in the bank premises tollfree number is displayed Take a note of this and call this number when they met across such frauds. The convenience of net banking has revolutionized the way we manage our finances, but it also comes with a heightened risk of banking frauds. As technology advances, fraudsters employ sophisticated tactics to exploit vulnerabilities in online banking systems. Therefore, it is crucial for banks and financial institutions to invest in robust security measures, such as two-factor authentication, encryption, and regular software updates, to safeguard their customers' sensitive information. Moreover, customers must also remain vigilant and take necessary precautions, like using strong passwords, monitoring their accounts regularly, and being cautious of phishing scams. By working together, we can reduce the incidence of banking frauds and ensure a safer online banking experience

References:

1.https://www.paisabazaar.com/banking/internet-banking-e-banking/

2 cybercelldelhi.in/netbanking.html

3.https://enterslice.com

4 Wikipedia