UNIT – V

Mobile banking and risks of E- Banking

Mobile banking : Meaning - ‘advantages - launching of MCHQ in India - Inter-bank mobile payment service - security and consumer decision making - e-payment proposition. New Trends. Smart card - mobile banking - technology and security. Risks of e-banking external attacks - legal risk - money laundering risk - cross - border risk - strategic risk -other risks.

Mobile banking

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted.

Transactions through mobile banking may include obtaining account balances and lists of latest transactions, electronic bill payments, and funds transfers between a customer's or another's accounts. Some apps also enable copies of statements to be downloaded and sometimes printed at the customer's premises; and some banks charge a fee for mailing hardcopies of bank statements.

From the bank's point of view, mobile banking reduces the cost of handling transactions by reducing the need for customers to visit a bank branch for non-cash withdrawal and deposit transactions. Mobile banking does not handle transactions involving cash, and a customer needs to visit an ATM or bank branch for cash withdrawals or deposits.

Advantages

1. It utilizes the mobile connectivity of telecom operators and therefore does not require an internet connection.
2. With mobile banking, users of mobile phones can perform several financial functions conveniently and securely from their mobile.
3. You can check your account balance, review recent transaction, transfer funds, pay bills, locate ATMs, deposit cheques, manage investments, etc.
4. Mobile banking is available round the clock 24/7/365, it is easy and convenient and an ideal choice for accessing financial services for most mobile phone owners in the rural areas.
5. Mobile banking is said to be even more secure than online/internet banking.

Disadvantages

1. Mobile banking users are at risk of receiving fake SMS messages and scams.
2. The loss of a person’s mobile device often means that criminals can gain access to your mobile banking PIN and other sensitive information.
3. Modern mobile devices like Smartphone and tablets are better suited for mobile banking than old models of mobile phones and devices.
4. Regular users of mobile banking over time can accumulate significant charges from their banks.

MCHQ in India

MChq is another revolutionary step in keeping with our philosophy of churning out innovative products. It completely transforms the way people shop. This service provides value-addition to the way we use credit cards and mobile phones. Customers now have one more convenient channel to pay for their shopping requirements, thus increasing their payments options.

TOP TRENDING MOBILE WALLETS:

Paytm

Paytm is by far the most popular e-Wallet in India. Reserve Bank of India approved and authorized, this is one of the most versatile mobile wallets present in India. Paytm is today a $4 billion company and offers its very own ecommerce platform too. It not only allows online payments but has come up with offline payment options also where there is no need for an active internet connection to transfer money. It can be done simply by scanning a QR code or also by using an OTP which is generated right within the app.

MobiKwik

This e-Wallet has been another major player in the e-Wallet system. It also offers a host of payment options and has partnered with many popular and well-known brands in market such as Domino's Pizza, Big Bazar, Pizza Hut, eBay, Jabong, ShopClues, Naaptol, akeMyTrip, Pepperfry, BookMyShow and more. This e-Wallet too has Reserve Bank of India authorization and license, making it one of the most trusted mobile wallets present in Indian market.

Oxigen Wallet

Claiming to have over 20 million user base, this mobile wallet is one of the most popular mobile wallets operational in India. Just like MobiKwik and Paytm, Oxigen Wallet is also RBI approved and it actually claims to be the first non-bank wallet which has managed to tie up with National Payments Corporation of India or NCPI to allow instant money transfer

Citrus Wallet

This wallet comes directly from the house of Citrus Pay – a popular payment gateway. Movies, dinners and drinks, bill payments, money transfers – everything with only a few taps, Citrus Wallet has managed to receive license from Reserve Bank of India. Boasting a network of 21 million user base, Citrus Wallet is feature rich and it even allows splitting bills with friends.

ItzCash

Authorized by Reserve Bank of India, ItzCash is a mobile wallet which is operated by Itz Cash Card Ltd. Part of Essel Group, which is conglomerate of $2.4 billion dollars' business, ItzCash offers a holistic payments solution with secured money transfer option to bank accounts. It allows a host of digital transactions like balance transfer, prepaid mobile recharge, movie tickets purchase, railway ticket booking and more.

FreeCharge

FreeCharge started as an independent mobile wallet system and it was then eventually acquired by Snapdeal – one of the largest ecommerce businesses in India. Before the company was acquired by Snapdeal, the company boasted a user base of 5 million. Offering a number of digital transactions like prepaid mobile recharge, utility bill payment, recharging

for metro card and more, this mobile wallet is definitely a feature-rich wallet. This wallet can be managed directly from mobile app as well as from a web browser.

Axis Bank Lime

This e-Wallet comes from bank and hence, it actually comes with a combo package. Axis Bank is one of the most popular banks in India and it has come a long way to provide excellent banking services to millions of Indians. Any bank that operates in India needs RBI approval and hence, Axis Bank Lime is basically authorized and licensed by RBI. Coming to the mobile wallet part, it allows utility bill payment, mobile recharges, ticket booking, etc. It even has a neat feature of analyzing spending habits and also, you can set and manage goals towards saving money.

Airtel Money

it is one of the leading telecom companies in India and it has launched its very own e-Wallet application. Online shopping, money transfer to bank accounts and contacts, performing mobile phone recharges, booking train tickets – Airtel Money has some neat feature but it is not really as versatile as Paytm, MobiKwik etc.

ICICI Pockets

Created and run by ICICI Bank, Pockets is another highly popular digital wallet. This digital wallet is powered by VISA. It is not limited to just users of a single bank, i.e. ICICI Bank. Actually, user of any bank can use this wallet and carry up to 20,000 balance in the account. It comes with a unique feature of applying for a Saving account with ICICI bank. Pockets has 60,000 merchants onboard. This means that users of this wallet can actually enjoy a wide range of products and services on a daily basis.

Jio Money

Jio Money from Reliance Jio Infocomm Ltd. It has a long way to go. It allows very basic wallet operations like transferring money, accepting money, paying bills. One of the eye-catching features of the app is that it offers various discounts and offers from various brands.

mRupee

it is owned by a fully owned subsidiary of Tata Teleservices Limited. This wallet has also received authorization from Reserve Bank of India. It allows transferring money to various bank accounts. It allows payments to merchant outlets, recharging prepaid phone numbers, paying utility bills etc.

SBI Buddy

This bank also offers a complete e-Wallet app for those who love to use digital wallets. Available in 13 languages, this wallet allows sending money, asking for money, recharging mobiles and DTH services, paying utility bills, booking cinema tickets, hotels and flights etc. One of the best parts of SBI Buddy is that you can actually supercharge your Buddy account by enabling internet banking.

Vodafone M-Pesa

M-Pesa is one of the primary players in mobile wallet world. However, despite the fact that it comes from Vodafone, the wallet has failed to leave a mark like the popular ones of the likes of Paytm, Freecharge, MobiKwik etc. DTH recharge, mobile recharge, transferring funds to bank account, utility bill payment etc. are some of the common features

that you can find in M-Pesa. It comes with IMPS system built within the app which allows sending money to a bank account or to a mobile number.

HDFC PayZapp

HDFC PayZapp is a mobile wallet actually allows basic things like bill payments, mobile recharges, DTH recharge, etc. It allows shopping as well from ecommerce sites and it actually allows you to browse products from ecommerce companies directly from its own interface. Though initially it was designed only for customers of HDFC Bank, it has now been opened for customers of all banks.

Interbank Mobile Payment Services [IMPS]

Interbank Mobile Payment System (IMPS) from National Payments Corporation of India (NPCI) is a new service that is set to revolutionise the retail money payment sector in India. With this Service all the registered Consumers will be able to transfer money instanlty from their accounts to any other account in the country using their cellphones via IMPS.

IMPS transfers can be done at anytime on a 24/7 basis and on all 365 days in a year, including on Sundays and other bank holidays. Through IMPS, interbank transfers can be initiated through multiple channels such as mobile banking, internet banking, SMS, ATMs, etc. Unlike other types of fund transfer methods, the main advantage of IMPS over NEFT and RTGS is that the service is available round the clock. The IMPS services is managed by the National Payments Corporation of India (NPCI) and comes under the purview of the Reserve Bank of India (RBI).

The participants of IMPS:

1. Remitter (Sender)
2. Banks
3. Beneficiary (Receiver)
4. National financial switch by NPCI

Features of IMPS

1. The money transfer through IMPS is as safe and secure as NEFT and RTGS .
2. It is easy to use this facility on any smart device or phone with an internet connection.
3. This is one of the fastest ways to transfer money between bank accounts
4. Money can be sent to anyone, simply with their cell phone number.
5. The recipient gets the amount credited instantly without any delays.
6. People do not need to share their bank details especially their account numbers for the transfer of funds in this platform.
7. The service is available throughout the year and 24 by 7.
8. There are no charges levied to any parties to avail this service.
9. Notifications are sent to both the parties when the transaction is completed, saying debited and credited.
10. Currently the transfer limit for IMPS is Rs. 50,000 only.
11. You should have your bank's ATM cum Debit Card.
12. You should be registered with your bank for SMS alerts.
13. If you have a basic handset, then you can use this service through SMS and texting only.
14. Customers with cell phones that have GPRS (General Packet Radio Service) enabled by their Service Provider as well as JAVA may use it online for higher security and amount.
15. Some banks have their own applications for smart phones were IMPS can be done quickly.

Smart card :

The appearance of a smart card is similar to a credit card in size and shape. It is a plastic card embedded with microprocessor chip or memory chip. The microprocessor embedded under a gold contact plate on one side of the card can be compared to minicomputer. The chip in the smart card is tamper proof and it provides enhanced security for cardholder's personal data and financial transactions. This protection is based on the data encryption standard (DES) which is approved by International Standard Organisation (ISO) as safe enough for protecting electronic funds transfer (EFT) transactions. The smart cards with a microcontroller chip have the ability to perform on-card processing functions and it can add, delete and manipulate information in the chip's memory. Smart cards are now universal and are fast replacing magnetic stripe card technology.

Security in smart card technology

Smart card technology offers a number of features that can be used to provide or enhance privacy protection in systems. The following is a brief description of some of these features and how they can be used to protect privacy.

1.Authentication.

Smart card technology provides mechanisms for authenticating others who want to gain access to the card or device. These mechanisms can be used to authenticate users, devices, or applications wishing to use the data on the card's or device's chip.

2.Secure data storage.

Smart card technology provides a means of securely storing data on the card or device. This data can only be accessed through the smart card operating system by those with proper access rights. This feature can be utilized by a system to enhance privacy by, for example, storing personal user data on the card or device rather than in a central database. In this example, the user has better knowledge and control of when and by whom their personal data is being granted access.

3.Encryption.

Smart card technology can provide a robust set of encryption capabilities including key generation, secure key storage, hashing, and digital signing. These capabilities can be used by a system to protect privacy in a number of ways. This protects the email message from subsequently being tampered with and provides the email recipient with an assurance of where it originated. The fact that the signing key originated from a smart card or device adds credibility to the origin and intent of the signer.

4.Strong device security.

Smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks. For example, the chips are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.

5.Secure communications.

Smart card technology can provide a means of secure communications between the card/device and readers. Similar in concept to security protocols used in many networks, this feature allows smart cards and devices to send and receive data in a secure and private manner. This capability can be used by a system to enhance privacy by ensuring that data sent is not intercepted or tapped into.

6.Biometrics.

Smart card technology can provide mechanisms to securely store biometric templates and perform biometric matching functions. These features can be used to improve privacy in systems that utilize biometrics. For example, storing fingerprint templates on a smart card or device rather than in a central database can be an effective way of increasing privacy in a single sign-on system that uses fingerprint biometrics as the single sign-on credential.

7.Personal device.

A smart card is, of course, a personal and portable device associated with a particular cardholder. The smart card plastic is often personalized, providing an even stronger binding to the cardholder. These features, while somewhat obvious, can be leveraged by systems to improve privacy. For example, a healthcare application might elect to store drug prescription information on the card instead of in paper form to improve the accuracy and privacy of a patient's prescriptions. Smart card technology is also built into other portable personal devices, such as mobile phones and USB devices.

8.Certifications.

Many of today's smart cards and devices have been certified that they comply with industry and government security standards. They obtain these certifications only after completing rigorous testing and evaluation criteria by independent certification facilities. These certifications help systems protect privacy by ensuring that the security and privacy features and functions of the smart card hardware and software operate as specified and intended.

Mobile banking

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted.

Transactions through mobile banking may include obtaining account balances and lists of latest transactions, electronic bill payments, remote check deposits, P2P payments, and funds transfers between a customer's or another's accounts. Some apps also enable copies of statements to be downloaded and sometimes printed at the customer's premises; and some banks charge a fee for mailing hardcopies of bank statements.

Advantages

1. **Time saving** : Instead of allocating time to walk into a bank, you can check account balances, schedule and receive payments, transfer money and organise your accounts when you're on the go.
2. **Convenient** : The ability to access bank accounts, make payments, and even track investments regardless of where you are can be a big advantage Do your banking at a time and place that suits you, instead of waiting in queues.
3. **Secure :** Generally, good mobile banking apps have a security guarantee or send you a SMS verification code you need to input to authorise a payment for added security. Mobile banking is said to be even more secure than online/internet banking.
4. **Easy access to your finances:** with the introduction of mobile banking, you are able to access your financial information even beyond the working hours. It helps to avail banking services even by making a call to the bank.

5. **Increased efficiency**: mobile banking functions are functional, efficient and competitive. It also helps in decongesting the banking halls and reduces the amount of paperwork for both the banker and the customer
6. **Fraud reduction:** one very real advantage to implementing mobile banking. "Customers are being deputized in real time to watch their accounts.
7. It utilizes the mobile connectivity of telecom operators and therefore does not require an internet connection.
8. You can check your account balance, review recent transaction, transfer funds, pay bills, locate ATMs, deposit cheques, manageinvestments, etc.
9. Mobile banking is available round the clock 24/7/365, it is easy and convenient and an ideal choice for accessing financial services for most mobile phone owners in the rural areas.

Disadvantages

1. Mobile banking users are at risk of receiving fake SMS messages and scams.
2. The loss of a person's mobile device often means that criminals can gain access to your mobile banking PIN and other sensitive information.
3. Modern mobile devices like Smartphone and tablets are better suited for mobile banking than old models of mobile phones and devices.
4. Regular users of mobile banking over time can accumulate significant charges from their banks.
5. Even though there are 1.5 billion computers on the Internet and 4.5 billion people using mobile phones, there's currently no significant operating system supporting the mobile space. "Hackers want to do the least amount of work for the biggest gain..
6. Most mobile banking apps need an internet connection to be able to operate, so if you live in a rural area or experience problems with your internet connection, then you won't be able to access your account. The same applies if your mobile phone runs out of battery.
7. Many phones aren't yet compatible with anti-virus software. Most cell phones don't come standard with anti-virus protection even if they have the capacity to browse the internet.
8. Some banks don't offer the same level of protection for cell phone banking that they do for online or in person transactions. Because the risks are still generally unknown some banks have been slow to make promises about what will or will not be covered when you use cell phone banking.

Comparison between Mobile and Internet Banking:

Basis	Mobile Banking	Internet Banking
Use	Through a mobile app that is downloaded onto the computer	Through a web browser
Device	On the mobile, i.e. smartphone	Over the internet, most commonly via the computer or laptop
Functions	Typically limited functions	Typically more functions
Download	The banking application needs to be downloaded onto the phone	No download required
Internet	Requires access to internet, either through Wi-Fi or data	Requires access to internet, typically though Wi-Fi or wired connection.

Risks of e-banking

1.external attacks –

Most of the hacking tools are placed on the web, and they are downloaded into the user's PC when the user opens the web or e-mail. These tools can easily capture the password, account number, and personal data which the user entered. Moreover, they are even capable of replacing the input screen, and make the user see a counterfeit website of the bank which the hacker had installed in advance.

2.legal risk

Legal risk arises from violations of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established. As e-banking is relatively new area of business, not knowing, or not understanding certain thing regarding legal policy can source risk. There are many more sources that can lead to legal risk, and the number of sources is rising every day

3.money laundering risk –

Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy. As Internet banking transactions are conducted remotely banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk.

4.cross - border risk –

Banks may face different legal and regulatory requirements when they deal with customers across national borders. For new forms of retail electronic banking, such as Internet banking, and for electronic money, there may be uncertainties about legal requirements in some countries. In addition, there may be jurisdictional ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risk associated with non-compliance with different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules, and money laundering laws.

5.strategic risk

A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. On strategic risk E-banking is relatively new and, as a result, there can be a lack of understanding among senior management about its potential and implications.

6.other risks.

Traditional banking risks such as credit risk, liquidity risk, interest rate risk, and market risk may also arise from electronic banking and electronic money activities, though their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational, and legal risks. This may be particularly true for banks engaged in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in electronic medium.