Go, change the world

Introduction to Cybersecurity

Unit - IV

E-Commerce and Digital Payments

E-Commerce or Electronic Commerce

Electronic commerce (e-commerce) refers to companies and individuals that buy and sell goods and services over the internet.

E-commerce operates in different types of market segments and can be conducted over computers, tablets, smartphones, and other smart devices.

Nearly every imaginable product and service is available through e-commerce transactions, including books, music, plane tickets, and financial services such as stock investing and online banking.

Transaction of money, funds, and data are also considered as E-commerce. These business transactions can be done in four ways: Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C), Customer to Business (C2B).

Online stores like Amazon, Flipkart, Shopify, Myntra, Ebay, Quikr, Olx are examples of E-commerce websites.

So when you log into your Amazon and purchase a book, this is a classic example of an e-commerce transaction. Here you interact with the seller (Amazon), exchange data in form of pictures, text, address for delivery etc. and then you make the payment.

As of now, e-commerce is one of the fastest growing industries in the global economy. As per one estimate, it grows nearly 23% every year. And it is projected to be a $8 trillion industry by the end of this decade.

Types of E-Commerce Models

Electronic commerce can be classified into four main categories. The basis for this simple classification is the parties that are involved in the transactions. So the four basic electronic commerce models are as follows,

1. Business to Business

This is Business to Business transactions. Here the companies are doing business with each other. The final consumer is not involved. So the online transactions only involve the manufacturers, wholesalers, retailers etc.

2. Business to Consumer

Business to Consumer. Here the company will sell their goods and/or services directly to the consumer. The consumer can browse their websites and look at products, pictures, read reviews. Then they place their order and the company ships the goods directly to them. Popular examples are Amazon, Flipkart, Jabong etc.

3. Consumer to Consumer

Consumer to consumer, where the consumers are in direct contact with each other. No company is involved. It helps people sell their personal goods and assets directly to an interested party. Usually, goods traded are cars, bikes, electronics etc. OLX, Quikr etc follow this model.

4. Consumer to Business

This is the reverse of B2C, it is a consumer to business. So the consumer provides a good or some service to the company. Say for example an IT freelancer who demos and sells his software to a company. This would be a C2B transaction.

Examples of E-Commerce

- Amazon
- Flipkart
- eBay
- Fiverr
- Upwork
- Olx
- Quikr

Advantages of E-Commerce

1. **Global Reach** E-commerce provides the sellers with a global reach. They remove the barrier of place (geography). Now sellers and buyers can meet in the virtual world, without the hindrance of location.
2. **Low transaction cost** Electronic commerce will substantially lower the transaction cost. It eliminates many fixed costs of maintaining brick and mortar shops. This allows the companies to enjoy a much higher margin of profit.
3. **Customer Satisfaction** It provides quick delivery of goods with very little effort on part of the customer. Customer complaints are also addressed quickly. It also saves time, energy and effort for both the consumers and the company.
4. **Convenience** One other great advantage is the convenience it offers. A customer can shop 24×7. The website is functional at all times, it does not have working hours like a shop.
5. **No intermediaries** Electronic commerce also allows the customer and the business to be in touch directly, without any intermediaries. This allows for quick communication and transactions. It also gives a valuable personal touch.

Disadvantages of E-Commerce

1. **Start-up Cost** The start-up costs of the e-commerce portal are very high. The setup of the hardware and the software, the training cost of employees, the constant maintenance and upkeep are all quite expensive.

2. **High Risk of failure** Although it may seem like a sure thing, the e-commerce industry has a high risk of failure. Many companies riding the dot-com wave of the 2000s have failed miserably. The high risk of failure remains even today.
3. **Lack of personal touch** At times, e-commerce can feel impersonal. So it lacks the warmth of an interpersonal relationship which is important for many brands and products. This lack of a personal touch can be a disadvantage for many types of services and products like interior designing or the jewelry business.
4. **Security** Security is another area of concern. Only recently, we have witnessed many security breaches where the information of the customers was stolen. Credit card theft, identity theft etc. remain big concerns with the customers.
5. **Fulfillment Problems** Then there are also fulfillment problems. Even after the order is placed there can be problems with shipping, delivery, mix-ups etc. This leaves the customers unhappy and dissatisfied.

Why is cyber security important in ecommerce?

Cybersecurity or cybersecurity is a concept that encompasses a set of strategies, tactics and technologies that aim to defend systems, digital services and online electronic data belonging to consumers, institutions and companies like yours against theft, manipulation, blocking, disorientation and other damage caused by cybercriminals.

Cybersecurity is crucial in e-commerce to protect sensitive customer information, secure financial transactions, prevent data breaches & maintain the trust of online shoppers. A breach can lead to financial losses, reputational damage & legal consequences.

Components of E-Commerce

• **User:**Thismay beindividual / organization or anybody using the e-commerce platforms.

• **E-commerce vendors:**This is the organization/ entity providing the user, goods/ services. E.g.:www. flipkart.com.

• **Technology Infrastructure:** This includes Server computers apps etc.Computers, Servers and DatabaseThese are the backbone for the success of the venture. They store the data/program used to run the whole operation of the organization.

Internet/ Network: This is the key to success of e-commerce transactions.

• Internet connectivity is important for any e-commerce transaction to go through.

• The faster net connectivityleads to better e-commerce. Many mobile companies in India have launched 4G services.

• **Web Portal:**This shall provide the interface through which an individual/organization shall perform e-commerce transactions.

• **PaymentGateway:**Credit / Debit Card Payments, Online bank payments, Vendors own payment wallet, Third Party Payment wallets, like SBI BUDDY or PAYTM, Cash on Delivery (COD) and Unified Payments Interface (UPI).

E-commerce Vendors further needs to ensure following for better, effective and efficient transaction.

- **Suppliers and Supply Chain Management**: For effectiveness, they need to ensure that :

  Enough and the right goods suppliers.

  Suppliers should be financially and operational safe.

  Suppliers are able toprovide real-time stock inventory.

  Order to delivery time is short.

- **Warehouse operations:** From this place online retailers pick products, pack them and prepare those products to be delivered. Many e-commerce companies are investing huge amounts of money in automating the warehouses.

- **Shipping and returns:** Shipping is supplementary and complementary to warehouse operations. Fast and safe returns is also very important for e- commerce vendors.

- **E-Commerce catalogue and product display:** Proper displayincluding product details, technical specifications, is necessary for better sales.

- –**Marketing and loyalty programs:** Loyalty programs is to establish a long- term relationship with customer.E.g. In airline industry, customer can get good discount/ free tickets based on loyalty points accumulated.

- **Showroom and offline purchase:** Few e-commerce vendors over period have realized that their products can be sold fast if customers are able to feel / touch / see those products. These vendors have opened outlets for customer experience of their products.

- **Different Ordering Methods:** These are the way customer can place his/her order, say Cash on Delivery is today most preferred method.

- **Guarantees:** The product/service guarantee associated with product/service being sold e.g. Money back guarantees.

- **Privacy Policy:** Customers are very concerned about the information that they are sharing. E- commerce vendors need to clearly explain them what the vendor plan to do with the information they have collected.

- **Security:** Vendor website needs to state that online data used to transact is safe that vendors is using appropriate security including security systems like SSL (Secure Socket Layer). This guarantees that the data provided by customer will not fall into the hand of a hacker.

Elements of e-commerce Security

Confidentiality: Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.

Integrity: Information should not be altered during its transmission over the network.

Nonrepudiation: It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.It is prevention against any one party from reneging on an agreement after the fact

Authenticity: There should be a mechanism to authenticate a user before giving him/her an access to the required information.Confidentiality: protection against unauthorized data

Utility: To prserve the utility of information, we should mandatorily back up copies of all crucial information and should control the use of protective mechanisms such as cryptography

Availability: Information should be available wherever and whenever required within a time limit specified.

e-commerce Threats

It's every website owner's nightmare to wake up one day to find that a security hole has been exploited to hack their website. Unfortunately, this is a situation that happens more often than one might imagine.
Above all, as soon as you own a business and have a certain reputation, the risk is even greater, as the challenge of hacking the site becomes interesting.
This is why it is so important to make sure that everything is in place so that the website is well protected and to do regular checks to see if there are any potential vulnerabilities.

Types of threats to E-commerce:

Payment conflict: In E-commerce, payment conflicts can arise between users and the E-commerce platforms. These electronic funds transferring systems might process extra transactions from the users which will lead to a payment conflict by the users due to some glitches or errors.

Financial fraud: Whenever an online transaction or transfer of funds takes place, it always asks for some pin or passwords to authenticate and allows only the authorized person to process the transactions. But due to some spyware and viruses used by attackers, they can also process the transactions of the users by allowing the unauthorized person, which will lead to causing a financial fraud with the user.

E-wallets: E-wallets are now an essential part of E-commerce platforms. Attack on E-wallets can lead to the leak of the sensitive banking credentials of the users which can be used by the attackers for their own profit. Regulators tend to monitor all the activities related to the financial security of the money of the users.

Phishing: It is one of the most common attacks nowadays on the users, where the attackers send emails and messages to a large number of users which contain a special link in it. When the users open that link in their browser, the malware starts downloading in the background and the attacker gets full control over the financial information about the users. They make fake websites to make the users believe their website and fill out their financial credentials.
SQL injections: SQL injections are used by attackers to manipulate the database of large organizations. Attackers enter malicious code full of malware into the database and then they search for targeted queries in the database and then they collect all the sensitive information in the database.

Cross-site scripting (XSS): Hackers target the website of E-commerce companies by entering malicious code into their codebase. It is a very harmful attack as the control of the entire website goes into the hands of the attackers. It can enable the attackers to track the users by using their browsing activity and their cookies. For More details please read the what is cross-site scripting XSS article.

Trojans: Attackers make software that may appear to be useful before downloading, but after downloading the software it installs all the malicious programs on the computer. It collects data like personal details, address, email, financial credentials and it may cause data leaks.
Brute force attacks: Hackers draw patterns and use random methods to crack into someone else's account as an unauthorized user. It requires the use of multiple algorithms and permutations and combinations to crack the password of an account by the attacker.

Bots: The hackers use a large number of bots on E-commerce websites to track the competitor in the E-commerce industry rankings and his user's buying policies in order to scrap the sales and revenue of the competitor. It also decreases the ranking of their E-commerce website as compared to the competitors due to bad experiences faced by the users. It results in overall price decreasing and less revenue overall in sales.

DDoS attacks: Distributed Denial of Service (DDoS) attacks are most commonly used by hackers to not allow original legitimate users to access and buy and sell products from the E-commerce platforms. Hackers use a large number of computers to flood the number of requests to the server so that at one time the server crashes out.

Skimming: Skimming is a popular method to spread out the malware on the website's main pages which are used by a large number of people. It steals and leaks all information entered by the users on that webpage and all this information goes to the attacker through skimming.

Man-in-the-Middle attack: In this type of attack, the attacker can clearly get all the information in the conversation taking place between the consumer and the E-commerce platform itself. The attacker sees the conversation between both of them and uses this as an opportunity to make the user face some vulnerability.

Why cyber security is a matter of concern for e-commerce?

Cyber security is essential for e-commerce because cyber attacks can result in loss of revenue, of data and of overall viability for businesses.

Cyber criminals use advanced tactics to steal information from businesses.

With e-commerce, it's not just your data that you're protecting; it's your customers' data that you need to be careful with. A breach in your cyber security systems could mean the loss of your customer's information. And that could cost your business the trust and reputation that you've worked to build up.

Take the following steps to make your online store more cyber secure.

How to protect yourself as an e-commerce provider?

There is no foolproof way of protecting your e-commerce store against cyber criminals. But by taking these steps you can do everything possible to keep your business secure.

Have a cyber security policy in place

The first line of defence against cyber criminals is to have a cyber security policy.

With a cyber security policy, you can ensure that everyone you work with is on the same page about staying cyber secure.

You – as a small-or medium-sized business owner or manager - may be clear on what needs to be done to protect your cyber systems. But if your employees aren't as clear on what they should be doing, your system is at risk from a cyber threat .

A cyber security policy sets rules for everyone in your organization to follow, clearly stating that key activities can't fall through the cracks.

This is especially important in the midst of COVID-19, when most employees are working remotely and it may be more difficult for managers and owners to enforce cyber security best practices.

Create strong passphrases

A password is one of your most important defences against cyber criminals.

Creating a passphrase or a strong password protects your website and your information from being hacked.

Use a secure e-commerce platform

E-commerce platforms have an obvious interest in offering their clients the best possible protection against cyber threats.

Why? Because a customer with cyber security problems isn't a happy customer.

That's why e-commerce platforms offer cyber security solutions for merchants.

If you're looking for a new e-commerce platform, research the various security features and options that are offered. This could include things like multi-factor authentication , customer data encryption , real-time threat alerts and compliance features.

If you already have an e-commerce platform, you might want to re-evaluate the features it offers.

And, as always, be sure to update any software you're using. Out-of-date software can have security vulnerabilities that may give cyber criminals a backdoor into your online store.

Don't fall for phishing scams

Cyber criminals are taking advantage of COVID-19 and increasingly carrying out phishing scams. Unfortunately, online merchants aren't immune from these attempts from cyber criminals to trick victims into giving up information that can compromise customers' information and lead to loss of revenue and trust.

That's why it's important for online merchants to stay vigilant in steering clear of phishing attempts.

Main components of e-commerce security

The 7 Critical Components of E-Commerce Security

As more and more brick-and-mortar retailers move their businesses online, the question of e-commerce security becomes ever more critical. What security features do you need to safely sell products online?

The customer purchase funnel presents too many opportunities for security breaches.

Think about it – at every step of the customer's purchase process, how many opportunities are there for identity theft, data breaches, or scamming attempts? In a brick-and-mortar location, you can test cash with a counterfeit pen or check an ID against a credit card. Online, however, you have to trust your security procedures to protect your customers – and your business.

E-commerce security breaks down to seven critical components:

- Payment encryption
- Personal data security
- Multi-factor authentication
- Customer communication
- Malware and ransomware protection
- Phishing and e-skimming protection
- Security compliance

So, how can you best protect your online business from security threats?

Start by encrypting payment information for secure transactions.

Most e-commerce platforms like Shopify, BigCommerce, Magento, and WooCommerce offer built-in encryption services to protect credit card numbers, bank information, and other transactional data.

Secure personal data with locked-down customer profiles.

Payment information isn't the only data to encrypt: Customer information like shipping addresses and contact info should be treated with the same respect. One of the best ways to protect your customers' personal information is to require strong passwords for every account.

Guarantee you are who you say you are with multi-factor authentication.

This goes both ways, for the business and for the customer. Multi-factor authentication, like verification codes and security calls, keeps up legitimacy between the business owner and the customer.

For example, in addition to a username and password, protect your customers' online accounts by requiring an SMS or voice call verification code every time they log in to your site from a new device.

Keep clear lines of communication open about customer security policies.

If you run an online business, it's critical to communicate clearly with your customers about their security. For example, Amazon and other online retail bigwigs have clear security policies that state when their representatives will reach out for customer-specific data – and more importantly, when they won't.

Take this security note from BigCommerce, for example: *"BigCommerce will never send you an email with a link to update your store or your login credentials. If you receive an email, phone call, or text from 'BigCommerce' in which personal information is requested, contact customer support directly for validation."*

Protect your business from malware and ransomware attacks.

Locking down your business data with regular backups, suspicious file quarantine, and other security services is critical to maintaining an online presence. Remote monitoring and management (RMM) is one of the best ways to protect an e-commerce business. Through RMM, your managed service provider can identify and deal with threats before they ever pose a risk to your business/

Safeguard your website from phishing and e-skimming.

E-commerce targeted phishing scams are becoming more and more common. Recently, we helped a client lock down their business's Amazon account after a scammer, posing as an Amazon representative, tried to access the client's bank account and credit card information.

E-commerce businesses should also be aware of *e-skimming*, a type of cybersecurity attack that targets credit card and other payment information as it's entered on a website. A successful phishing attack can give hackers control of your website, transaction data, and transaction process, installing keyloggers or other malicious software to steal customer data from your website.

Keep up with security compliance to legitimize your online business.

Finally, make sure your online business is staying current with local and international compliance laws. Stay up to date on online updates like switching to HTTPS security protocols, Payment Card Industry Data Security Standards (PCI DSS), and data security requirements from the International Organization for Standardization (ISO).

Pro tip: We just threw a lot of industry-specific abbreviations at you there, so if you're not sure how to get started with dotting your ISOs and crossing your SQLs, we're here to help.

E-commerce website security measures to cover you 24/7

1. Use Multi-Layer Security

It is helpful to employ various security layers to fortify your security. A Content Delivery Network (CDN) that is widespread can block DDoS threats and infectious incoming traffic. They use machine learning to keep malicious traffic at bay.

2. Get Secure Server Layer (SSL) Certificates

One of the primary benefits of SSL Certificates is to encrypt sensitive data shared across the internet. It ensures that the information reaches only the intended person. It is a very crucial step because all data sent will pass through multiple computers before the destination server receives it.

3. **Use solid-rock Firewalls**

Use effective e-commerce software and plugins to bar untrusted networks and regulate the inflow and outflow of website traffic. They should provide selective permeability, only permitting trusted traffic to go through.

You can trust the Astra firewall to stop Spam, XSS, CSRF, malware, SQLi, and many other attacks on your website. It ensures that the only traffic that accesses your eCommerce store consists of the real users. Moreover, we have specialized WAF solutions for WordPress, Magento, Opencart, Prestashop, Drupal, Joomla, and custom made PHP sites.

In a nutshell, the Astra firewall protection from:

- OWASP top 10 threats
- Protection from bad bots.
- Spam protection.
- Protection against 100+ types of attacks.

4**. Anti-Malware Software**

Your electronic devices, computer systems, and web system need a program or software that detects and block malicious software, otherwise known as malware. Such protective software is called Anti-malware software. An effective anti-malware should render all the hidden malware on your website.

One such scanner is the Astra Malware Scanner. It scans your web system for all malicious software round the clock and is at your disposal It also lets you automate your scans with its "Schedule a Scan" feature. You can schedule the scans daily, weekly, monthly or fortnightly.

With Astra Scanner, you can enjoy:

- unlimited scans
- Notifications in case of any changes in file
- scanning powered by machine learning.
- collective intelligence

Online Banking

Securing Online Banking

Most industries have deployed internet technologies as an essential 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 online banking customers the facilities to access and manage their bank accounts easily and globally.

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

Online banking has been deployed more frequently over the past few decades to support and improve the operational and managerial performance within the banking industry.

Threats to Online Banking

There are some information security threats and risks associated with the use of online banking systems. The confidentiality, privacy and security of internet banking transactions and personal information are the major concerns for both the banking industry and internet banking.

Attacks on online banking today are based on deceiving the user to steal login data. Phishing, pharming, Cross-site scripting, adware, key loggers, malware, spyware, Trojans and viruses are currently the most common online banking security threats and risks.
The following are the major attack scenarios:

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

What is masquerading in cyber security?

- A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.

Best practices for online Banking Users
For Users
Protect your PC:

- Install anti-virus software and keep it updated on a regular basis to guard against new viruses
- Install anti-spyware security software against those programs that monitor, record and extract the personal information you type in your PC (passwords, card numbers, ID numbers, etc.)

- Install personal firewalls to protect your PC against unauthorized access by hackers
- Keep your operating system and internet browser up to date, checking for and downloading new versions/security enhancements from the vendor's web site

Protect your personal information:

- Create hard-to-guess security access codes (User ID & password) for Online Banking and make them unique (e.g. they should not be the same as those you use to access your e-mail account)
- Change your security access codes periodically
- Memorize your security access codes, avoid writing them down and keep them strictly personal and confidential
- Do not disclose to ANYONE your security access codes: Bank will never initiate or contact you for your e-banking or ATM PINs, card or account numbers, personal identification information, neither over the phone nor in any electronic or written message. Also refrain from providing ATM pin for ecommerce transactions.
- Never leave your PC unattended when logged into Online Banking
- Always remember to log off from your online session using the "Log-off" button when finished using the e-banking services

Use the Internet cautiously:

- Always access Online Banking internet only by typing the URL in the address bar of your browser.
- Never attempt to access Online Banking internet through an external link of unknown or suspicious origin appearing on other websites, search engines or e-mails
- Before logging in, check for the Bank's Security Certificate details and the various signs (e.g. green address line and Lock, HTTPs) that confirm you are visiting the secure pages of Bank.
- Ignore and delete immediately suspicious fraudulent (phishing, spoof, hoax) e-mails that appear to be from Bank, asking you to urgently click a link to a fraudulent (spoof) website that tries to mimic the Bank's site and to lure you into giving out your sensitive personal information (PIN, account or card numbers, personal identification information et al.)
- Never click on a link contained in suspicious e-mails
- Avoid using Online Banking from public shared PCs (as in internet cafes, libraries, etc.) to avoid the risk of having your sensitive private information copied and abused

Stay alert:

- Sign-on to Online Banking regularly and review your account transactions, checking for any fraudulent activity on your account (e.g. transactions you do not recognize)
- Keep track of your last log-on date and time, displayed at the top left side of the Online Banking Home page
- Once logged into Online Banking, you can also monitor the actions performed online

Prompt reporting of suspicious activity:

- Contact your bank immediately, if you think someone knows your security access code or in case of theft of your code/ money or in case you have forgotten your credentials.
- Forward any suspicious e-mails to the bank on their phishing reporting email as well as on CERT-In email incident@cert-in.org.in
- Your prompt action is crucial to prevent any (further) damage

Reference:

http://www.cert-in.org.in/

Mobile Banking
Securing Mobile Banking

The increasing usage of Smartphones has enabled individuals to use various applications including mobile banking applications. More and more individuals have started using mobile applications for banking as compared to the traditional desktop/Web-based banking applications.

Mobile banking refers to the use of a Smartphone or other cellular device to perform online banking tasks while away from your home computer for various uses such as monitoring account balances, viewing mini statement, account statement, transferring funds between accounts, bill payment etc.

Threats to Mobile Banking :
Mobile Banking Malwares:

There have been incidents that involved sophisticated virus infecting bank's mobile apps users to steal password details and even thwart two-factor authentication, by presenting victims with a fake version of the login screen when they access their legitimate banking application. A key vector by which the mobile banking malware get into the mobile device is through malicious applications posing as legitimate applications that users download and then become infected.
For prevention against Malware attacks:

- Download and use anti-malware protection for the mobile phone or tablet device.
- Keep the Banking App software up to date: Using the latest version of software allows receiving important stability and security fixes timely.
- Use security software: Applications for detecting and removing threats, including firewalls, virus and malware detection and intrusion-detection systems, mobile security solutions should be installed and activated.
- Reputed applications should only be download onto the smart phone from the market after look at the developer's name, reviews and star ratings and check the permissions that the application requests and ensuring that the requests match the features provided by that application.

Phishing/Smishing/Vishing Attack:
An attacker attempts phishing on to a mobile phone through SMS (Short Message Service), text message, telephone call, fax, voicemail etc. with a purpose to convince the recipients to share their sensitive or personal information.
For prevention against phishing attacks

- Emails or text messages asking the user to confirm or provide personal information (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) should be adequately implemented in mobile banking apps thus helping to prevent phishing and man-in-the-middle attacks.

Jailbroken or Rooted Devices:

This is practiced to gain unrestricted or administrative access to the device's entire file system, at the risk of exposing the device vulnerable to the malicious apps download by breaking its inherent security model and limitations, allowing mobile malware and rogue apps to infect the device and control critical functions such as SMS. Thus the mobile banking app security is exposed to extreme risk on a jailbroken device.

Outdated OSs and No Secure Network Connections:

Risk factors such as outdated operating system versions, use of no secure Wi-Fi network in mobile devices allow cybercriminals to exploit an existing online banking session to steal funds and credentials.

For prevention: Use Secure Network Connections: It's important to be connected only to the trusted networks. Avoid the use of public Wi-Fi networks. More secure and trusted WiFi connections identified as "WPA or WPA2" requiring strong passwords should be used.
Best Practices for Users to remain safe

- Enable Passwords On Devices: Strong passwords should be enabled on the user's phones, tablets, and other mobile devices before mobile banking apps can be used. Additional layers of security inherently provided by these devices should be used.
- Bank account number or IPIN should not be stored on the user's mobile phone.
- The user should report the loss of mobile phone to the bank for them to disable the user's IPIN and his access to the bank's account through Mobile Banking app.
- When downloading the Bank's Mobile app in the mobile device, the user should go to a trusted source such as the App Store on the iPhone® and iPod touch® or Android Market. User can alternately check the Bank's website for the details of the ways to receive App download URL, whether in the response to his SMS or email to the bank and then install the application. The app from any other third party source should not be downloaded.

Reference:
http://www.cert-in.org.in/

Security of Credit Card and Debit Card
Secure Usage of Credit & Debit Card/ATM
Security Threats
Identity theft
The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

Application fraud
Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

Account takeover
Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

Credit card fraud

Credit card fraud is committed by making use of credit/debit card of others for obtaining goods orservices. The threat emerge due to stealing of information like Credit card number, PIN number,password etc. Theft of cards and cloning of cards are also employed to commit such frauds.

Hackers use complex techniques like Phishing, Skimming etc. to gain credit card information from innnocent users.

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and creditcard details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can procure victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card and makes note of card details for further use.

Vishing

It is one of the method of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and "phishing".

Social Engineering

Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance.

Steps to be followed before Credit card & Debit card/ATM card usage :

- Whenever you receive the card from the bank make sure the mail is completely sealed and there is no damage.
- Whenever you receive the card from the bank immediately sign on the card.
- Try to cover the last three digit number on the card.
- Register your phone number to check the account transactions.
- Change the pin number immediately.

Secure usage of credit/Debit cards at Shopping malls and Restaurants

- Always keep an eye how the vendor swipe your card.
- Always make sure that the transactions happen at your presence.

- Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt.
- Don’t give away your personal information in the survey forms given in restaurants/shopping malls.

Secure usage of credit / Debit card over internet

- Always use secure websites for transaction and shopping.
- Please look for signs of security.
- Identify security clues such as a lock image at the bottom of your browser, A URL that begins with http (These signs indicates that your purchases are secured with encryption to protect Your account information).
- Always shop with merchants you know and trusts.
- Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies
- Treat all e-mail messages with suspicion to avoid phishing scams. Do not respond to e-mail messages asking for personal information including financial information, as banks do not ask for such information.
- Never send payment information via e-mail. Information that travels over the Internet (such as e-mail) may not fully protected from being read by outside parties.
- Please be careful when providing personal information online.
- Please be wary of promotional scams. Identity thieves may use phony offers asking for your personal information.
- Please keep your passwords secret. Some online stores may require you to register with them via a username and password before buying. Online passwords should be kept secret from outside parties the same way you protect your ATM PIN.
- Always make sure to use the virtual keyboard for net banking.

Do’s

- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Shield the ATM pin number during transaction. Don’t carry the transaction receipts along.
- Please change your ATM PIN once in every 3 months. As advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your receipts against your monthly statement.
- Only carry around credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it. (bills)
- Notify your credit card issuers in advance of your change of address, then you change home address.
- If you lose your credit card, please report the loss immediately.
- When you dispose a card at the time of renewal/upgradation, please make sure to cut it diagonally before disposal.

Don’ts

- Don’t accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card.
- Don't carry around extra credit cards that you rarely use.
- Don’t disclose your Credit Card Number/ATM PIN to anyone.

- Don’t hand over the card to anyone, even if he/she claims to represent the Bank.
- Don’t get carried away by strangers who try to help you use the ATM machine.
- Don’t use the ATM machines if the device is not in good conditions.
- Don’t transfer or share your account details with unknown/non validated source.
- Don’t access Netbanking or make payment using your Credit/Debit card from shared or unprotected computers in public places.
- Don’t open unexpected e-mail attachments from unexpected sources or instant message download links. Delete suspicious e-mail immediately.
- Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card info out when you receive a phone call. (This is called Vishing)
- Don’t provide your credit card information on a website that is not a secure site.
- Don’t share any confidential information such as password, customer id, Debit card number, Pin CVV2, DOB to any email requests, even if the request is from government authorities like Income Tax department, RBI or any card association company like VISA or Master card.
- Don’t address or refer to your bank account problems or your account details and password on social networking site or blogs.
- Don’t store critical information like your ATM PIN number on your mobile phone.

UPI Security

Online Payments through Unified Payment Interface(UPI)

Unified Payment Interface (UPI) is an initiative by National Payments Corporation of India (NPCI), set up with the support of the Reserve Bank of India with a vision of migrating towards a "less-cash" and more digital society.

UPI is a system that enables peer to peer online payments for users holding different bank accounts, to send and receive money or to pay directly to merchants from their Smartphone without the need to enter bank account information or net banking UserID / Password.

UPI has built on the Immediate Payment Service (IMPS) platform.

How it works

For using Unified Payment Interface, users need to create a Virtual ID or Virtual Payment Address (VPA) of their choice to link it to any bank account. This process doesn't require either the payee or payer to share bank details. The VPA acts as their financial address and users need not remember beneficiary account number, IFSC codes or net banking user id/password for sending or receiving money.

Registration

Steps for Registration:

- User downloads the Unified Payment Interface application from the App Store / Banks website.
- User creates his/ her profile by entering details like name, virtual id (payment address), password etc.
- User goes to "Add/Link/Manage Bank Account" option and links the bank and account number with the virtual id.

Generating M-PIN:

- User selects the bank account from which he/she wants to initiate the transaction.
- User clicks on the given options as required.

Performing a Unified Payment Interface Transaction

PUSH-sending money using virtual address

- User logs in to UPI application.
- After successful login, user selects the option of Send Money / Payment.
- User enters beneficiary's / Payee virtual id, amount and selects account to be debited.
- User gets confirmation screen to review the payment details and clicks on Confirm.
- User now enters MPIN.
- User gets successful or failure message.

PULL-Requesting money

- User logs in to his bank's UPI application.
- After successful login, user selects the option of collect money (request for payment).
- User enters remitters / payers virtual id, amount and account to be credited.
- User gets confirmation screen to review the payment details and clicks on confirm.
- The payer will get the notification on his mobile for request money.
- Payer now clicks on the notification and opens his banks UPI app where he reviews payment request.
- Payer then decides to click on accept or decline.
- In case of accept payment, payer will enter MPIN to authorize the transaction.
- Transaction complete, payer gets successful or decline transaction notification.
- Payee / requester get notification and SMS from bank for credit of his bank account.

Advantages

- With UPI, user's bank account can be used as a wallet with a simplified two-factor authentication which eliminates the need to store funds in any other wallet.
- Use of Virtual ID makes it more secure since there is no need to share credentials.
- UPI transaction can be made via IMPS in real time, which makes it available 24*7.
- Users can link multiple bank accounts to a single Smartphone. Hence sending or receiving money across banks is easier.
- For merchants, it is Suitable for electronic Commerce and a mobile Commerce transaction as well as it resolves the Cash on Delivery collection problem.
- Banks can create their own application interfaces as UPI provides flexibility and an open architecture.

Security Measures

- Beware of Mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store.
- Keep strong passwords for your phone as well as for your UPI application.
- Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.
- Use biometric authentication if possible.
- Update your mobile OS and applications as often as possible to be secure from vulnerabilities.
- It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone.
- Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device, You can contact your subscriber to block the subscription of the SIM card.

- Avoid connecting phones to unsecured wireless networks that do not need passwords to access.

Reference:

http://www.cert-in.org.in/

E-Wallet Security

Security of Electronic-wallets

An Electronic-wallet(e-wallet) is an electronic application that enables online e-commerce transactions like purchasing goods, paying utility bills, transferring money, booking flight etc. with a financial instrument (such as a credit card or a digital currency) using smart phones or computers. A plethora of these e-wallets are provided online for downloading through "apps" to support both point of sale transactions and peer-to-peer transactions between individuals. Being preloaded with currency by the user, they are designed to be convenient to them over the traditional-wallets, by providing better manageability over their payments, accounts, receiving of offers, alerts from merchants, storing digital receipts and warranty information and being secure by requiring to access only through correct passphrase, password and such authentication information.

A number of IT companies, Banks, Telecoms firms, online e-commerce portal, taxi-services, supermarket chains etc. provide e-wallets .

A number of personally identifiable information (PII's) of the customer like his name, mobile phone number and his protected personal information like Customer card numbers, secret PIN, net banking credentials etc is permanently stored in e-wallets, requiring just final authorization from the user through means like biometrics authentication, one-time passwords(OTP) etc. The payment process involves security mechanisms like certificate pinning and use of encryption.

Threats to E-Wallets and countermeasures

Impersonation, SIM swapping

SIM SWAP Impersonation occurs when a fraudster steals information and then poses as a genuine user to do a transaction using the stolen e-wallet details and password.

SIM swaps occurs when fraudsters first collect the user's information, and use it to get his mobile phone SIM card blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudster who then generates one-time passwords using stolen information.

For prevention against Impersonation and SIM swapping attacks:

- Avoid falling prey to social engineering tricks: Financial service providers and support staff will never ask their customers for sharing their private information such as passwords or payment account numbers over email requests or phone inquiries etc.
- Some Mobile network operators send an SMS to alert their customers of a SIM swap, the affected customer can act and stop this fraud in its tracks by contacting the mobile operator immediately.

Man-in-the-middle attack and Phishing

Sophisticated threats like Man-in-the-Browser or Man-in-the-Middle attacks intercept online transactions by reading payment data from the Internet browser while the user is typing his credit card or bank account details. Phishing attacks are used to steal users' login details and personal data, making e-wallet accounts susceptible to fraud.

For prevention against phishing attacks:
The URL of the web-page should be verified, by establishing the authenticity of the website by validating 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 the browser window. Emails or text messages asking the user to confirm or provide personal information (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.

Malware Attacks

Malware attacks on apps have threatened the safety of user's money. An attacker can inject a malware to attack the app and collect details from his phone to misuse it.
For prevention against Malware attacks:
Keep the wallet software up to date: Using the latest version of software allows receiving important stability and security fixes timely. Updates can prevent problems of various severities, include new useful features and help keep the wallet safe. Installing updates for all other software on the computer or mobile is also significant to keep the wallet environment safer.

Use security software: Applications for detecting and removing threats, including firewalls, virus and malware detection and intrusion-detection systems, mobile security solutions should be installed and activated.

Best Practices for Users to remain safe :

- Enable Passwords On Devices: Strong passwords should be enabled on the user's phones, tablets, and other devices before e-wallets can be used. Additional layers of security provided by these devices should be used.
- Use Secure Network Connections: It's important to be connected only to the trusted networks. Avoid the use of public Wi-Fi networks. More secure and trusted WiFi connections identified as "WPA or WPA2" requiring strong passwords should be used.
- Install Apps From Trusted Sources: Reading the user ratings and reviews can provide some clues about the integrity of the e-wallet app. The user must check for the e-wallet provider to be showing strong legacy of securely, reliably and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud).
- Keep Login Credential Secure: Avoid writing down information used to access the digital wallets in plain view or storing them in an unprotected file to avoid their misuse.
- Create a Unique Password for Digital Wallet: Use hard-to-guess password unique to the digital wallet to prevent against the risk of unauthorized access.
- Stay vigilant and aware of cellphone's network connectivity status and register for Alerts through SMS and emails: The user should not switch off his cellphone in the event when numerous annoying calls are received, rather answering the calls should be avoided. This could be a ploy to get him to turn off his phone or put it on silent to prevent him from noticing that his connectivity has been tampered with. The customer should realize that when he is not receiving any calls or SMS notifications for a long time against his e-wallet uses, he should make enquiries with his mobile operator to be sure about not falling victim to such scam.
- Identify Points of Contact in case of Fraudulent Issues: For any fraudulent activity occurring on the user's account in the scenarios like when phone is lost or stolen, an individual card stored in the wallet is lost or account has been hacked, appropriate points of contact for resolving the issues should be understood by the user. The user must completely understand the e-wallet providers contract terms and conditions.

Refrence

http://www.cert-in.org.in/

Micro ATM Security

Security of Micro ATM

Micro ATMs are Point of Sale(PoS)Devices that work with minimal power, connect to central banking servers through GPRS, thereby reducing the operational costs considerably. Micro ATM solution enables the unbanked rural people to easily access micro banking services in a very effective manner.

The basic interoperable transaction types that the micro ATM will support are:

1. Deposit
2. Withdrawal
3. Funds transfer
4. Balance enquiry and mini-statement.

The micro ATM will support the following means of authentication for interoperable transactions:

1. Aadhaar + Biometric
2. Aadhaar + OTP
3. Magnetic stripe card + Biometric
4. Magnetic stripe card + OTP
5. Magnetic stripe card + Bank PIN

Threats to Micro ATMs :

Data Vulnerabilities

With respect to POS data vulnerabilities, there are three specific areas that should be given attention including data in memory; data in transit; data at rest. Data in memory in this context is when the card track data is brought into the system at the POS system via a POI (Point of Interface or some other input device). Data in memory is nearly impossible to defend if an attacker has access to the POS system. Traditionally, data input into the POS system was in memory in clear text, which is what allowed, attackers¿ memory scrapers to be very successful. The way to minimize this risk is by encrypting the card data as soon as possible and keeping it encrypted to the maximum extend throughout its life within the system. Point to Point Encryption (P2PE) could be used to address the issue of encrypting data in memory.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can obtain victim's credit card number using a small electronicCredit Card device near the card acceptance slot and store hundreds of victim's credit card numbers.

Social Engineering

Social engineering involves gaining trust - hence the fraudster poses as a member of staff. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of micro ATM machine and requires assistance.

Best practices for users:

- Before using micro ATM, please ensure that there are no strange objects in the insertion panel of the ATM(to avoid skimming)
- Cover the PIN pas while entering PIN. Destroy the transaction receipts securely after reviewing.

- Change ATM PIN on a regular basis.
- Keep a close eye on bank statements, and dispute any unauthorized charges or withdrawals immediately.
- Shred anything that contains credit card number written on it.(bills etc)
- Notify credit/debit card issuers in advance for change of address.
- Don not accept the card received directly from bank in case if it is damaged or seal is open.
- Do not write PIN number on credit/debit card.
- Do not disclose Credit Card Number/ATM PIN to anyone.
- Do not hand over the card to anyone, even if he/she claims to represent the bank.
- Do not get carried away by strangers who try to help you use the microATM machine.
- Do not transfer or share account details with unknown/non validated source.
- In case of any suspected transactions or loss of cards, contact the service provider/bank immediately.

Best practices for service providers

- The microATM must not transmit any confidential data unencrypted on the network
- The microATM must automatically logout the operator and lock itself after a period of inactivity
- Keep all the microATM software ,application,anitvirus regularly dated
- Educate the customer about basic functionalities and security best practices

Digital Payments

A digital payment, sometimes called an electronic payment, is the transfer of value from one payment account to another using a digital device or channel.

This definition may include payments made with bank transfers, mobile money, QR codes, and payment instruments such as credit, debit, and prepaid cards. Digital payments can be partially digital, primarily digital, or fully digital.phone, POS (Point of Sales) or computer, a digital channel communications. Funds are transferred much faster relative to traditional payment methods like checks.

What is digital payment and its types?

There are different modes and types of digital payments that are prevalent in India, which are discussed in detail in the following lines. Banking Cards. USSD (Unstructured Supplementary Service Data) UPI (United Payment Interface) AEPS (Aadhaar enabled Payment System)

What is the importance of digital payments?

Since electronic payments are made digitally, funds are transferred much faster relative to traditional payment methods like checks. ePayments allow users to make payments online at any time, from anywhere in the world, and also remove the need to go to banks.

What are the benefits of digital payments?

Some of the key advantages of digital payment in India that have made them a preferred choice for transactions are:

1. Faster Payments

Digital payments allow immediate transactions that can be processed immediately, reducing the waiting time that one has to go through with traditional payment methods. This makes transactions seem smooth and efficient.

2. Convenience in the Payment Procedure

Digital payments enable swift and hassle-free transactions from your devices, eliminating the need for physical presence or documents. Whether you're paying bills, shopping online, or transferring funds, digital payment methods offer a user-friendly experience that saves both time and effort.

3. Better Payment Security

Digital payment systems use encryption and system authentication protocols, which minimise the risk of unauthorised access and effectively prevent fraud. Your financial information is protected, keeping you stress-free throughout the entire process of making digital payments.

4. Improved Efficiency

Automation and digitisation in payment processes have significantly enhanced operational efficiency. By minimising manual intervention, errors are reduced, and financial workflows are streamlined, resulting in a more efficient and error-free system.

5. Digital Record of Transactions

Digital payments provide a traceable account of transactions, thereby guaranteeing safety. Such efficiency and credibility allow individuals and businesses to maintain accurate financial records. It is easy to monitor the payment history and can be referred to when required.

6. Reduced Costs

The digital payment framework eliminates the requirement of physical infrastructure, paperwork, and manual handling. This reduces the cost of transactions for business enterprises and financial institutions. Also, digital transactions usually include a lower cost of transfer as compared to traditional banking methods.

7. Ease of Use

The payment systems facilitate customer comfort. The old cash-processing machines that could only recognise clear notes and coins are being replaced by ATMs, which are accessible and easy to use. Digital payment systems are easy to operate and will not take additional effort to understand how they work.

8. Low Fees

Digital payment methods typically entail lower transaction fees compared to banking methods, contributing to overall cost efficiency.

9. Boost Revenue

Merchants can benefit from a wider consumer base and better cash flow by utilising digital payment methods, leading to higher revenue. Digital payments offer an efficient system,

leading to higher customer satisfaction and smoother transactions, which can attract more customers in the future.

10. Discounts and Savings
Many online platforms provide discounts, cashback, or loyalty programmes. These discounts motivate the customers to go for the digital payment option, which saves them money and provides several benefits.

11. Low Risk of Theft
Digital payments diminish the possibility of the actual loss of money since it's not physical. Transactions occur in the digital world, therefore rendering the necessity of holding large amounts of currency physically unnecessary. This safeguards payments by preventing direct cash transactions and ensuring their protection.

12. Customer Management
Digital payment systems can frequently oversee and monitor the customers' transactions, preferences, and feedback, which gives the business more control over these aspects. This improves overall customer management by adjusting service offerings based on customer behaviour.

13. Better Customer Experience
The ease and convenience offered by digital payments enable customers to enjoy superior service, thereby enhancing their experience. Simplified payment processes result in increased customer satisfaction and a greater likelihood of future collaboration with the business.

14. Efficient Record-Keeping Features
Through the digital infrastructure, digital payments for offline businesses are recorded efficiently; thus, the business environment is friendlier than before. Today businesses and individuals can easily track, control, and analyse their financial activities to obtain financial transparency and improve the financial management process.

e-Payments allow users to make payments online at any time, from anywhere in the world, and also remove the need to go to banks. As part of the 'Digital India' campaign, the government has an aim to create a 'digitally empowered' economy that is 'Faceless, Paperless, Cashless'.

Digital payments are broadly classified as follows:
A partially digital payment
In a partially digital payment scenario, both the payer and the payee utilize cash through intermediaries (a third-party agent), while payment providers facilitate the digital transfer of funds between these intermediaries.

A primary digital payment
In a primarily digital payment scenario, the payer initiates a digital payment to an intermediary, who in turn receives the digital payment, but the payee receives the payment in cash from that intermediary.

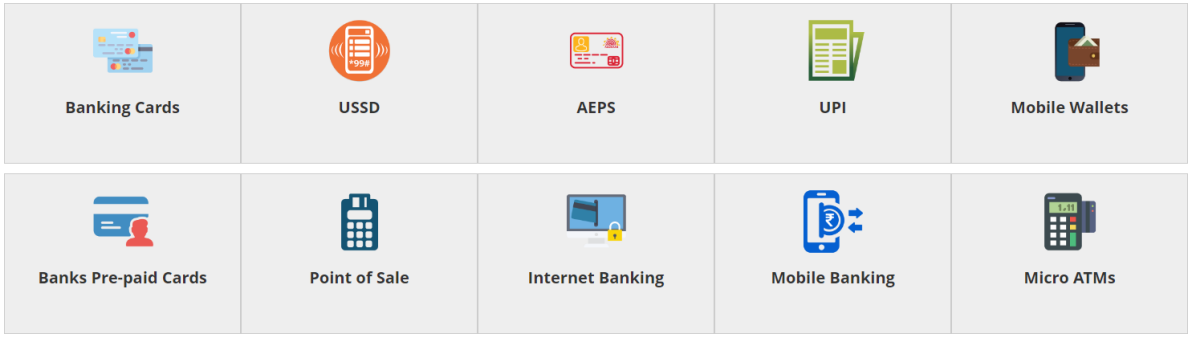
A fully digital payment
A fully digital payment refers to a situation in which the payer initiates the payment digitally to a payee who receives it digitally, and it is then kept and spent digitally.

Digital payments are encrypted to protect critical data during transmission and storage to ensure its confidentiality and integrity using a variety of technologies, including encryption, tokenization, and secure socket layer (SSL/ TLS) certificates.

Modes of Digital Payment

The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy. "Faceless, Paperless, Cashless" is one of professed role of Digital India.

As part of promoting cashless transactions and converting India into less-cash society, various modes of digital payments are available.



#1: Banking Cards Indians widely use Banking cards, or debit/credit cards, or prepaid cards, as an alternative to cash payments. Andhra Bank launched the first credit card in India in 1981. These cards provide 2 factor authentication for secure payments e.g secure PIN and OTP. RuPay, Visa, MasterCard are some of the example of card payment systems. Payment cards give people the power to purchase items in stores, on the Internet, through mail-order catalogues and over the telephone. They save both customers and merchants' time and money, and thus enable them for ease of transaction. Cards are preferred because of multiple reasons, including, but not limited to, convenience, portability, safety, and security. This is the only mode of digital payment that is popular in online transactions and physical transactions alike. Nowadays, many apps are being launched with the sole purpose of managing card transactions like Cred, Square, etc.

#2: Unstructured Supplementary Service Data(USSD)

USSD was launched for those sections of India's population which don't have access to proper banking and internet facilities. Under USSD, mobile banking transactions are possible without an internet connection by simply dialing *99# on any essential feature phone.
This number is operational across all Telecom Service Providers (TSPs) and allows customers to avail of services including interbank account to account fund transfer, balance inquiry, and availing mini statements. Around 51 leading banks offer USSD service in 12 different languages, including Hindi & English.

#3: Aadhaar Enabled Payment System (AEPS)

AEPS is a bank-led model for digital payments that was initiated to leverage the presence and reach of Aadhar. Under this system, customers can use their Aadhaar-linked accounts to transfer money between two Aadhaar linked Bank Accounts. As of February 2020, AEPS had crossed more than 205 million as per NPCI data.

AEPS doesn't require any physical activity like visiting a branch, using debit or credit cards or making a signature on a document. This bank-led model allows digital payments at PoS (Point of Sale / Micro ATM) via a Business Correspondent(also known as Bank Mitra) using Aadhaar authentication. The AePS fees for Cash withdrawal at BC Points are around Rs.15.

#4: Unified Payments Interface (UPI)

UPI is a payment system that culminates numerous bank accounts into a single application, allowing the transfer of money easily between any two parties. As compared to NEFT, RTGS, and IMPS, UPI is far more well-defined and standardized across banks. You can use UPI to initiate a bank transfer from anywhere in just a few clicks.

The benefit of using UPI is that it allows you to pay directly from your bank account, without the need to type in the card or bank details. This method has become one of the most popular digital payment modes in 2020, with October witnessing over 2 billion transactions.

#5: Mobile Wallets

Mobile Wallets, as the name suggests, are a type of wallet in which you can carry cash but in a digital format. Often customers link their bank accounts or banking cards to the wallet to facilitate secure digital transactions. Another way to use wallets is to add money to the Mobile Wallet and use the said balance to transfer money.

Nowadays, many banks have launched their wallets. Additionally, notable private companies have also established their presence in the Mobile Wallet space. Some popularly used ones include Paytm, Freecharge, Mobikwik, mRupee, Vodafone M-Pesa, Airtel Money, Jio Money, SBI Buddy, Vodafone M-Pesa, Axis Bank Lime, ICICI Pockets, etc.

#6: Bank Prepaid Cards

A bank prepaid card is a pre-loaded debit card issued by a bank, usually single-use or reloadable for multiple uses. It is different from a standard debit card because the latter is always linked with your bank account and can be used numerous times. This may or may not apply to a prepaid bank card. A prepaid card can be created by any customer who has a KYC-complied account by merely visiting the bank's website. Corporate gifts, reward cards, or single-use cards for gifting purposes are the most common uses of these cards.

#7: PoS Terminals

PoS(Point of Sale) is known as the location or segment where a sale happens. For a long time, PoS terminals were considered to be the checkout counters in malls and stores where the payment was made. The most common type of PoS machine is for Debit and Credit cards, where customers can make payment by simply swiping the card and entering the PIN.

With digitization and the increasing popularity of other online payment methods, new PoS methods have come into the picture. First is the contactless reader of a PoS machine, which can debit any amount up to Rs. 2000 by auto-authenticating it, without the need of a Card PIN.

#8: Internet Banking

Internet Banking, also known as e-banking or online banking, allows the customers of a particular bank to make transactions and conduct other financial activities via the bank's website. E-banking requires a steady internet connection to make or receive payments and access a bank's website, which is called Internet Banking.

Today, most Indian banks have launched their internet banking services. It has become one of the most popular means of online transactions. Every payment gateway in India has a virtual banking option available. NEFT, RTGS, or IMPS are some of the top ways to make transactions via internet banking.

#9: Mobile Banking

Mobile banking refers to the act of conducting transactions and other banking activities via mobile devices, typically through the bank's mobile app. Today, most banks have their mobile banking apps that can be used on handheld devices like mobile phones and tablets and sometimes on computers.

Mobile banking is known as the future of banking, thanks to its ease, convenience, and speed. Digital payment methods, such as IMPS, NEFT, RTGS, IMPS, investments, bank statements, bill payments, etc., are available on a single platform in mobile banking apps. Banks themselves encourage customers to go digital as it makes processes easier for them too.

#10: Micro ATMs

Micro ATM is a device for Business Correspondents (BC) to deliver essential banking services to customers. These Correspondents, who could even be a local store owner, will serve as a 'micro ATM' to conduct instant transactions. They will use a device that will let you transfer money via your Aadhaar linked bank account by merely authenticating your fingerprint. Essentially, Business Correspondents will serve as banks for the customers. Customers need to verify their authenticity using UID(Aadhaar). The essential services that will be supported by micro ATMs are withdrawal, deposit, money transfer, and balance inquiry. The only requirement for Micro ATMs is that you should link your bank account to Aadhaar.

#11.Bharat Interface for Money (BHIM):

Bharat Interface for Money (BHIM) is a mobile app for easy and quick payment transactions using Unified Payments Interface (UPI). User can make instant bank-to-bank payments and pay and collect money using Mobile number, Bank a/c and IFSC code, Aadhaar number or Virtual Payment Address (VPA). BHIM has the facility to scan & pay through QR code. User can check transaction history and can also raise complaint for the declined transactions by clicking on Report issue in transactions.

BHIM is available in 20 regional languages (English, Hindi, Marathi, Tamil, Telugu, Malayalam, Oriya, Punjabi, Gujarati, Marwari, Haryanvi, Bhojpuri, Urdu, Konkani, Manipuri, Mizo, Khasi, Kannada, Bengali, Assamese) for better user experience. Users can also make transaction using from their feature phone as well by dialling *99#.

#12.UPI 123PAY:

UPI 123PAY is an instant payment system for feature phone users who can use Unified Payments Interface (UPI) payment service in a safe and secure manner. Feature phone users will now be able to undertake a host of transactions based on four technology alternatives. They include calling an IVR (interactive voice response) number, app functionality in feature phones, missed call-based approach and proximity sound-based payments.

#13.UPI Lite:

"UPI LITE" offers a wallet in BHIM-UPI app for an amount of up to ₹2,000 on a smart phone, eliminating the need for the user to first obtain electronic authorisation from his/her bank while making the payment, offering the user better experience in terms of improved speed and transaction success rate.

#14.National Electronic Toll Collection (NETC) FASTag NETC FASTag provides an easy and convenient digital payment mechanism for topayments. This is an interoperable solution

available to individuals nationwide. With the use of Radio Frequency Identification (RFID) technology, the FASTag device allows for making toll payments directly while the individuals vehicle is in motion.

#15. e-RUPI

e-RUPI is a person and purpose specific, contactless and cashless digital payment solution. It can be issued as a prepaid QR code or SMS based electronic voucher which can be used by the Government/Private organizations for delivery of a specific subsidy or welfare benefit to the targeted citizens. The beneficiaries will be able to redeem e-RUPI voucher without a card, digital payments app or internet banking access, at the merchants accepting e-RUPI, simply by showing SMS or QR code.This contactless e-RUPI is easy, safe, and secure as it keeps the details of the beneficiaries completely confidential. The entire transaction process through this voucher is relatively faster and at the same time reliable, as the required amount is already stored in the voucher.

Different fund transfer systems in india

1. **National Electronic** Funds **Transfer** (NEFT) NEFT is a nationwide payment system facilitating one-to-one **fund transfer**. It operates on a deferred settlement basis, where transactions are processed in batches during specific timings.NEFT transactions are not instantaneous and can take up to a few hours for the funds to be credited to the beneficiary account.There is no minimum or maximum limit for NEFT transactions, but individual banks may impose limits. For carrying out NEFT, you need to have the receiver's bank account number and the bank's IFSC code.
2. **RTGS (Real Time Gross Settlement):**
   RTGS is also an electronic fund transfer system used for large-value transactions.It operates on a real-time basis, meaning transactions are processed immediately and on an individual basis.RTGS transactions are instantaneous and final, with immediate transfer of funds from the remitter's account to the beneficiary's account.RTGS is typically used for high-value transactions, as it usually involves significant fees.
3. **UPI (Unified Payments Interface)**:
   UPI is a real-time payment system that allows users to transfer money between any two bank accounts using a smartphone.It enables instant transfer of funds 24x7, including weekends and holidays.UPI transactions can be initiated using a mobile app, and they require a virtual payment address (VPA), account number, or Aadhaar number of the beneficiary.UPI has gained popularity for its convenience, speed, and interoperability across banks and payment service providers.
4. **IMPS (Immediate Payment Service)**:
   IMPS is an instant payment system that enables interbank electronic fund transfers in real time.It allows customers to transfer funds using mobile phones or internet banking on a 24x7 basis.IMPS transactions can be initiated using the beneficiary's mobile number and MMID (Mobile Money Identifier) or account number and IFSC (Indian Financial System Code).IMPS is widely used for person-to-person (P2P) transfers, bill payments, and other purposes requiring immediate fund transfer.

Digital payments related common frauds and preventive measures

Payment fraud pertains to any illegitimate or unlawful transaction conducted by a cybercriminal. Using the Internet, the criminal deprives the victim of money, valuables, interests, or private information.

There are three ways to define payment fraud:

1. Fraudulent or unauthorized transactions
2. Lost or stolen merchandise
3. False requests for a refund, return, or bounced check

E-commerce companies charge clients for goods and services mainly through electronic transactions, which has led to an increase in fraudulent operations.

What are the types of payment fraud?

Payment fraud arises in numerous ways, as fraudulent actors use many techniques to take advantage of weaknesses in payment systems. Some of the most popular techniques are as follows:

Skimming

Criminals utilize the skimming technique to steal credit or debit card information. They attach tiny gadgets known as “skimmers” on card readers at ATMs or point-of-sale (POS) terminals. The skimmer captures card information when a user swipes their card at an ATM, which fraudsters use to make fake cards or conduct unauthorized transactions.

Identity theft

Identity theft happens when a fraudster acquires and utilizes another person’s personal information, such as their credit card number, bank account information, or social security number, to open new accounts, make unauthorized transactions, or engage in other types of fraud. Hackers can penetrate firewalls by using outdated security measures or by stealing login credentials from public Wi-Fi.

Phishing

Phishing is when people try to trick you into giving them sensitive information like your login details, credit card numbers, or personal data. They might pretend to be someone you trust, like your bank, but if you don’t recognize the source, it could be a scam. Be careful and always double-check before giving out any important information.

False chargebacks

Chargeback fraud occurs when a customer uses their credit card to make a purchase and then falsely disputes the charge with the card issuer, claiming that they did not receive the merchandise or that the transaction was unauthorized. This type of fraud is also known as “friendly fraud.” The fraudster aims to obtain a refund while retaining the goods or services.

Business email compromise

BEC is a type of payment fraud where scammers pretend to be executives or vendors to trick employees into giving them money or personal information. They do this by hacking or spoofing email accounts and using social engineering tricks to deceive the victims.

Card-not-present scam

CNP fraud is a fraudulent transaction that occurs when the card is not physically present, like in online or over-the-phone purchases. Fraudsters use stolen credit card information to make unauthorized purchases, which can be challenging to detect and prevent since there is no physical verification of the card.

Pagejacking

E-commerce website owners should be aware of potential hacking threats. Hackers can steal a portion of the website and redirect traffic to a harmful website, which could lead to a breach in network security. Vigilance is necessary to prevent any dubious internet activity from causing harm to the business.

Merchant identity fraud

Scammers utilize a particular strategy to utilize stolen credit cards by creating a merchant account that seems like it belongs to a legitimate company. The hackers vanish before the cardholders realize the unauthorized payments and try to cancel the transactions. Consequently, the payment facilitator becomes accountable for the financial loss and additional expenses linked to credit card chargebacks.

Advanced fee and wire transfer scams

Hackers frequently target credit card users and e-commerce store owners by tricking them into paying in advance for a credit card or by offering money at a later date. This deceitful tactic is aimed at exploiting unsuspecting individuals and businesses with the ultimate goal of stealing money or sensitive financial information.

Everyone needs to remain vigilant and cautious when dealing with such offers and to always verify the legitimacy of any requests before making any payments or divulging personal information.

RBI guidelines on digital payments and customer protection in unauthorised banking transactions

Here are the RBI's guidelines regarding UPI fraud –

1. The banks must have a dedicated framework for their customers to report cases of such fraud. This ensures quick actions can be taken.
2. Banks need to be prompt and accurate in reporting all the fraudulent activities associated with UPI transactions to the RBI.
3. Banks should also focus on 'Fraud Prevention and Management Function' to launch investigations into such matters. They must also engage with law enforcement agencies to start the process of catching the apprehenders.
4. The CEO, audit committee, and a special committee of the bank must oversee all such fraud protection and risk management investigations.
5. Additionally, after approval from their board, each bank must frame its internal fraud detection and investigation policies.
6. Banks are mandated to send all Fraud Monitoring Returns (FMR) using the XBRL system. Furthermore, banks must nominate General Manager Designation personnel to manage this process.
7. Also, banks must engage in educating customers regarding the latest frauds and safe digital payment practices.

Besides these guidelines, RBI has a clear framework regarding the refund against such fraudulent activities. Here are the details –

Within 3 days: According to the apex bank of India, if you, as a customer, report any incident of a fraudulent transaction within 3 days of the incident, then you will bear zero liability for it. As a result, the total amount will be refunded to your respective bank account.
Within 4-7 days: If you register your complaint after 3 days and between 7 days of the fraudulent transaction, then you will have to bear the limited liability of INR 5,000 to INR 25,000, whichever is lower. After deducting the lowest amount, the rest of it will be returned to you.
After 7 days: If you fail to report such unauthorised transactions within 7 days, the bank will not be liable to refund any amount to you.

The PSS Act, 2007 provides for the regulation and supervision of payment systems in India and designates the Reserve Bank of India (Reserve Bank) as the authority for that purpose and all related matters. The objectives of the Payment and Settlement System Act, 2007 are to regulate and supervise payment methods through-out India. The Act vests RBI as the supreme authority and grant powers and to regulate payment gateways. It also provides legal framework for 'netting' and 'settlement finality'.

The objectives of the Payment and Settlement System Act, 2007 are to regulate and supervise payment methods through-out India. The Act vests RBI as the supreme authority and grant powers and to regulate payment gateways. It also provides legal framework for ‘netting’ and ‘settlement finality’. The RBI established a Board consisting of industry experts for Regulation and Supervision of Payment and Settlement Systems as a central body with the jurisdiction to control and oversee payment and settlement systems (BPSS). The Payment and Settlement Systems Regulations, 2008 were also produced by the RBI. The two regulations went into effect on August 12th, 2008.

The 2008 Payment and Settlement Systems Regulations has the following goals:

1.It covers topics pertaining to the format of an application to allow starting/operating a payment system as well as the granting of authorization.
2.It establishes the standard for payment systems and specifies payment instructions.
3.It includes topics pertaining to the delivery of returns, documents, or other information.
4.It also covers how system providers produce accounting and balance sheets.

Authorization of payment system

Section 4 of the PSS Act grants powers only to RBI to operate or launch any payment system, and anyone else who wants to do so must apply to RBI for permission under Section 5 of the Act in order to do so. The authorisation request must be submitted using Form A in accordance with PSS Regulations, 2008, Regulation 3(2). The application must be completed and sent to the RBI together with the necessary paperwork and a cost of 10,000. The application fee can be paid in cash, cashier's checks, demand draughts, money orders, checks payable to RBI, or electronic fund transfers. It can also be submitted electronically. The RBI must grant permission for the system providers running the payment systems or wishing to establish such a payment system via this link. Under this Act, any unlawful use of a payment system would constitute a crime and be subject to punishment.