UNIT 4 Notes

Online Banking Security

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.

Reference:

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

Definition of E- Commerce

What is e-commerce in cyber security?

Ecommerce security refers to **the measures taken to protect your business and your customers against cyber threats**.
E-Commerce or Electronic Commerce means buying and selling of goods, products, or services over the internet. E-commerce is also known as electronic commerce or internet commerce. These services provided online over the internet network. 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). The standard definition of E-commerce is a commercial transaction which is happened over the internet. Online stores like Amazon, Flipkart, Shopify, Myntra, Ebay, Quikr, Olx are examples of E-commerce websites. By 2020, global retail e-commerce can reach up to $27 Trillion. Let us learn in detail about what is the advantages and disadvantages of E-commerce and its types.

E-Commerce or Electronic Commerce

E-commerce is a popular term for electronic commerce or even internet commerce. The name is self-explanatory, it is the meeting of buyers and sellers on the internet. This involves the transaction of goods and services, the transfer of funds and the exchange of data.

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 $27 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.

What is m-Commerce?

Examples of E-Commerce

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

Advantages of E-Commerce

- 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.
- 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.
- 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.

- 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.
- 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

- 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.
- 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.
- 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.
- 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.
- 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?

Having good cybersecurity is extremely important in e-commerce, as **it allows you to protect your company and your customers from cybercriminals**. Like it or not, it guarantees a better shopping experience in your online store.

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.

In e-commerce, cybersecurity is primarily aimed at protecting consumer data. In this way, it must prevent data such as address, telephone, CPF, credit card numbers and navigation data, for example, from being leaked or used by people with bad intentions.

Therefore, cybersecurity is premised on ensuring:

- **Reliability**: only authorized persons can have access to systems and data;
- **Integrity**: data cannot be altered or deleted without authorization;
- **Authenticity**: The identity of the people who send data to your company must be preserved.

For this, your company's cybersecurity must be dedicated to protecting servers, databases, networks and endpoints. It must find vulnerabilities and fix them before cybercriminals do. This is, in short, a task that requires great efforts and a good budget.

IMPORTANCE IN E-COMMERCE

Having good cybersecurity is extremely important in e-commerce, as it allows you to protect your company and your customers from cybercriminals. Like it or not, it guarantees a better shopping experience in your online store.

In order for people to be able to shop at your online store, they need to feel secure enough to enter personal details and payment details. This is a process that requires a lot of trust. One slip here and trust goes down the drain.

That's what cybersecurity is for. Without it, consumers are vulnerable. But with it, consumers can buy without fear. So be sure to invest in it.

Why cyber security matters 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

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.

Ecommerce Security: Importance, Issues & Protection Measures

What is eCommerce or electronic commerce security?

eCommerce security is the guideline that ensures safe transactions through the internet. It consists of protocols that safeguard people who engage in online selling and buying goods and services. You need to gain your customers' trust by putting in place eCommerce security basics. Such basics include:

- Privacy
- Integrity
- Authentication
- Non-repudiation

1. Privacy

Privacy includes preventing any activity that will lead to the sharing of customers' data with unauthorized third parties. Apart from the online seller that a customer has chosen, no one else should access their personal information and account details.

A breach of confidentiality occurs when sellers let others have access to such information. An online business should put in place at least a necessary minimum of anti-virus, firewall, encryption, and other data protection. It will go a long way in protecting credit card and bank details of clients.

2. Integrity

Integrity is another crucial concept of eCommerce Security. It means ensuring that any information that customers have shared online remains unaltered. The principle states that the online business is utilizing the customers' information as given, without changing anything. Altering any part of the data causes the buyer to lose confidence in the security and integrity of the online enterprise.

3. Authentication

The principle of authentication in eCommerce security requires that both the seller and the buyer should be real. They should be who they say they are. The business should prove that it is real, deals with genuine items or services, and delivers what it promises. The clients should also give their proof of identity to make the seller feel secure about the online transactions. It is possible to ensure authentication and identification. If you are unable to do so, hiring an expert will help a lot. Among the standard solutions include client login information and credit card PINs.

4. Non-repudiation

Repudiation means denial. Therefore, non-repudiation is a legal principle that instructs players not to deny their actions in a transaction. The business and the buyer should follow through on the transaction part that they initiated. eCommerce can feel less safe since it occurs in cyberspace with no live video. Non-repudiation gives eCommerce security another layer. It confirms that the communication that occurred between the two players indeed reached the recipients. Therefore, a party in that particular transaction cannot deny a signature, email, or purchase.

Common Ecommerce Security Issues

1. Lack of trust in the privacy and eCommerce security

Businesses that run eCommerce operations experience several security risks, such as:

- **Counterfeit sites**– hackers can easily create fake versions of legitimate websites without incurring any costs. Therefore, the affected company may suffer severe damage to its reputations and valuations.
- **Malicious alterations to websites**– some fraudsters change the content of a website. Their goal is usually to either divert traffic to a competing website or destroy the affected company's reputation.
- **Theft of clients' data**– The eCommerce industry is full of cases where criminals have stolen the information about inventory data, personal information of customers, such as addresses and credit card details.
- **Damages to networks of computers**– attackers may damage a company's online store using worm or viruses attacks.
- **Denial of service**– some hackers prevent legit users from using the online store, causing a reduction in its functioning.
- **Fraudulent access to sensitive data**– attackers can get intellectual property and steal, destroy, or change it to suit their malicious goals.

2. Malware, viruses, and online frauds

these issues cause losses in finances, market shares, and reputations. Additionally, the clients may open criminal charges against the company. Hackers can use worms, viruses, Trojan horses, and other malicious programs to infect computers and computers in many different ways. Worms and viruses invade the systems, multiply, and spread. Some hackers may hide Trojan horses in fake software, and start infections once the users download the software. These fraudulent programs may:

- hijack the systems of computers
- erase all data
- block data access
- forward malicious links to clients and other computers in the network.

3. Uncertainty and complexity in online transactions

Online buyers face uncertainty and complexity during critical transaction activities. Such activities include payment, dispute resolution, and delivery. During those points, they are likely to fall into the hands of fraudsters.

Businesses have improved their transparency levels, such as clearly stating the point of contact when a problem occurs. However, such measures often fail to disclose fully the collection and usage of personal data.

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.

2. 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.

3. 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

E-commerce securities

WHAT IS E-COMMERCE SECURITY

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

6 dimensions of e-commerce security

1. Integrity: prevention against unauthorized data modification
2. Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
3. Authenticity: authentication of data source
4. Confidentiality: protection against unauthorized data disclosure
5. Privacy: provision of data control and disclosure
6. Availability: prevention against data delays or removal

E-COMMERCE THREATS

Threats: anyone with the capability, technology, opportunity, and intent to do harm.Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element.Terrorists, insiders, disgruntled employees, and hackers are included in this profile (President's Commission on Critical Infrastructure Protection)

1. Intellectual property threats -- use existing materials found on the Internet without the owner's permission, e.g., music downloading, domain name (cybersquatting), software pirating

2. Client computer threats
   - Trojan horse
   - Active contents
   - Viruses

3. Communication channel threats
   - Sniffer program
   - Backdoor
   - Spoofing
   - Denial-of-service

4. Server threats
   - Privilege setting
   - Server Side Include (SSI), Common Gateway Interface (CGI)
   - File transfer
   - Spamming

ELECTRONIC PAYMENT SYSTEMS

A medium of payment between remote buyers and sellers in cyberspace: electronic cash, software wallets, smart cards, credit/debit cards.

Offline payment methods

Number of transactions: cash (42%), check (32%), credit card (18%) (Figure 6.1)

Dollar amount: check(52%), credit card (21%), cash (17%) (Figure 6.2)

Payment systems	Properties	Costs	Advantages	Disadvantages
Electronic	– 31%	– Internet cash	– Efficient	– Money

cash e.g., PayPal	of US population do not have credit cards — micropayments (< $10) — Independent — Portable — Divisible	transfer: no fixed cost of hardware — No distance costs — Small processing fee to banks	— Less costly	laundering — Forgery — Low acceptance — Multiple standards
Electronic wallets e.g., Passport	— Stores shipping & billing information — Encrypted digital certificate	— Lengthy download for client-side wallets	— Enter information into checkout forms automatically	— Client-side wallets are not portable — Privacy issue for server-side wallets
Smart cards e.g., Blue	— Embedded microchip storing encrypted personal information	— Time value of money	— Convenience	— Need a card reader — Card theft — Low acceptance
Credit cards e.g., VeriSign	— Line of credit — Purchase dispute protection — Secure Electronic Transaction (SET) Protocol	— Unpaid balance charge — $50 limit on frauds — Processing fee	— Most popular — Worldwide acceptance	— Costly

Different Types of Threat to E-Commerce

E-commerce is basically the process of buying and selling commodities and goods over the Internet. In E-commerce, transactions take place via digital methods via electronic funds and the processing of online transactions.

Since E-commerce deals with the transfer of money digitally, hackers and attackers use this as an opportunity to break into E-commerce websites and gain some financial profit from them.

E-commerce Security:

- E-commerce Security basically deals with a set of protocols specially designed for E-commerce platforms to process electronic transactions with security. E-commerce Security helps to buy and sell goods over the Internet with full protection and security.
- The absence of E-commerce Security leads to the loss of the banking credentials of the customers, the leaking of private sensitive information of users, phishing attacks, stealing of money, and frauds related to credit cards.
- Electronic payment system which is an essential part of E-commerce Security helps to operate in a user-friendly manner and avoids difficult documentation procedures and also saves some cost of transactions.
- E-commerce Security enables to provide security to Electronic payment systems so that they can easily process the data and transfer electronic funds with security in an easy manner.

Types of threats to E-commerce:

- **Tax Evasion:** Organizations show the legal paper records of revenue to the IRS. But in the case of E-commerce shopping, online transactions take place due to which funds get transferred electronically due to which IRS is not able to count the transactions properly and there are high chances of tax evasions by these organizations.
- **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.
- **Middlemen 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.

Prevent threats:

We can prevent the following E-commerce threats in the following ways:

- **Anti-malware:** We can deploy Anti-malware and Anti-virus software on all our computer systems so that we can prevent these conditions to happen. Anti-malware and Anti-virus software prevent all types of malware and viruses to infect the data on our computer.

- **HTTPS:** HTTPS helps to keep the website data secure from any kind of digital attack. SSL and HTTPS encrypt all the data of the users which is harder to crack by the hackers.
- **Payment gateway:** We can secure the payment gateway used on the E-commerce websites which very high security and strict policies against leaking of any financial credentials of any user.

Threat to E-Commerce

E-Commerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc.

Electronic payments system:

With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, colour, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labour cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system.

The Risk of Fraud

An electronic payment system has a huge risk of fraud. The computing devices use an identity of the person for authorizing a payment such as passwords and security questions. These authentications are not full proof in determining the identity of a person. If the password and the answers to the security questions are matched, the system doesn't care who is on the other side. If someone has access to our password or the answers to our security question, he will gain access to our money and can steal it from us.

The Risk of Tax Evasion

The Internal Revenue Service law requires that every business declare their financial transactions and provide paper records so that tax compliance can be verified. The problem with electronic systems is that they don't provide cleanly into this paradigm. It makes the process of tax collection very frustrating for the Internal Revenue Service. It is at the business's choice to disclose payments received or made via electronic payment systems. The IRS has no way to know that it is telling the truth or not that makes it easy to evade taxation.

The Risk of Payment Conflicts

In electronic payment systems, the payments are handled by an automated electronic system, not by humans. The system is prone to errors when it handles large amounts of payments on a frequent basis with more than one recipients involved. It is essential to continually check our pay slip after every pay period ends in order to ensure everything makes sense. If it is a failure to do this, may result in conflicts of payment caused by technical glitches and anomalies.

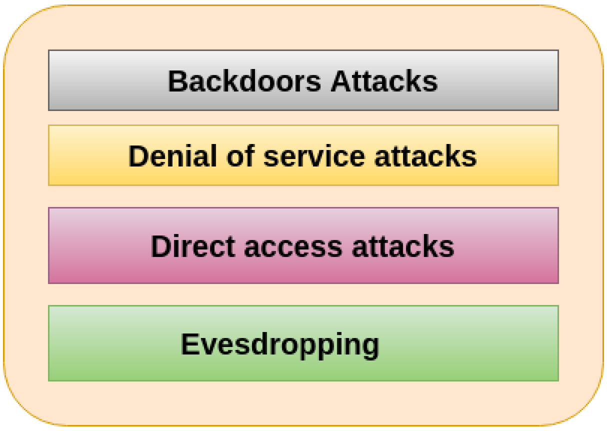
E-cash

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.

E-cash has four major components-

1. **Issuers** - They can be banks or a non-bank institution.
2. **Customers** - They are the users who spend the e-cash.
3. **Merchants or Traders** - They are the vendors who receive e-cash.
4. **Regulators** - They are related to authorities or state tax agencies.

In e-cash, we stored financial information on the computer, electronic device or on the internet which is vulnerable to the hackers. Some of the major threats related to e-cash system are-



E-cash Threats

Backdoors Attacks

It is a type of attacks which gives an attacker to unauthorized access to a system by bypasses the normal authentication mechanisms. It works in the background and hides itself from the user that makes it difficult to detect and remove.

Denial of service attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

Direct Access Attacks

Direct access attack is an attack in which an intruder gains physical access to the computer to perform an unauthorized activity and installing various types of software to compromise security. These types of software loaded with worms and download a huge amount of sensitive data from the target victims.

Eavesdropping

This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

Credit/Debit card fraud

A credit card allows us to borrow money from a recipient bank to make purchases. The issuer of the credit card has the condition that the cardholder will pay back the borrowed money with an additional agreed-upon charge.

A debit card is of a plastic card which issued by the financial organization to account holder who has a savings deposit account that can be used instead of cash to make purchases. The debit card can be used only when the fund is available in the account.

Some of the important threats associated with the debit/credit card are-

ATM (Automated Teller Machine)-

It is the favourite place of the fraudster from there they can steal our card details. Some of the important techniques which the criminals opt for getting hold of our card information is:

Skimming-

It is the process of attaching a data-skimming device in the card reader of the ATM. When the customer swipes their card in the ATM card reader, the information is copied from the magnetic strip to the device. By doing this, the criminals get to know the details of the Card number, name, CVV number, expiry date of the card and other details.

Unwanted Presence-

It is a rule that not more than one user should use the ATM at a time. If we find more than one people lurking around together, the intention behind this is to overlook our card details while we were making our transaction.

Vishing/Phishing

Phishing is an activity in which an intruder obtained the sensitive information of a user such as password, usernames, and credit card details, often for malicious reasons, etc.

Vishing is an activity in which an intruder obtained the sensitive information of a user via sending SMS on mobiles. These SMS and Call appears to be from a reliable source, but in real they are fake. The main objective of vishing and phishing is to get the customer's PIN, account details, and passwords.

Online Transaction

Online transaction can be made by the customer to do shopping and pay their bills over the internet. It is as easy as for the customer, also easy for the customer to hack into our system and steal our sensitive information. Some important ways to steal our confidential information during an online transaction are-

- By downloading software which scans our keystroke and steals our password and card details.
- By redirecting a customer to a fake website which looks like original and steals our sensitive information.
- By using public Wi-Fi

POS Theft

It is commonly done at merchant stores at the time of POS transaction. In this, the salesperson takes the customer card for processing payment and illegally copies the card details for later use.

E-Commerce security best practices Good Link:

Best eCommerce platforms in 2023

For some time now, the growth of e-commerce has been exponential, so it is not uncommon for there to be countless programs to create virtual stores.

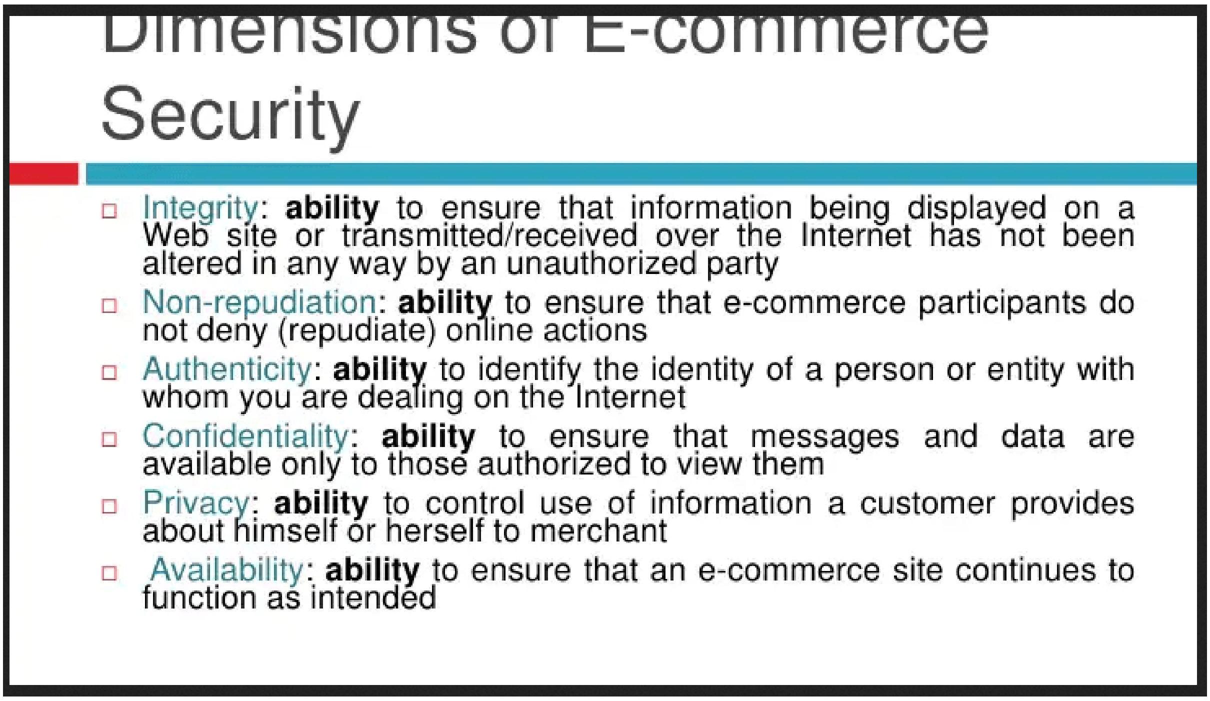
When we consider opening our online store, we will have to be very clear about both the current needs and the possible future needs of it, to choose the most optimal software.

If we had to choose 12 platforms to create e-commerce, these would be the ones that, without a doubt, we would take into account:

- Shopify
- Magento Commerce

- Template Monster
- 3DCart
- BigCommerce
- WooCommerce
- Salesforce Commerce Cloud
- Squarespace
- Yo!Kart
- Volusion
- Prestashop
- Wix

What is eCommerce security?



Dimensions of E-commerce Security

- □ Integrity: **ability** to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorized party
- □ Non-repudiation: **ability** to ensure that e-commerce participants do not deny (repudiate) online actions
- □ Authenticity: **ability** to identify the identity of a person or entity with whom you are dealing on the Internet
- □ Confidentiality: **ability** to ensure that messages and data are available only to those authorized to view them
- □ Privacy: **ability** to control use of information a customer provides about himself or herself to merchant
- □ Availability: **ability** to ensure that an e-commerce site continues to function as intended

Ecommerce security meaning – It is the guideline that ensures safe transactions on an ecommerce web store. It consists of protocols that safeguard people who engage in online selling and buying goods and services. You need to gain your customers' trust by putting in place eCommerce security basics.
For these reasons, security systems have been developed for Internet transactions: Encryption, Digital Signature, and Quality Certificate, which guarantee confidentiality, integrity and authenticity respectively.

For this reason, it is essential to bet on a series of specialized ecommerce security solutions aimed at protecting your digital environment. Consider these security challenges in consumer-oriented eCommerce before you think of opening an ecommerce website.
You must earn the trust of your customers by putting the fundamentals into practice. These fundamentals include:

- **Privacy**

Privacy includes the prevention of any activity that will lead to the sharing of customer data with unauthorized third parties.

Other than the online seller that a customer has chosen, no one else should access their personal information and account details.

- **Integrity**

Integrity is another crucial concept . This means ensuring that all the information that customers have shared online remains unchanged.

The principle states that online commerce uses customer information as it is given, without changing anything. Altering any part of the data causes the buyer to lose confidence in the security and integrity of the online business.

- **Authentication**

The principle of authentication in security requires both seller and buyer to be real.

Customers are also required to provide proof of identity to make the seller feel secure when transacting online. It is possible to provide authentication and identification.

If you can’t do it, bringing in an expert will help a lot.

- **Non-repudiation**

Repudiation means denial. Therefore, non-repudiation is a legal principle that requires players not to deny their actions in a transaction.

The company and the buyer must follow up on the part of the transaction that they have initiated. Ecommerce may seem less secure because it takes place in cyberspace without live video. Non-repudiation gives e-commerce security another layer.

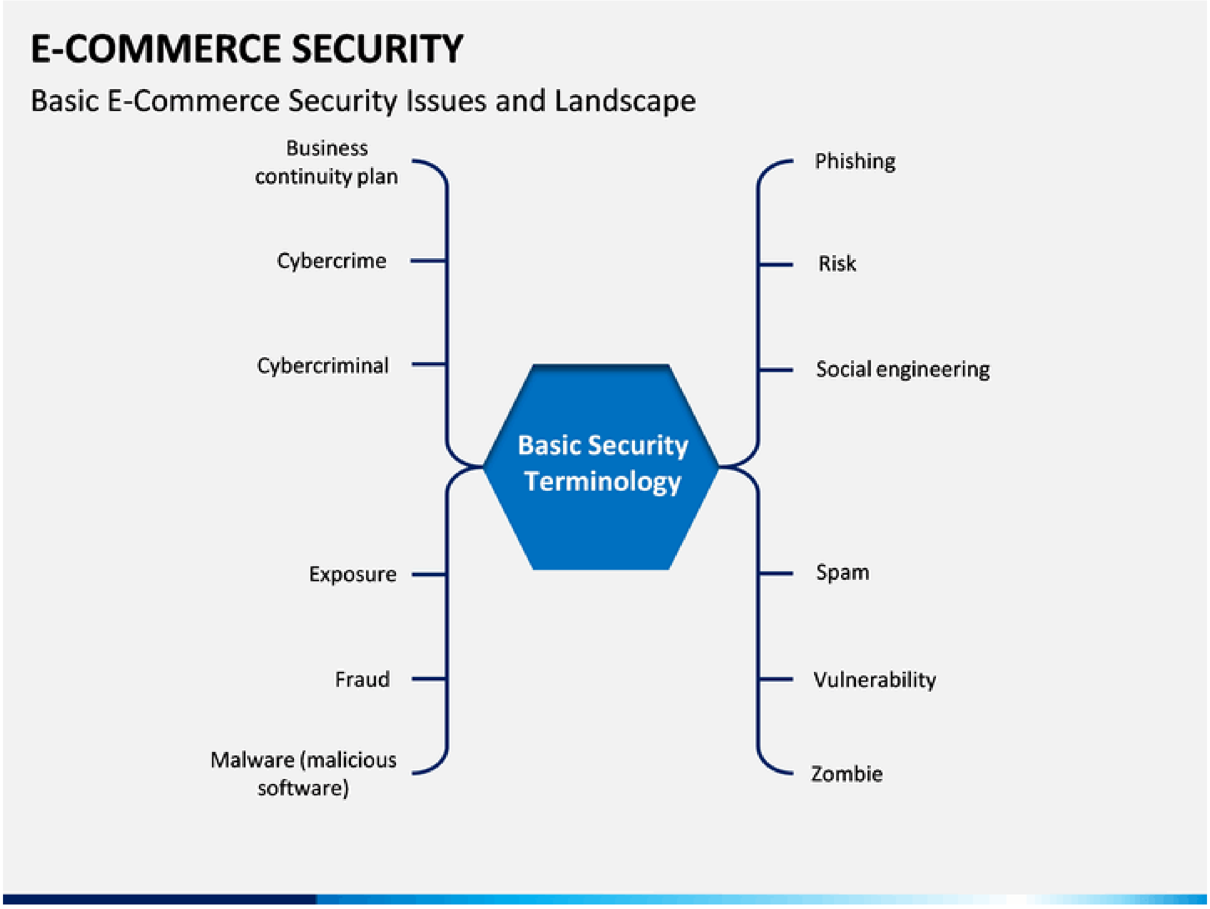
Therefore, a party in this particular transaction cannot decline a signature, email, or purchase.

Common Ecommerce Security Issues

1. Lack of trust in the privacy

2. Malware, viruses, and online frauds

3. Uncertainty and complexity in online transactions



E-COMMERCE SECURITY

Basic E-Commerce Security Issues and Landscape

Basic Security Terminology

Business continuity plan

Cybercrime

Cybercriminal

Exposure

Fraud

Malware (malicious software)

Phishing

Risk

Social engineering

Spam

Vulnerability

Zombie

What are the benefits and drawbacks of e-commerce?

The truth is that the appearance of e-commerce has been one of the greatest revolutions in recent years. And although there were already other forms of telematics sales (by catalog, by telephone, etc.).

Nothing is comparable to the turn of the screw that e-commerce has entailed for the purchase and sale of goods and services.

As we know through studies, only in the USA, 7 out of 10 Internet users already make online purchases, which represents a total of 20 million people. And the USA is not the country with the highest penetration of e-commerce. This gives us a clear answer to how prosperous e-commerce is today.

The security in e-commerce and specifically in commercial transactions is a very important aspect. For this, it is necessary to have a secure server through which all confidential information is encrypted and travels safely.

This provides confidence to both suppliers and buyers who make e-commerce their usual form of business.

Now, let's analyze what are all those advantages and disadvantages that this new way of doing business provides us:

Advantages of eCommerce

If we have to think of a top 10 benefits of e-commerce, we can think of many more advantages than 10, but the most relevant would be the following:

- **International sales**

In a traditional store, we can only make sales to those people who visit our store. Whereas in an online store, the possibilities are endless.

- **Show your products better**

Good photos, at a good angle and with the right camera, can turn a mediocre product into a quality product.

- **Custom user experience**

Thanks to big data we can know in advance a lot of data about our potential buyers, which will make the purchase totally personalized to their interests, with an impeccable digital experience.

- **Flexibility when making payments**

Currently, online stores offer various forms of payment to facilitate the purchase to the user: Paypal, bank transfer, credit card, installments…

- **Possibility of income for 24 hours 365 days**

Traditional commerce has a great disadvantage compared to online business since it is only open for certain hours a day and not every day. That in online stores is not a problem.

- **Remarketing to connect with customers**

Thanks to remarketing we can once again impact old clients or potential clients who have been interested in our products, to regain their attention and buy our products

- **Easier to obtain user data**

In most online stores, today, the buyer is asked to register and there we can get information from him that, in a transaction in a traditional store, would be impossible to collect.

- **Faster growth**

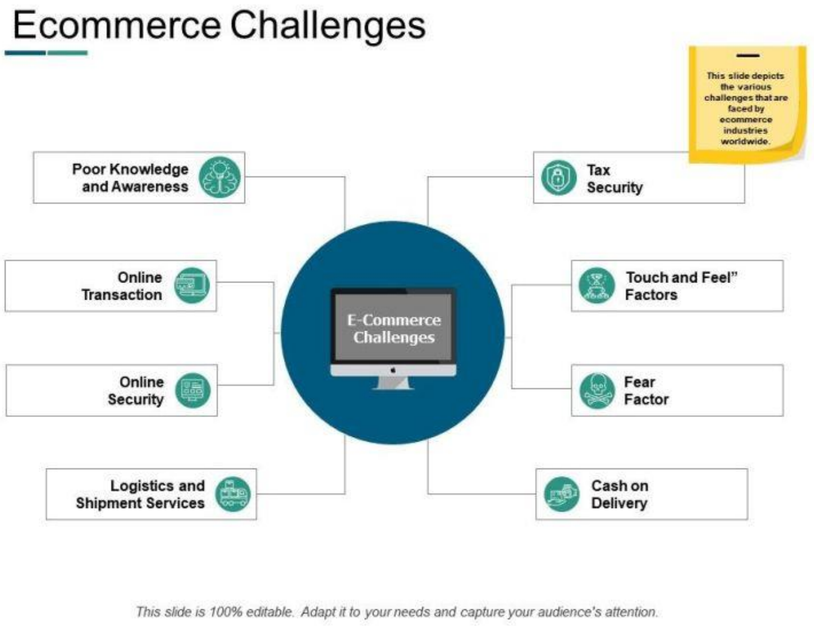
By having almost infinite possibilities in the online world, business growth can occur much faster than if we compare it with the growth options we have in the offline world.

- **Improvement of the brand image**

Having an online presence gives us a more innovative image than traditional commerce. In addition, we have complete control of what we want to show and say about ourselves, which will give us relative control of what they think of us. The e-commerce Headless also allows us to customize our online store to the maximum.

- **Reduction of expenses and intermediaries**

Not having the need to buy or lease premises will be a very high saving for any business, for example.



Ecommerce Challenges

This slide depicts the various challenges that are faced by ecommerce industries worldwide.

Poor Knowledge and Awareness

Online Transaction

Online Security

Logistics and Shipment Services

E-Commerce Challenges

Tax Security

Touch and Feel" Factors

Fear Factor

Cash on Delivery

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

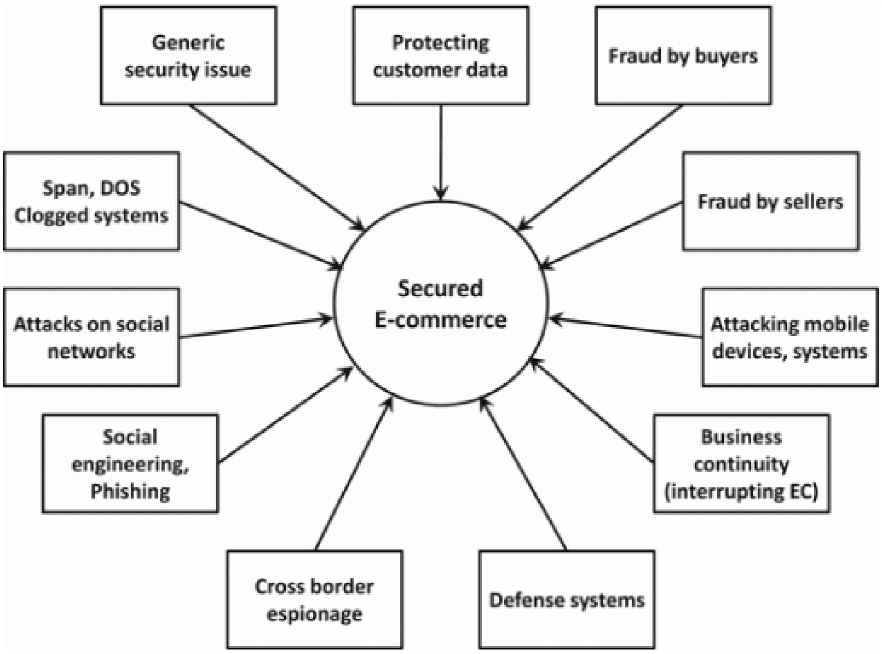
Disadvantages of eCommerce

As we mentioned previously, the advantages of e-commerce can be divided between benefits for companies and benefits for consumers. Based on the advantages for companies, we can list the following:

- **Cost reduction**: It is not the same to open an online store as a physical store, just as it is not the same to advertise on TV as on social networks. Having an online store is infinitely cheaper than a physical store.
- **Greater knowledge of your customer**: When a person goes to buy from a physical store, you do not know anything about that person. Nor where is he from, what interests does he have, etc. However, thanks to big data, you will be able to know a lot of details about the buyers (or potential buyers) of your store, to offer them the products or services that may interest them the most. So you can customize the sale to the maximum.
- **Organic growth**: If you do not have a large advertising budget, content marketing, social networks, positive product reviews by the client, etc. They will help you get new sales without “investing” money in advertising.
- **24/7 presence**: And as we mentioned at the beginning, you will be able to sell your products at any time and from anywhere, making the sales options grow exponentially.

In this sense, below we want to share some of the best security tips for Ecommerce websites.

Types of Ecommerce Security, Threats & Issues


Generic security issue
Protecting customer data
Fraud by buyers
Span, DOS Clogged systems
Fraud by sellers
Secured E-commerce
Attacks on social networks
Attacking mobile devices, systems
Social engineering, Phishing
Business continuity (interrupting EC)
Cross border espionage
Defense systems

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.

Hackers are creative and have a multitude of types of attacks that they can try to hack your site. The following tips are general and do not represent absolute solutions, but may still help prevent most potential problems.

It is also important to prioritize according to your type of website.

According to Google, the number of hacked websites increased by around 32 percent in 2016 compared to 2015.

Fortunately, the search engine was able to reduce webspam in 2017, as over 80 percent of the hacked websites were removed from search results.

While Google is making significant strides in combating website hacking, you shouldn't be complacent. Aggressive hackers track compromised websites. If you don't secure your outdated website now, you may be the next target of their attack.

Spam

Hacked spam is the most common type of website compromise. Spammers inject content into a legitimate website in order to direct traffic to a malicious or deceptive website.

Hackers may redirect content to pharmaceutical, gambling, or pornographic websites that can cause real harm to your actual website. They are trying to use your website's reputation to rank their bad content.

More and more threats revolve around e-commerce. From Vipnet360 we want to review some of the dangers that affect one of the most widespread commercial practices in our society.

The risks in e-commerce are especially directed towards the sensitive data of the user in order to compromise their security to economic, technical and personal level.

Next, we will list some of the main dangers to which you must be cautious now to make your purchases from the network.

Phishing

Phishing is a kind of fraud committed by electronic means by which the fraudster tries to achieve, legitimate user, confidential information fraudulently.
The scammer or phisher impersonates the identity of a trusted person or company so that the recipient of an apparently official electronic communication, via e-mail, fax, SMS or telephone, believes in its veracity and thus facilitates the resulting private data of interest to the scammer.

Pharming

Criminals redirect their victims to bogus web pages using various methods, such as emails with flashy subjects for victims to open and be attacked; endangering private information.

Pharming includes sending fake emails from legitimate companies or entities and directing the recipient to fake websites that replicate those of the legitimate company or entity.

Also Read – WordPress Pharma Hack

Malicious Codes / Malware

Today there is a new trend that reflects that fraud techniques through the Internet are moving from those based on social engineering, towards those based on the injection of malicious code or malware.

This change in trend is the result of increased public awareness about security, hence the increased caution of citizens when providing their personal data and other methods are used beyond deception to collect user information.

The malware present on computers intended, for example, to steal banking data of users using systems to intercept the keys and passwords or programs that corrupts navigation infrastructure and redirect users to fake websites. It can lead to many issues such you might start seeing a red screen with "Deceptive site ahead" written in it, its rendered by Google on sites identified as phishing or hacked to ensure the safety of the visitors.

Carding and skimming

These techniques consist of the fraudulent use of cards (carding) and the copying of magnetic stripes (skimming). This allows access to bank accounts, stolen card numbers, magnetic stripe overturns as well as personal profiles.

Crimeware
This technique includes password stealers and grabbers that record data from the keyboard, perform video capture or take screenshots and send the data collection sites. The crimeware is often associated with rootkits (malicious programs that hide the crimeware and make it invisible to many security tools).

This form of attack specializes in targeted attacks, penetrating computers that visit fraudulent websites and eluding detection by antivirus unless they are able to identify them generically or through behavioral analysis.

Clickjacking
This technique, also known as click hijacking, is a vulnerability that affects browsers and other web products.
Through this technique, an attacker can force the user's computer to click on any link or link on a website, being able to direct navigation to websites with viruses, Trojans or unwanted ads, without the user realizing what is happening.

DDoS Attacks
Distributed Denial of Service (DDoS) attacks and DOS (Denial of Service) attacks aim to disrupt your website and affect overall sales. A DOS exploit attack flood your servers with numerous requests until they succumb to them and your website crashes.
Further Study – The Impact of DDoS on E-commerce
Brute Force Attacks
These attacks target your online store's admin panel in an attempt to figure out your password by brute-force. It uses programs that establish a connection to your website and use every possible combination to crack your password. You can protect yourself against such attacks by using a strong, complex password. Do remember to change it regularly. **Read more** – WordPress Brute Force Attack – How To Protect Your Website?
SQL Injections
SQL injections are cyber-attacks intended to access your database by targeting your query submission forms. They inject malicious code in your database, collect the data and then delete it later on. Techniques like SQL injection, malware files can allow hackers to:

- Fake (spoof) their identity
- Take control of your computers and networksGain complete access to all the data on your system
- Tamper with your databases
- Send malicious emails on your behalf
- Malware hack that Redirect website to another spam website

Because malware strategies are constantly evolving, so too must your anti-virus protocols. To protect your site against security threats to your e-business, consider installing a firewall to

Price scraping
Price scraping bots can be sent by competitors to monitor your pricing, pricing strategy, inventory levels, marketing plans, and more, allowing them to undercut your prices or outrank you in search engine results.

Tips To Improve eCommerce Store Security & Best Practices
Several actions can be taken to **protect your e-commerce site from hackers.**
With the growing power and expertise of regulatory bodies, consumer associations, competition (which often uses the former to denigrate and annoy).

And the threats of cybercrime, an e-commerce site can no longer afford in 2021 to ignore the elementary precautions that guarantee its sustainability.

Here is now in detail the implementation of technical and legal security on your e-commerce site.

1) Change your passwords
It might sound like basic advice, but yet every year you see how lax people are at this level. Already, we often see how passwords that are too simple are still commonly used. The "1234" and "abcd" are to be avoided, especially when it comes to accessing the back-end of the site and entering the database.

The study found that an average of 19.1% of corporate users set poor passwords, whether those that have been used elsewhere, have been shared, or are particularly weak. This translates to 1 in 5 corporate users having a password that could easily be guessed by a malicious actor.
On the other hand, even if you use complicated passwords, it is still better to change them often. To help you stay on top of this, you can use a password manager.

For those lacking inspiration, using tools like KeePass or LastPass can give you passwords that are complex enough to fool hackers.
Also keep in mind that it is not recommended to use the same password for more than one service, because if you are the victim of a hack, you are particularly vulnerable.

2) Monitor activity on your database/site
Databases are particularly vulnerable to attacks, especially when users can submit attached files or fill out forms where they could write code.

It is, therefore, necessary to assess whether there is a potential for people who visit the site to be able to access the code and make modifications to it using this technique.

If you are able to do this, test yourself. Otherwise, do not hesitate to hire experts to accomplish this task.

In this regard, note that enabling Google Webmaster Tools (Google Search Console) is a great way to be made aware of abnormal activity happening on your site.

Indeed, as Google regularly updates its search index, it is able to quickly spot any activity deemed suspicious. Also Read – How to Track (Monitor) User Activity in WordPress?

3) Check that the software is updated
All software associated with your website should be updated regularly. You are probably using CMS or software associated with your server.

During each update, additional protections are integrated and Security Vulnerabilities are sealed.

Therefore, these "updates" are of vital importance. You can also use software that will alert you to the presence of vulnerabilities in the software.

When you receive a notification, be sure to respond as quickly as possible.

4) Make sure you share as little information as possible

For example, when your site issues error messages, you should make sure that these messages do not reveal too much information (including API keys).

In all situations, make sure that the information and messages you share with users contain as little specific data as possible.

5) Apply HTTPS everywhere on your website

Haven't applied HTTPS to your site yet? Don't delay doing it! Especially if your site does not adhere to this security protocol, some search engines like Google and Bing will penalize it by lowering it in the rankings.

In short, HTTPS is a communication protocol that guarantees among other things to the visitor that his information is sent to the site's server and that the data is encrypted, thus avoiding the possibility that third parties can access it.
It is all the more important to use it on pages where visitors must send sensitive information (passwords, personal data).

Also, note that the HTTP protocol should be activated with an SSL certificate. Indeed, the latter represents a form of additional protection as much for your visitors as for yourself.

6) Install security plug-ins

Some wordpress security plugins that you can install on your website will increase the security of your website, their main purpose being to block the path of would-be hackers.
You will find a lot of options, depending on your needs. For example, some plugins are specifically designed for WordPress while others work with CMS.

Do your research and watch the reviews to get a good idea of how reliable they are.

Use an Address Verification System (AVS)

One of the safest ways online retailers can facilitate credit card processing is by the use of an Address Verification System (AVS). This system is capable of comparing a customer's billing address against the information stored on file by a credit card issuer. It can block any suspicious transactions if the information provided doesn't match with the one stored on the credit card.

7) Make regular backups

Back-ups of your website should be done at regular intervals. How can backups help improve site security? In fact, if you have a problem, you can quickly restore the site and get it back up and running without much hassle.

Most hosting services will offer a backup option. You can also see if your CMS software contains the option or if you can install a plug-in that does the job automatically.

On this point, let us specify that we must compare the number of backups that must be made with the number of updates made on the site.

So, if you update every other day, you should have 15 backups done per month.

8) Use a tool to test the security of the website

There are tools that allow you to make a general diagnosis of the security level of your site and suggest you tips to improve website security.

These tools are very useful and can be activated on a regular basis, either weekly or monthly, as needed. Security scans should also be performed whenever a medium or large change is made to the site.

9) Consult cybersecurity specialists

Regarding the previous point, it should be noted that these tools are not infallible and that nothing replaces the expertise of cyber security specialists!

This is why you should use the services of a firm or a self-employed person who has a lot of experience in this field.

10) Fix loopholes quickly

Whatever your situation, one of the most important things to do is fix any flaws you find on your website as quickly as possible.

Do not wait for a problem to arise before reacting! Indeed, even if the flaw is minor, it could expose you to significant problems. You don't have the expertise to make the necessary changes? Call on specialists!

We have referred to it several times during the course of the article, but it is important to specify it again: security measures are all the more essential when it comes to an e-commerce site. Visitors to your site need to know they can trust you.

11) Install SSL Certificate

We are moving to the next level, because here the more technical part of your site comes into play.

The security "s" and the small padlock in front indicate that the connection is secure.

The http protocol (formerly used) does not encode the data exchanged during an online transaction, but sends it as plain text, thus risking leaving this information available.

In order for this "s" to appear in your online store address, you must install an SSL certificate that encrypts data sent between the user and the server (or in your case between the buyer and your store).
Most online shoppers know that a site without https is less secure, which can cause them to abandon their purchases.

In addition, the fact of not installing an SSL certificate on your site impacts your organic positioning, because Google penalizes sites without https.

This is why, for the sake of your organic positioning and your sales, be sure to update yourself!

12) Use a firewall

A firewall is a hardware or software system that serves as a communication between two or more networks, allowing access to authorized traffic and blocking any suspicious user.

There are a multitude of firewalls, but for your e-commerce we recommend proxies, which work as an intermediary between the buyer and your online store.

Define your payment methods

The payment options you offer your customers are critical to finalizing a sale. If you don’t offer any of the important options, some buyers might look elsewhere.

If a security breach occurs and their personal data is stolen, it will be very difficult for you to regain their trust.

Most of the advice presented above applies to e-commerce sites, but for an additional guarantee, you should seek the advice of an expert.

Such professional services can present you with actions precisely tailored to your needs and those of your users.

13) Deploy Multi Layer 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.You can go ahead and squeeze in an extra security layer, such as Multi-Factor Authentication. A two-factor authentication is a good example.

Introduction to 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 such as a mobile phone, POS (Point of Sales) or computer, a digital channel communications such as mobile wireless data or SWIFT (Society for the Worldwide Interbank Financial ...

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 three benefits of digital payments?

4 Benefits of Digital Payments

- The advantages of digital payments.
- Online retail provides an additional sales channel.
- Improved cash flow.

- Security at the forefront.
- Improved payment options for your customers.

- How many types of digital payments are there?
- Multiple payment options: Several types of payment modes including **credit cards, debit cards, net banking, EMIs, and UPI, along with Paytm Wallet and Paytm Postpaid**. Merchant discount rate: Zero MDR for payments done through UPI and RuPay cards.

Digital Payments in India: Definition, Methods, and Importance

What are Digital Payments?

Digital payments are transactions that take place via digital or online modes, with no physical exchange of money involved. This means that both parties, the payer and the payee, use electronic mediums to exchange money.
The Government of India has been undertaking several measures to promote and encourage digital payments in the country. As part of the '**Digital India**' campaign, the government has an aim to create a 'digitally empowered' economy that is '**Faceless, Paperless, Cashless**'. There are various types and methods of digital payments.

Please note that digital payments can take place on the internet as well as on physical premises. For example, if you buy something from Amazon and pay for it via UPI, it qualifies as a digital payment. Similarly, if you purchase something from your local Kirana store and choose to pay via UPI instead of handing over cash, that also is a digital payment.

What are the different methods of digital payments?

After the launch of Cashless India, we currently have ten methods of digital payment available in India. Some methods have been in use for more than a decade, some have become popular recently, and others are relatively new.

#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.
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.

What are the benefits of digital payments?

In a country like India, where disparities are sometimes poles apart, ensuring financial equality becomes an issue of prime importance. One of the reasons why our government started vocalizing Cashless Economy and Digital India was to improve access to financial resources. There are multiple benefits that digital payments bring to the table.

Ease and convenience

One of the most significant advantages of digital payment is the seamless experience they provide to customers. Reduced dependency on cash, fast transfer speed, and the ease of transacting make online payments a preferred option. Traditional payment methods like cash and cheques add to factors like risk, steps, and physical presence. With digital payment, you can send and receive funds from anywhere in the world at the click of a button.

Economic progress

Customers transact more online when they see the ease, convenience, and security of online payments. This means that more and more people feel comfortable buying online, investing digitally, and transferring funds via electronic mediums. The increase in money movement and online business contributes to the progress of the economy. This is why online ventures are being launched every day and even more are making profits daily.

Safety and efficient tracking

Handling and dealing in cash is a cumbersome and tedious task. Along with the risk of losing money, there is the hassle of carrying cash everywhere you go and keeping it safe. With digital payments, one can keep their funds secured in online format effortlessly. Nowadays, your mobile phone alone is enough to make and receive payments – thanks to UPI, netbanking, and mobile wallets. Additionally, most digital payment channels provide regular updates, notifications, and statements for a customer to track his funds.

Razorpay Payment Gateway: Your digital payment partner

Carrying forward the mission of Cashless and Digital India, Razorpay is India’s first full-stack financial solutions provider. We aim to enable all businesses, enterprises, entrepreneurs, and freelancers to adopt digital payment methods to grow their businesses. Razorpay Payment Gateway is our flagship product, providing holistic payment solutions to enterprises, big and small.

A payment gateway is like a portal connecting your bank account to the platform where your transactions occur. This third-party addition is the simplest way for a business to collect online payments via their website. If your venture has a website or an app, then Razorpay Payment Gateway should be your go-to option.

With Razorpay Payment Gateway, you can accept end-to-end payments easily and seamlessly. Some of the key features and benefits include:

- Accept all payment modes: A strong supporter of digital payments, we provide multiple options like Domestic and International Credit & Debit cards, EMIs, PayLater, Netbanking, UPI, and mobile wallets
- Flash Checkout: Thanks to the option of saving cards, your customer no longer needs to type in the card details every time – saving time and increasing sales
- Powerful Razorpay Dashboard: Dashboard provides efficient monitoring by way of reports, detailed statistics on refunds and settlements, and much more
- Protected and Secured: PCI DSS Level 1 compliant along with frequent third-party audits and a dedicated internal security team to make sure your data is always safe
- Run Offers Easily: Razorpay dashboard allows you to run any and every promotional offer at the click of a button

Razorpay Payment Links

Payment Links are one of the easiest ways to accept payments online. You can simply generate a link from the Razorpay Dashboard or ePOS app and share it with your clients. By clicking on the link, your customer can make the payment within minutes.
Razorpay Payment Links ensure safe money movement with our 100% secure ecosystem guarded with PCI DSS compliance. These are extremely simple to generate and require no prior coding or design knowledge. It offers more than 100 payment options to a customer, which ensures timely and accurate payment.

Razorpay Payment Button

We developed a product to integrate digital payments on an existing website since most businesses already have an online presence. Razorpay Payment Button allows you to accept payments on any website or webpage by simply adding a line of code. Within 5 minutes, you will have a customized code embedded on your website to start accepting payments.
Payment Buttons can help you:

- Add an integrated checkout on your website
- Start accepting fees without any integration or coding efforts
- Use one of our existing templates or create one of your own

Razorpay Payment Pages

For people who want to give information and receive payments simultaneously, Razorpay has a better alternative. With Razorpay Payment Pages, you can set up your venture's mini-website in less than 5 minutes. Payment Pages allow you to add your business information, showcase pictures, and accept payments – all in one. With our ready-to-use templates, you can accept payments for multiple payment modes.

Razorpay Subscriptions

Razorpay Subscriptions is a means to collect recurring payments without troubling the customer to intervene at each payment. This means that professionals can obtain a steady flow of fee payments without worrying about operational barriers. It ensures complete visibility and flexibility, and the customer has full control over his regular payments.
Nowadays, recurring payments via cards are becoming less popular with the rise of digital payments. Thus, Razorpay Subscriptions also brings with it the useful feature of UPI AutoPay. Under this feature, customers can set up recurring payments within minutes via their UPI app.

Modes of digital payments- Banking

What are the modes of digital payment?

Modes of Digital Payments

- Modes of Digital Payments.
- Unified Payments Interface (UPI):

- Bharat Interface for Money (BHIM):
- UPI 123PAY:
- UPI Lite:
- Cards (including RuPay Debit Cards)
- Immediate Payment Services (IMPS):
- Aadhaar Enabled Payment System (AePS):

Modes of Digital Payments

Modes of Digital Payments

Unified Payments Interface (UPI):

Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application, merging several banking features, seamless fund routing & merchant payments into one hood. It also caters to the "Peer to Peer" (P2P) collect request which can be scheduled and paid as per requirement and convenience.

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#.

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.

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.

Cards (including RuPay Debit Cards)

Debit Cards, one of the many payment modes, are issued by banks that allow individuals to purchase items at physical stores through Point of Sale (POS) devices or e-commerce marketplaces. RuPay Debit Cards, developed by National Payments Corporation of India (NPCI) was launched by the Government of India to allow individuals to make payments digitally. To get a RuPay debit card, you can reach out to your bank and ask them to issue you one.

Immediate Payment Services (IMPS):

Immediate Payment Services (IMPS) is a real-time interbank electronic fund transfer service capable of processing person to person (P2P), person to account (P2A) and person to merchant (P2M) transactions. Individuals can make payments 24x7 using their mobile number, Aadhaar number, bank account and IFSC code. Users can access IMPS through multiple channels such as mobile, internet, ATM and SMS.

Aadhaar Enabled Payment System (AePS):

Aadhaar Enabled Payment System (AePS) is a bank led model which allows online interoperable financial inclusion transaction at Point of sale (MicroATM) through the Business correspondent of any bank using the Aadhaar authentication. AePS allows you to do six types of transactions, the inputs required for a customer to do a transaction Bank Name, Aadhaar Number, Fingerprint captured during enrolment.

Banking Services Offered by AePS

- Cash Deposit
- Cash Withdrawal
- Balance Enquiry
- Mini Statement
- Aadhaar to Aadhaar Fund Transfer
- Authentication
- BHIM Aadhaar Pay

BHIM Aadhaar Pay enables Merchants to receive digital payments from customers over the counter through Aadhaar Authentication. It allows for any Merchant associated with any acquiring bank live on BHIM Aadhaar Pay, to accept payment from customer of any bank by authenticating customer's biometrics.

To be able to affect the same, merchant should have an Android mobile with BHIM Aadhaar app and certified biometric scanner attached with mobile phone/Kiosk/Tablet on USB Port or Micro-ATM/POS, mPOS. Both Customer and Merchant should have their Aadhaar linked to their Bank Account.

Bharat Bill Payment System (BBPS):

Bharat Bill Payment System (BBPS) is a one-stop platform that provides an interoperable and easily accessible recurring and bill payment service to consumers via multiple channels like Internet Banking, Mobile Banking, Mobile Apps, UPI, etc. Users are able to bill payments across various categories including electricity, gas, water bills, telecom, DTH, etc.

National Electronic Toll Collection (NETC) FASTag

NETC FASTag provides an easy and convenient digital payment mechanism for toll payments. 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.

e-RUPI

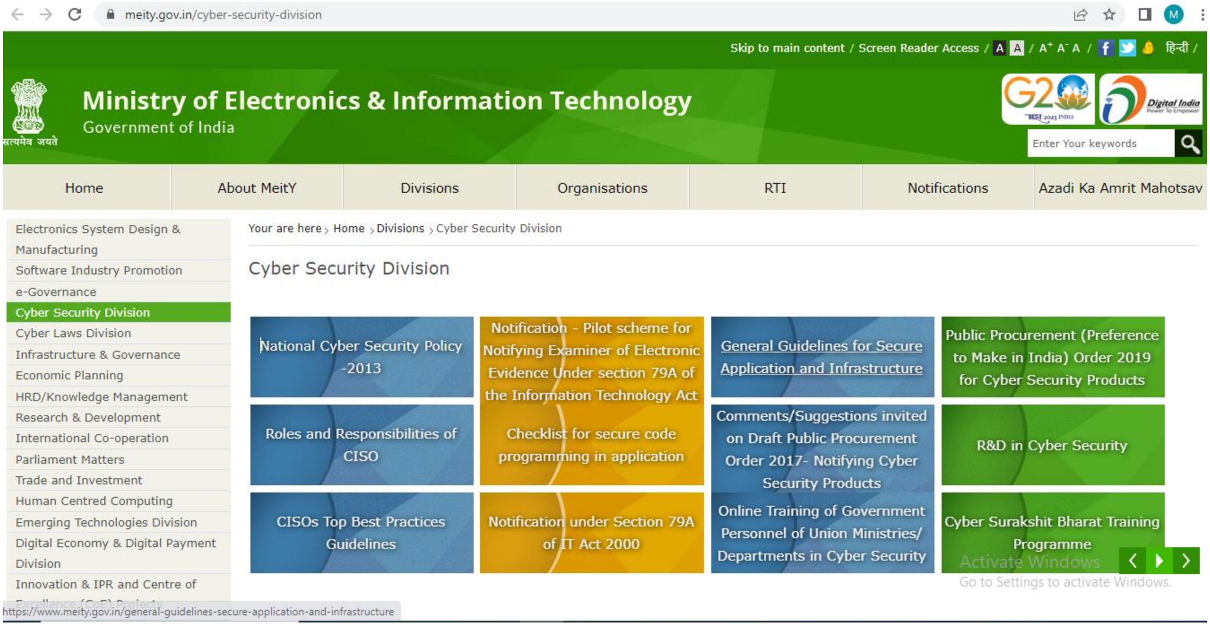
e-RUPI is a person and purpose specific, contactless and cashless digital payment solution. It can be issued as a prepaid QR code or SMS based electronic voucher which can be used by the Government/Private organizations for delivery of a specific subsidy or welfare benefit to the targeted citizens. The 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.

Unstructured Supplementary Service Data (USSD) / *99#:

*99# is a USSD based digital payment and banking service. Customers can avail this service by dialing *99#, a "Common number across all Telecom Service Providers (TSPs)" on their mobile phone and transact through an interactive menu displayed on the mobile screen. *99#

service is currently offered by almost all leading banks & all GSM service providers and can be accessed in 13 different languages including Hindi & English.
Key services offered under *99# service include:

- Interbank account to account fund transfer
- Balance enquiry
- Mini statement besides host of other services


meity.gov.in/cyber-security-division
Skip to main content / Screen Reader Access / A A / A+ A- A / हिन्दी /
सत्यमेव जयते
Ministry of Electronics & Information Technology
Government of India
Digital India
Enter Your keywords
Home
About MeitY
Divisions
Organisations
RTI
Notifications
Azadi Ka Amrit Mahotsav
Electronics System Design & Manufacturing
Software Industry Promotion
e-Governance
Cyber Security Division
Cyber Laws Division
Infrastructure & Governance
Economic Planning
HRD/Knowledge Management
Research & Development
International Co-operation
Parliament Matters
Trade and Investment
Human Centred Computing
Emerging Technologies Division
Digital Economy & Digital Payment Division
Innovation & IPR and Centre of Excellence (CoE) Projects
Your are here › Home › Divisions › Cyber Security Division
Cyber Security Division
National Cyber Security Policy -2013
Notification - Pilot scheme for Notifying Examiner of Electronic Evidence Under section 79A of the Information Technology Act
General Guidelines for Secure Application and Infrastructure
Public Procurement (Preference to Make in India) Order 2019 for Cyber Security Products
Roles and Responsibilities of CISO
Checklist for secure code programming in application
Comments/Suggestions invited on Draft Public Procurement Order 2017- Notifying Cyber Security Products
R&D in Cyber Security
CISOs Top Best Practices Guidelines
Notification under Section 79A of IT Act 2000
Online Training of Government Personnel of Union Ministries/ Departments in Cyber Security
Cyber Surakshit Bharat Training Programme
Activate Windows
Go to Settings to activate Windows.
https://www.meity.gov.in/general-guidelines-secure-application-and-infrastructure

Digital Payment Definition

Digital payment is referred to as those payments that take place using the various types of electronic medium. These methods do not require payment to be made in the form of cash or providing cheque.

There are different modes and types of digital payments that are prevalent in India, which are discussed in detail in the following lines.

1. Banking Cards
2. USSD (Unstructured Supplementary Service Data)
3. UPI (United Payment Interface)
4. AEPS (Aadhaar enabled Payment System)
5. Mobile wallets
6. Point of Sale Machines (PoS)
7. Mobile Banking
8. Internet Banking

1. Banking Cards: Banking cards are the most widely used digital payment system in India. It offers a great set of features that provides convenience as well as security to the users. Cards offer the flexibility of making other types of digital payments. Customers can store card information in the mobile application and pay for the services using the stored card information.

Banking cards (debit and credit cards) can be used for a variety of digital transactions like PoS terminals, online transactions, as a payment medium in mobile apps, which provide any kind of service like grocery, healthcare, rental cab booking, flight tickets, etc.

The most popular cards are issued by service providers like VISA, MASTERCARD, RuPay, AMEX etc.

2. USSD (Unstructured Supplementary Service Data): USSD is another popular digital payment method. It can be used for carrying out cashless transactions using mobile, without the need of installing any banking app.

The good thing about USSD is that it works without the requirement of mobile data. The main aim of this digital payment service is to include those sections of people of the society who are not included in the mainstream.

The striking feature of the USSD is that it can be availed in Hindi. The USSD can be used for the following types of activities:

a. Initiating fund transfers

b. Making balance enquiries

c. Getting the bank statements

3. AEPS (Aadhaar enabled payment system): AEPS can be used for all the following banking transactions such as balance enquiries, cash withdrawal, cash deposit, aadhaar to aadhaar fund transfers. All such transactions are carried out through a banking correspondent which is based on Aadhaar verification.

This service can be availed if the aadhaar is registered with the bank where an individual has a bank account.

4. UPI (Unified Payment Interface): UPI is the latest digital payment standard where the user having a bank account can transfer money to any other bank account using UPI based app. UPI enabled payments occur throughout the day and all 365 days in a year.

Payment can be done using a Virtual Payment Address (VPA). To use UPI services one must have a bank account and a mobile number registered with that bank account.

5. Mobile Wallets: Mobile wallets are another popular payment option. Here the users can add money to their virtual wallet using debit or credit cards and use the money added in the wallet to perform digital transactions.

Some of the most popular mobile wallets are PayTM, Mobikwik, PhonePe, etc.

6. Point of Sale Terminals: PoS terminals are installed in shops or stores where payments for purchases can be done through debit and credit cards. There are variations of PoS, one which can be Physical PoS and the other one is mobile PoS. The mobile PoS does away with the need of maintaining a physical device.

7. Mobile Banking: Mobile banking is a service provided by the banks through their mobile apps in a smartphone for performing transactions digitally. The scope of mobile banking has expanded extensively after the introduction of UPI and mobile wallets.

Mobile banking is a term used to describe a variety of services that are availed using mobile/smartphones.

8. Internet Banking: Internet banking is the process of performing banking transactions from the comfort of your home using a mobile phone/laptop/ desktop and an active internet connection. The major type of transactions can all be done using internet banking.

Internet banking services can be availed round the clock and all 365 days in a year, which makes it a popular choice for performing digital transactions.

Benefits of Digital Payments

Following are some of the most important benefits of using digital payments:

1. Transactions performed through digital payments systems are faster, easier and more convenient than traditional banking transactions performed physically by visiting the branch.
2. DIgital transactions are cheaper than the traditional payment system.
3. Digital payments are more rewarding as individuals can get access to a variety of coupons and freebies for performing digital transactions.
4. The digital transactions leave behind a definite track of the complete transaction which is helpful to trace payments.
5. Digital payment systems such as PayTM help in payment of electricity, broadband, gas and recharges for phone and DTH.

This concludes our article on the topic of Types of Digital Payments, which is an important topic in Business Studies for Class 11 Commerce students. For more such interesting articles, stay tuned to BYJU'S.

Unified Payment Interface (UPI),

Transferring money from one bank to another was a big deal before NPCI (National Payments Corporation of India) facilitated the option of inter-bank transactions using mobile applications. This RBI regulated interface, termed as UPI or as UPI full form stands for- Unified Payment Interface allows users to transfer funds instantly using a mobile device. Mobile payment applications such as Paytm have made it further easy to perform UPI transactions at the comfort of your home.

You would have clearly heard the term "UPI" multiple times before, but do you know exactly what is UPI?

Let's find out!

What is UPI?

Unified Payment Interface (UPI) is a popular mobile payment method that allows you to transfer funds from one bank account to the other, instantly and free of charge. Ever since its inception, UPI has made financial transactions much easier for account holders.

Transferring money through UPI requires each user to have an ID, termed as the UPI ID. The UPI ID is a unique identification for a bank account that is used to send and receive funds from one bank to another. In UPI payment applications such as Paytm, you don't need to enter the receiver's UPI ID. You can simply select the receiver's contact from your phone book or enter the receiver's contact number to send money via UPI. The UPI PIN, on the other hand, is a 4 or 6-digit personal identification number required to transfer money through UPI. Every account holder has the option to set his/her UPI PIN as per convenience.

Features of UPI

Nowadays, you would hear every bank account holder talk about transferring funds through UPI. If you haven't used UPI quite often, then here are the reasons behind the hype:

- UPI payments are very fast and typically, payment can be completed within seconds
- Almost every bank allows UPI transactions through mobile applications
- Payments are completely safe. To complete a payment, the user needs to have the SIM card of his mobile number present in his phone and also needs to enter the secret MPIN each time
- UPI Payment facility allows individuals to request money from some other individual, which is not an option with other payment methods like IMPS, NEFT
- These mobile payment applications also offer the facility of bill payments, meaning that you can set up timely reminders for all your bill payments and make the payments using the application at just one click
- In case of any trouble or suspicious activity on your account, you can easily file a complaint using the mobile payment application
- Payments can be made 24*7
- It's completely free!

Why Should You Use UPI?

Unified Payment Interface or UPI has more benefits than you can imagine. Here's a list of a few of them-

- Simplified, hassle-free online payments
- Safe and secure mode of money transfer
- Allows you to make payments towards your bills, shop on e-commerce websites, etc.
- Lets you make payments by scanning QR codes at your nearby departmental stores, chemist shops, etc.
- Regularly paying through UPI also helps you earn discount vouchers, cash back, and other rewards

Registration Process in UPI enabled application

UPI allows an individual to transfer money directly from his/her bank account to the recipient’s bank account in a few seconds. The facilitation of UPI has completely eliminated all this hassle. Once the sender has completed his/her UPI registration process, he/she can transfer the money with only a few clicks on a UPI payment application like Paytm.

Steps to Register in UPI

To complete your UPI registration process, follow these steps-

1. Download the Paytm UPI mobile payment application
2. Just enter your mobile number. If you have a dual SIM phone, you may be prompted to select the SIM slot in which your mobile number is present
3. An SMS will be sent from your number to verify your mobile number
4. Once this is done, you will have to select your bank name from the list that will be presented to you. Please make sure that the mobile number registered with your bank is the same as the one you entered earlier. Your bank account details will now be fetched from the bank using your mobile number
5. If you are linking your bank for the first time, you will be asked to set up a UPI PIN. You will need your debit card details for setting this up
6. Your bank account is now linked via UPI and you are ready to make your first payment

Generating UPI PIN

To generate your UPI PIN, you must first install a mobile payment application, such as Paytm on your mobile phone. After installing the application, you need to create your own UPI profile/account and follow the following steps to generate your UPI PIN-

1. Open a UPI payment application, such as Paytm, on your mobile phone
2. Tap on the ‘Profile‘ icon in the top left corner of the Paytm mobile application
3. In the left sidebar that opens, scroll down to the ‘Payment Settings’ option and click on it
4. Next, click on the ‘UPI & Linked Bank Accounts’ option and you will be able to see the list of your linked bank accounts
5. If UPI PIN is not set for a bank account, you will see a ‘Set PIN’ option under the bank account
6. Click on ‘Set PIN’
7. Now, enter the last 6 digits of your card number, along with its expiry date
8. After doing so, you will receive an OTP on your registered mobile number
9. Enter the OTP and the UPI PIN of your choice on the next screen that appears
10. Click on ‘Submit’ and your UPI PIN will be set!

How to Generate M-PIN?

Follow these steps to generate M-PIN:

1. Open the mobile payment application on your device and look for the "Create M-PIN" option
2. Enter your debit card details such as your card's expiry date, and the last 6 digits of your debit card
3. Enter the OTP sent to your registered mobile number
4. Now, enter the M-PIN of your choice and click on 'Submit'

What is Unified Payments Interface (UPI) Transaction?

A UPI transaction is basically a way to transfer money from one bank account to another. Paytm UPI mobile application allows you to transfer money in multiple ways. Whether it is a mobile number, QR code, UPI ID, or account number- each of these methods is equally easy to use.

Transferring money through UPI requires each user to have an ID, termed as the UPI ID. The UPI ID is a unique identification for a bank account that is used to send and receive funds from one bank to another. In UPI payment applications such as Paytm, you don't need to enter the receiver's UPI ID. You can simply select the receiver's contact from your phone book or enter the receiver's contact number to send money via UPI. The UPI PIN, on the other hand, is a 4 or 6-digit personal identification number required to transfer money through UPI. Every account holder has the option to set his/her UPI PIN as per convenience.

How to get started with using UPI using the Paytm App?

1. Download the Paytm, the best UPI app in India
2. Just enter your mobile number. If you have a dual SIM phone the app will prompt you to select the SIM slot in which your mobile number is present
3. Paytm will send an SMS on your number from the to verify the same
4. Once this is done, you will have to select your bank name from the list that is visible on the screen. Please make sure that the mobile number registered with your bank is the same as the one you entered earlier. Paytm app will now fetch your bank account details using your mobile number
5. If you are linking your bank for the first time, you will have to set up a UPI PIN by entering your debit card details for setting this up
6. You have now successfully linked your bank account via UPI and you are ready to make your first payment!

Check UPI Transaction Status on Paytm App

To check UPI transaction status on Paytm app, follow these steps-

1. Login to the Paytm application on your mobile device
2. On the home screen, under the section, ‘My Paytm’, click on ‘Balance & History’
3. The next screen that appears will show all the bank accounts linked with your Paytm app
4. Scroll down further on this screen to find your entire transaction history
5. You can click on any particular transaction to check its status and other details such as the transaction time, amount, transaction ID, etc.
6. If required, you can also share the details of any particular transaction by clicking on the ‘Share’ option on the top right corner of this screen
7. You can keep scrolling down on the screen to look at the previous transactions

Ways to Transfer Money Through UPI

You can transfer money using the mobile applications through the following ways-

1. **Mobile number –** This allows you to transfer money from your bank account mapped with your mobile number
2. **QR code –** Enables you to send money using the QR code enclosed with your VPA, Account number, IFSC, or mobile number
3. **VPA (Virtual Payment Address) –** Allows you to send or request money from a bank account using your UPI ID
4. **Account Number –** This lets you send money directly to the bank account

How to Make a UPI Transaction?

You can make a UPI transaction using either of the following methods-

1. **Selecting a Contact/Entering Mobile number –** Sending money is as simple as sending a message. Just select a phonebook contact or enter a mobile number, specify the amount to be transferred and enter your PIN. That’s it! Your payment will be completed in a few seconds.
2. **Scanning a UPI QR code –** You can also send money through UPI by scanning the receiver’s QR code. All you need to do is open the mobile payment application like Paytm on your phone, click on ‘Pay’, and select ‘QR code’. Scan the QR code of the receiver and enter the amount to be paid. Now enter your PIN and your payment will be completed in a few seconds.
3. **Entering UPI ID –** To send money through UPI ID, all you need to do so is open the mobile payment application, and enter the receiver’s UPI ID. After this, you need to enter the amount that needs to be transferred and verify the transaction by entering your MPIN. Your transaction will be completed in a few seconds.
4. **Entering Account Number & IFSC –** This the traditional way of payments and it is also supported on UPI. You may enter the account number & IFSC of the person you want to send money to, specify the amount and enter your PIN. Your payment will be completed in a few seconds.

Transfer money through UPI using Paytm today!

Is KYC Required For UPI Money Transfer?

The simple answer here is – NO. KYC is not required for making UPI money transfers on Paytm. Any user can make UPI-based transactions on the Paytm app without any concerns on the safety and security of user data. All the users registered on Paytm have to link a bank account with the Paytm app in order to perform UPI money transfers. Users become automatically verified when they link their bank account with the Paytm app since banks have already performed the KYC-check for all their users.

UPI Transaction Limit

To ensure the safety and security of transactions, all the UPI payment applications like Paytm are regulated by the guidelines of RBI. Owing to the current rules and regulations, the present UPI transaction limit per day on the Paytm app is Rs. 1 lakh per account, every 24 hours. However, it is important to note that the actual UPI transaction limit varies from bank to bank, which may also restrict the amount that can be sent at a lower amount too.

UPI Transactions Fees and Charges

Paytm mobile payments application that supports UPI services and it does not charge any charges for carrying out any UPI transaction. While there is a UPI transaction limit per day of Rs. 1 lakh on the Paytm application, there are no UPI transaction charges on the Paytm application.

How Does UPI Work?

To make a UPI transaction, you need a VPA (virtual payment address) just like you need a credit/debit card to make payment card payments. VPA stands for Virtual Payment Address which is basically the address to or through which you can make UPI money transfers.

A VPA is a unique financial address using which you can send and/or receive money in your bank account through UPI. As and when you create your UPI account on the Paytm app, your VPA gets created automatically. Now, to make a UPI transaction, you need to log in to your Paytm UPI payment application and click on the ‘UPI/Send Money To Anyone’ option. Select the receiver from your phone contact list, enter the mobile number of the receiver if it is not saved on your phone or scan the QR code of the receiver. Next, select the bank account from which you want to make the transfer and click on ‘Proceed’. Enter UPI PIN associated with the selected bank account and the amount will be immediately transferred from your bank account to the receiver’s bank account!

Participants in UPI

The following parties are involved in making a UPI transaction-

1. Remitter bank
2. Beneficiary bank
3. NPCI
4. Merchants
5. Bank account holder
6. Payer PSP
7. Payee PSP

What is UPI 2.0?

UPI 2.0 is basically and newer version of UPI which has improved features and added benefits. The upcoming UPI 2.0 is said to be a more secure and comprehensive payment method with easier and simpler authentication process.

Features of Upcoming UPI 2.0

Following are the salient features of upcoming UPI 2.0-

1. The UPI 2.0 facility allows the payment of utility bills such as rent, electricity, etc. using the UPI system
2. UPI 2.0 comes with a pre-authorized transaction feature, using which users will be able to authorize their regular transactions such as payment of mobile bills before their due date
3. The UPI 2.0 system will have the biometric authentication feature which has the fingerprint mapping technology and iris scanner. This will ensure increased security of UPI transactions
4. UPI 2.0 will keep a check on the speed of transactions to make sure that fraudulent transactions are detected and prevented from being successful
5. UPI 2.0 will allow transactions even if your mobile number is linked to other bank account, which the current UPI system does not allow
6. The UPI 2.0 payment system will also enable payments using the Aadhaar number to facilitate transactions directly from the bank accounts of individuals

e-Wallets

Digital Wallet Explained: Types With Examples and How It Works

What Is a Digital Wallet?

A digital wallet (or electronic wallet) is a financial transaction application that runs on mobile devices. It securely stores your payment information and passwords. These applications allow you to pay when you're shopping using your device so that you don't need to carry your cards around. You enter and store your credit card, debit card, or bank account information and can then use your device to pay for purchases.

Digital wallets can also store:1

- Gift cards
- Membership cards
- Loyalty cards
- Coupons
- Event Tickets
- Plane and transit tickets
- Hotel reservations
- Driver's license
- Identification cards
- Car keys

Learn more about digital wallets, how they work, and how you can use them.

KEY TAKEAWAYS

- Digital wallets are financial applications that allow you to store funds, make transactions, and track payment histories on devices like phones and tablets.
- You can store all of your financial information in a digital wallet; some even let you store identification cards and driver's licenses.
- Digital wallets may be included in a bank's mobile app or payment apps like PayPal or Alipay.
- Digital wallets allow people in financially underserved parts of the world to access financial services they may not have been able to before.

How a Digital Wallet Works

Digital wallets are applications designed to take advantage of the abilities of mobile devices to improve access to financial products and services. Digital wallets essentially eliminate the need to carry a physical wallet by storing all of a consumer's payment information securely and compactly.

Digital wallets use a mobile device's wireless capabilities like Bluetooth, wifi, and magnetic signals to transmit payment data securely from your device to a point of sale designed to read the data and connect via these signals.

Currently, the technologies used by mobile devices and digital wallets are:

- **QR codes**: Quick response codes are matrix bar codes that store information. You use your device's camera and the wallet's scanning system to initiate payment.
- **Near field communication (NFC)**: NFC is a technology that allows two smart devices to connect and transfer information using electromagnetic signals. It requires two devices to be within about an inch and a half (4 centimeters) from each other to connect.
- **Magnetic secure transmission (MST)**: The same technology used by magnetic card readers that read your card when you swipe it through a slot on a point of sale. Your phone generates this encrypted field that the point of sale can read.

The card information you've stored in your wallet and choose to use for a transaction is transmitted from your device to the point of sale terminal, which is connected to payment processors. Then, through the processors, gateways, acquirers, or any other third parties involved in credit and debit card transactions, the payment is routed through the credit card networks and banks to make a payment.

Because cryptocurrency has made its way into the financial system, companies like Bitpay invented cards that let you pay with cryptocurrency. Digital wallets like Apple Pay and Google Pay allow you to add a Bitpay debit card. The Bitpay card converts cryptocurrency to dollars at the current market value, which your wallet then uses to pay for your purchase.2

Types of Digital Wallets

There are several digital wallets available. Here are some of the most well-known:

- Cash App
- ApplePay
- Google Wallet
- Samsung Pay
- PayPal
- Venmo
- AliPay
- Walmart Pay
- Dwolla
- Vodafone-M-Pesa

Most wallets attempt to distinguish themselves from their competitors using different methods. For example, Google's digital wallet service allows you to add funds to the wallet on your phone or device. Then, you can spend this cash in-store and online at businesses that accept Google payments.3

Apple, on the other hand, entered into a strategic partnership with Goldman Sachs to issue Apple credit cards and expand its ApplePay services.4

Advantages and Disadvantages of Digital Wallets

One of the most significant advantages of digital wallets is that using one limits the amount of financial and personal information you need to carry as you go about your day. If you place everything in your digital wallet, you no longer need to carry physical cards or a physical wallet—there is no chance of a card falling out of your wallet or of leaving your card in the ATM slot. Additionally, you can't lose your entire wallet.

Digital wallets allow businesses and consumers worldwide to accept payments, receive funds, or send and receive remittances from friends and family in other nations.
Digital wallets do not require a bank account at a bank with a physical branch. Instead, you can place your funds in an online-only bank—which
gives unbanked and underbanked communities access to financial services, therefore enabling broader financial inclusion.5

Security might become an issue if you use a digital wallet from a provider that hasn't been vetted or doesn't have an established reputation. If your phone isn't password-protected, you risk giving someone else access to your finances if you lose your phone. Additionally, there might be local businesses you prefer to shop at that don't yet have a point of sale that accepts this technology.

What Is a Digital Wallet Example?

Google Pay and Apple Pay are some examples of more well-known digital wallets. Both services allow you to access your financial products through your devices and make purchases.

Is PayPal a Digital Wallet?

PayPal is a peer-to-peer payment and money exchange platform, but it has a digital wallet included in its app.6

Do I Need a Digital Wallet?

You don't necessarily need a digital wallet. However, they offer a convenient way to pay for your purchases because you don't have to carry credit and debit cards around. This also increases card security—you can't lose your cards if you don't carry them.

10 Top Digital Wallets In 2023

What Is A Digital Wallet?

An electronic wallet (EC), or, in other words, an electronic means of payment - that is how it is called in the law - is a payment instrument for storing money, mobile payments, transfers, and paying on the Internet. You sure have heard other names as mobile wallet or digital wallets.

In fact, these digital wallets are an analogue of a bank account, only money is stored not in a bank, but in a special computer program.

It is convenient for online shopping enthusiasts and freelancers: programmers, designers, copywriters, tutors. And also for those who are worried about the safety of funds in a bank account - if you transfer the required amount to an e-wallet and make a payment or transfer through it, scammers will not get to the bank account, as it's a key point during eWallet app development.

It is also convenient to use an e-wallet for international transfers. In addition, the e-wallet commission can be less, and transfers are instantaneous.

Differences Between Electronic Wallets And Bank Accounts

There is no cardinal difference between these payment methods (bank accounts and digital wallets) except for some points.

- When we make a payment on the Internet, for example, when we buy something in an online store, we enter our card details. It is not safe. The site may turn out to be fake, and then scammers can easily steal all the money from a bank account or even from deposits and piggy banks. It is much safer to keep a small amount in an electronic wallet to make mobile payments. In this case, even if the scammers steal money from it, they will not be able to get the rest of your funds.
- Easier to open. To do this, you do not need to interact with the bank and pay money. Get an e-wallet for free on the Internet and start using it right away.
- The e-wallet is convenient to use. Card data is not only dangerous to enter, but also long enough. And to take off some money from an electronic wallet, you only need a password and a mobile phone.
- Transactions through the e-wallet are instantaneous, regardless of the time of day, working days or holidays.

- Mobile wallets are not tied to a specific country and allow you to make payments and transfers regardless of location. For example, if you and the recipient are in different countries.
- An electronic wallet does not always mean an exclusively virtual look. Some operators issue cards for offline payment. In an ordinary store, in a market or in a cafe, you can pay with money from an electronic wallet and not endanger the funds in your bank account.

What Is A Digital Wallet?

An electronic wallet (EC), or, in other words, an electronic means of payment - that is how it is called in the law - is a payment instrument for storing money, mobile payments, transfers, and paying on the Internet. You sure have heard other names as mobile wallet or digital wallets.

In fact, these digital wallets are an analogue of a bank account, only money is stored not in a bank, but in a special computer program.

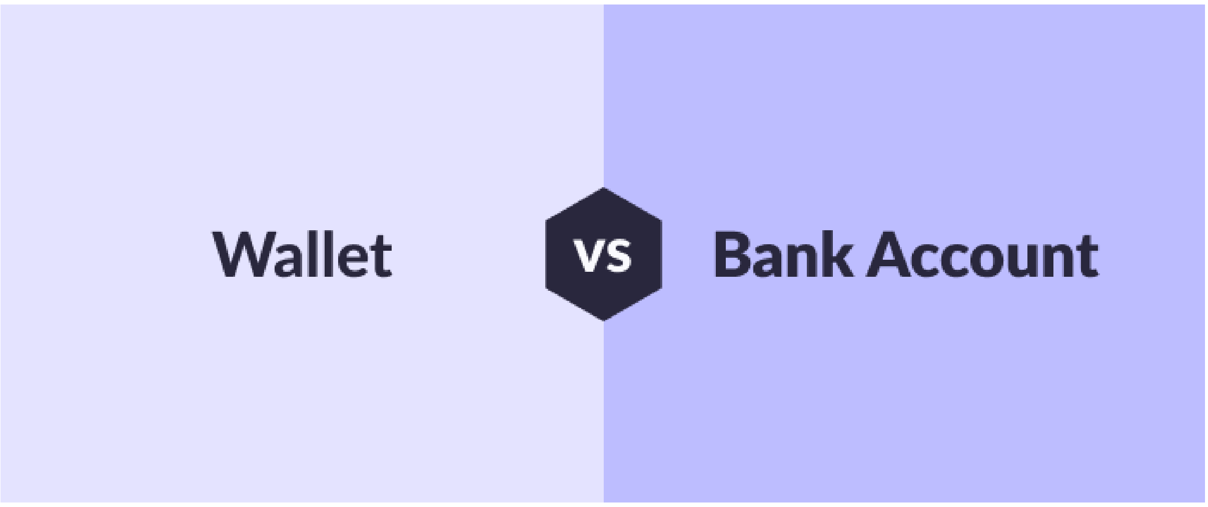
It is convenient for online shopping enthusiasts and freelancers: programmers, designers, copywriters, tutors. And also for those who are worried about the safety of funds in a bank account - if you transfer the required amount to an e-wallet and make a payment or transfer through it, scammers will not get to the bank account, as it's a key point during eWallet app development.

It is also convenient to use an e-wallet for international transfers. In addition, the e-wallet commission can be less, and transfers are instantaneous.

Differences Between Electronic Wallets And Bank Accounts

There is no cardinal difference between these payment methods (bank accounts and digital wallets) except for some points.

- When we make a payment on the Internet, for example, when we buy something in an online store, we enter our card details. It is not safe. The site may turn out to be fake, and then scammers can easily steal all the money from a bank account or even from deposits and piggy banks. It is much safer to keep a small amount in an electronic wallet to make mobile payments. In this case, even if the scammers steal money from it, they will not be able to get the rest of your funds.
- Easier to open. To do this, you do not need to interact with the bank and pay money. Get an e-wallet for free on the Internet and start using it right away.
- The e-wallet is convenient to use. Card data is not only dangerous to enter, but also long enough. And to take off some money from an electronic wallet, you only need a password and a mobile phone.
- Transactions through the e-wallet are instantaneous, regardless of the time of day, working days or holidays.
- Mobile wallets are not tied to a specific country and allow you to make payments and transfers regardless of location. For example, if you and the recipient are in different countries.
- An electronic wallet does not always mean an exclusively virtual look. Some operators issue cards for offline payment. In an ordinary store, in a market or in a cafe, you can pay with money from an electronic wallet and not endanger the funds in your bank account.



How Does It Work?

The basic functionality of an electronic wallet usually includes:

- non-cash payment for goods, services, fines, other payments;
- transfers to other digital wallets, bank cards, accounts, money transfer systems;
- replenishment through cards, terminals, as well as in other ways;
- receiving funds from external sources;
- linking a bank card.

You can link a bank card to an electronic wallet in the payment service and / or online bank.

As for withdrawing cash from electronic wallets, only holders of plastic cards issued by the corresponding services will be able to do this without intermediate operations. If the card is virtual, then it can be “populated” in a smartphone and withdraw cash from contactless ATMs. In other cases, to withdraw cash, you will need to first transfer money from an electronic wallet:

- to a bank card;
- to a bank account;
- through the money transfer system.

And only after that the money can be withdrawn / received on / from a mobile wallet.

10 Best Digital Wallets

Let's discover the most popular digital wallets.

1. Apple Pay

Apple Pay is a digital payment solution for contactless payments, created and operated only on Apple devices. Apple Pay accounts can be used to pay for a variety of goods and services through bank terminals equipped with NFC technology, as well as online stores or within applications.

In the first case, a mobile device (smartphone or smart watch) is used as a regular bank card with an NFC tag, and in the second case (applications and websites), the Wallet application is accessed through a special API.

The mechanism of the system is based on the technology of close data transmission NFC (at a distance of up to 20 cm) in conjunction with the Secure Element chip, which stores the bank card data in encrypted form. Secure Element represents the industry standard in financial transactions. This chip runs a special Java application.

Pros:

- all operations are performed using the gadget
- the ability to track all costs in order to optimize them
- the security of the service is at a high level, unauthorized intervention in the work is practically excluded
- if the phone is lost, the service data will be inaccessible to intruders

Cons:

- works only on Apple devices
- devices are often discharged

- system performance issues on outdated or refurbished models
- not all terminals are equipped with a contactless payment function

2. Cash App

Cash App is a peer-to-peer money transfer service developed by Square Inc. that allows users to send and receive money. This mobile wallet can help you pay bills, pay for purchases, share travel costs, or do any other money sending tasks you want to do with other Cash App users. This digital wallet app also functions similarly to a bank account, providing users with a debit card called a "Cash Card" that allows them to make purchases using the funds in their Cash App account. The app also allows users to invest their money in stocks and buy and sell bitcoins.

Mobile payment service Cash App has reached a key milestone in the development of Bitcoin payments and has become the most popular app in the finance category on the Google Play Store in the US, surpassing PayPal in terms of downloads. Initially introduced in 2013 as Square Cash, the service has changed little since its inception.

Pros:

- customers can buy and sell bitcoins directly from your Cash App balance
- high level of data protection
- encryption and offline storage of bitcoins

Cons:

- limited transparency when it comes to other transactions using the app
- you have to pay 1.5% commission to get money instantly
- you cannot make international digital payments

Your way through FinTech

Everything you need to know about FinTech collected in one guide presented by top Geniusee experts

3. Dwolla

Dwolla attracts users due to low transaction fees, simple automation and a high level of security. At its core, the system is an agent for both banks and individuals or entrepreneurs. Ideal for integrating bank transfers. To start using the service, you will need to create a personal account and then link a bank account to it. In total, this procedure will take no more than 10 minutes. Money is credited to the account within one day.

Dwolla actively cooperates with many major US banks, including Bank of America and Silicon Valley Bank, which is an indicator of reliability. The service offers three tariffs to choose from: free or trial, standard and corporate.

Using the service will be most beneficial for residents of the United States, in other countries it may be difficult to withdraw funds. The transaction limit is $5,000 for the standard plan and $10,000 for the corporate plan. The system only supports ACH payments, so it is not possible to make SEPA and SWIFT transfers. Dwolla does not plan to issue corporate or individual bank cards.

Pros:

- advanced features for developers
- first-class technical support
- fast payment processing
- "virtual wallet" for sending, storing and receiving funds

Cons:

- high price for the tariff plan
- no credit card transactions
- limited features for ordinary users

4. Google Pay

Google Pay / Android Pay is basically a mobile application for the Android operating system. The digital wallet stores credit and debit cards in one place. All user data is safe in these digital wallets. Adding a card to the system takes only a few minutes: it will be enough to download the application to the device and select the desired card in the "Cards" tab.

Google Pay account works in any place where it is possible to pay using a contactless payment terminal. Thus, residents of almost all countries can easily use the system. For each payment, Google Pay receives a small fee, but it is always paid by the merchant.

The company issues its own Google Wallet Card debit cards. Their owners have the opportunity to withdraw cash from ATMs and pay for purchases in stores. A plastic card is linked to the Google Pay system, and no commission is charged for its maintenance and issue. The card cannot be used outside the US. The service supports all possible currencies. Google Pay is not suitable for international SWIFT payments or SEPA transfers.

Pros:

- security and protection of personal data
- the ability to add several cards at the same time
- support for any gadget with the Android system
- fast transactions

Cons:

- only supports Android devices
- not everywhere there are contactless payment terminals
- ATMs do not support the system
- completely addicted to the phone

5. PayPal

If you often make purchases in foreign online stores, we recommend getting a PayPal wallet as one of the most popular digital wallets. It is recognized by almost all countries, so you can use the funds stored on your account anywhere in the world. PayPal is an electronic wallet that allows you to make online payments. PayPal started in 1998. Until

2015, it was part of eBay, an American auction, and only from July 18, 2015, PayPal became a separate independent company.

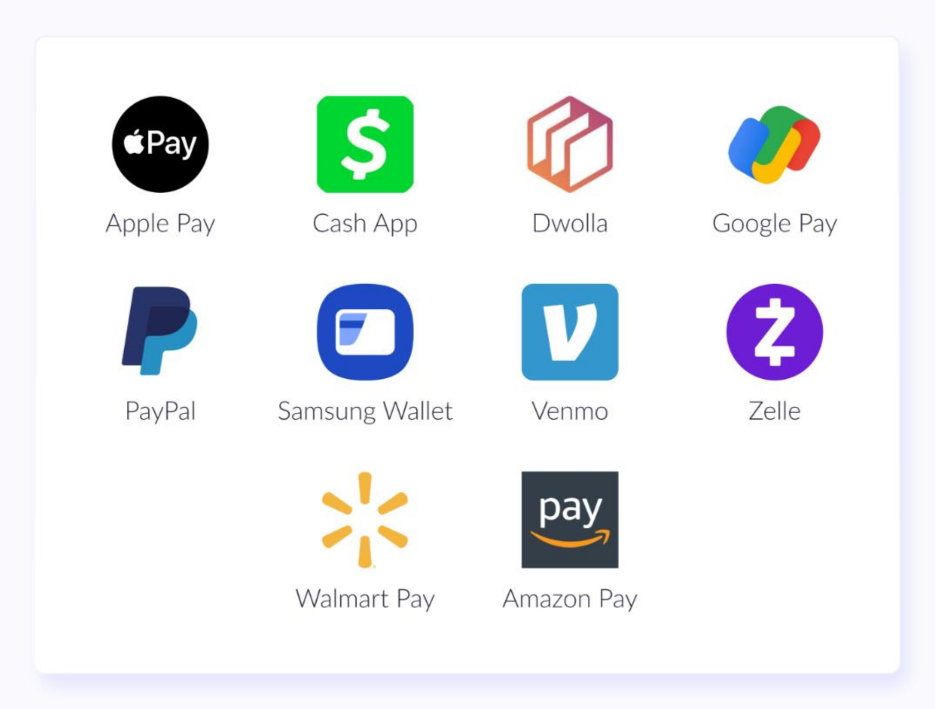
You can use PayPal by adding your payment cards, but not only - you also have the ability to link a bank account to it and fund your PayPal account with funds directly from this account. The service also provides the ability to send money to friends. Another advantage of PayPal is the ease of registration, which does not even require a bank account. Also, users note the work with 25 currencies of the world and a high degree of protection of financial transactions.

Pros:

- quick registration
- cooperation with well-known trading platforms
- high degree of protection

Cons:

- relatively low transaction speed



6. Samsung Wallet

Samsung is merging its two software services, Samsung Pay and Samsung Pass, into a single digital platform called Samsung Wallet. This will allow Galaxy device owners to securely and easily manage their digital keys, boarding passes, ID cards, loyalty cards and more in one mobile app. The idea is that it "keeps everything your digital life needs" in a convenient location without sacrificing security.

This last point is obviously the key issue when you throw all your digital eggs in one basket. However, Samsung promises "defense-grade security" through Samsung Knox, which is the company's own security and management system preinstalled on most Galaxy devices.

Pros:

- immediate activation
- fast and secure online payment
- rewarding application

Cons:

- works only on Samsung devices
- cannot be charged via ATMs, with paychecks, or at certain retail locations

7. Venmo

Venmo is part of the larger PayPal family of brands and is owned by PayPal. You can send and receive money instantly with this mobile payment app. The company advertises its service as "safe, easy and communicative" when it comes to sending money. Venmo can also be used to make purchases in person, online, or through the Venmo mobile app. It currently has a user base of 65 million people.

Venmo is a consumer-friendly digital wallet app with a social focus. It is intended to be a fast and free method for completing these transactions; it's whether you need to pay a friend's restaurant bill or split the rent with your roommate. Venmo is also used by some small businesses to accept payments.

Pros:

- it is easy to transfer and receive money, as well as shop online
- commissions are rarely charged
- has interactive social features
- debit and credit cards available

Cons:

- available only in the USA
- charges a 1.5% fee for instant transfers
- transactions may be public to app users, making it difficult to navigate through privacy settings

8. Zelle

Zelle is an online platform for quickly sending and receiving money between US bank accounts.

Zelle was designed by banks and made to be secure. Zelle is a secure payment method because it uses encryption to protect your payment information. Zelle also has a policy that you can get your money back "if a scammer or hacker gains unauthorized access to a bank account" and that "victims can work directly with their bank for a refund."

Pros:

- free application
- easy and fast to use
- funds you send or receive are protected up to $250,000 per account

Cons:

- does not protect approved payments from fraud
- if you send money to the wrong person, you have no choice but to wait for that person to return it

9. Walmart Pay

Walmart Pay uses QR codes generated by its app so that any smartphone user can pay without using a new generation mobile phone with an NFC chip or their regular credit or debit card.

Walmart's new payment system, in addition to being compatible with all smartphones on the market, allows us to use any type of credit or debit card, as well as the company's prepaid and gift cards. The user just needs to install the application on their device and it is convenient to buy. When a user is about to make a payment, they just need to open the app on their mobile phone, select Walmart Pay, and scan the QR code shown by the establishment's checkout. All you need is a simple mobile phone with a camera, no NFC chips or anything more technologically advanced.

Pros:

- works both for IOS and Android devices
- stores your receipts, which saves on paper
- several layers of security
- stores your credit, debit and even walmart gift cards information

Cons:

- works only in USA
- works only in Walmart sto

10. Amazon Pay

Amazon Pay makes it possible for partner companies to embed a button on their websites through which customers can pay for purchases and services. For stores, this service will be paid: 2.9% of the transaction amount + $0.3. For international transactions, the commission will be 3.9% + $0.3. To pay for the order, it will be enough to use the profile on amazon.com. The service guarantees complete data security.

Users of European countries can make SEPA payments - the service supports such a payment system. The same applies to SWIFT payments, which are available worldwide. Amazon issues credit cards for regular customers. The user does not need to pay a monthly commission for the use. You can get a card within a week after applying. The system allows you to make payments in the national currency with further conversion into US dollars at the average rate.

Pros:

- low transaction fees
- high level of security
- a simple registration procedure that takes only a few minutes
- no monthly service fee

Cons:

- integration of the service with the store may take time
- no free trial
- customer support team takes a long time to process user requests

USSD (Unstructured Supplementary Service Data)

USSD (Unstructured Supplementary Service Data) is a Global System for Mobile Communications (GSM) protocol that is used to send text messages. USSD is similar to Short Message Service (SMS).

USSD uses codes made up of the characters that are available on a mobile phone. A USSD message, which can be up to 182 characters long, establishes a real-time communication session between the phone and another device -- typically, a network or server.

USSD can be used for Wireless Application Protocol (WAP) browsing, mobile money services, prepaid callback service, menu-based information services and location-based content services.

With USSD, users interact directly from their mobile phones by making selections from various menus. Unlike an SMS message, during a USSD session, a USSD message creates a real-time connection. This means USSD enables two-way communication of information, as long as the communication line stays open. As such, queries and answers are nearly instantaneous.

How USSD works

Typically, USSD involves a query from a mobile phone user, such as a request for a bank account balance. Once the user sends the request, the USSD gateway forwards it to the user's USSD application, which responds to the request.

The process is then repeated in reverse, i.e., the response goes back to the USSD gateway, which displays the content of that response on the screen of the user's mobile phone. Generally, the responses, which contain a maximum of 182 alphanumeric characters, are sent in a format that's easy to display. The user sends and receives data by dialing a specific short code -- usually, five numbers.

USSD applications run on the network, not on a user's device. As such, they don't have to be installed on the user's phone, which is an advantage for users with feature phones that have limited storage space. USSD apps are instantly available to every subscriber the moment they're deployed to a network.

How USSD is used

USSD is used for several purposes, including the following:

- **Mobile banking.** Unlike banking apps that need internet access and smartphone functionality, USSD banking can work on any mobile device, including feature phones.
- **Network configuration and requests.** USSD is used to configure a user's mobile device on the network. It also provides a menu of service options a user can choose from for such things as buying airtime or requesting account balances.

- **Customer update requests.** USSD can integrate with enterprise resource planning (ERP) and customer relationship management (CRM) systems to request updated customer information. This enables better customer service and data accuracy.
- **Marketing surveys.** USSD can be used for mobile marketing. For example, organizations can send basic marketing surveys that users can respond to immediately, enabling companies to get customer feedback in real time.
- **Callback services.** Service organizations, such as insurance providers and financial services companies, can use USSD to determine customers' interests by enabling them to request callbacks after they present their offers.
- **Order confirmations.** Food delivery providers can use USSD to enable two-way communication between customers placing orders and the vendors to alert customers when their orders are on the way.
- **Coupons and vouchers.** Retailers can use USSD to communicate special offers to customers, as well as send coupons and vouchers.

USSD payments

USSD payment processing is performed by sending a text message to a service provider. When the service provider receives the text message, it either charges the amount of the purchase to an online payment system or adds the amount to the user's phone bill.

The merchant then releases the goods or services, and the money is transferred to the company's account. The delivery of digital goods is often conducted by Multimedia Messaging Service (MMS) that enables files to be sent to users with SMS. If the user bought a physical item, the receipt can be sent via SMS or MMS. Most purchases made using USSD or SMS occur in Europe and Asia.

Technical details

Most GSM phones have USSD capability. USSD is usually associated with real-time or instant messaging (IM) services. USSD does not offer a store-and-forward capability, as is typical of other short message protocols, such as SMS.

USSD services use the existing architecture of GSM networks. A user dialing a USSD service code begins a dialogue with a USSD app on a mobile network. The network node can be a mobile switching center, visitor location register, home locator register or other network entity, such as an application platform, which has access to the specific USSD service.

Technically, USSD enables the mobile station user and a public land mobile network operator-defined application to communicate in a way that's transparent to the mobile station user and to intermediate network entities.

A typical USSD message begins with an asterisk (*) followed by digits that comprise commands or data. Groups of digits can be separated by additional asterisks. The message is ended with a hashtag (#).

AADHAAR ENABLED PAYMENT SYSTEM (AEPS)

AEPS is a bank led model which allows online interoperable financial transaction at PoS (Point of Sale / Micro ATM) through the Business Correspondent (BC)/Bank Mitra of any bank using the Aadhaar authentication.

How to get it:

- Provide KYC (Know Your Customer) information to open a new account
- Aadhaar Number should be linked with bank a/c

Service Activation:

- None
- 1-2 minutes post Aadhaar seeding

What is required for Transaction:

- MicroATM
- Remember Aadhaar
- Give Bank name
- Present self (Aadhaar holder) with Bio-metrics (Finger and/or IRIS)
- Assisted mode

Transaction Cost:

- NIL to customer
- Merchant or BC may get charged or paid based on bank‘s discretion

Disclaimer: The transaction costs are based on available information and may vary based on banks.

Services Offered:

- Balance Enquiry
- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar funds transfer
- Payment Transactions (C2B, C2G Transactions)

Funds Transfer limit:

- Banks define limit. No limit for RBI.

Disclaimer: The funds transfer limits are based on available information and may vary based on banks.

Service Available from no. of operators:

- 118 banks
- Interoperable

What is AePS?

AePS full form is Aadhaar-enabled payment system. It is created by National Payments Corporation of India. Users can use the AePS service to make transactions on a micro-ATM by simply providing biometric information and an Aadhaar number. **The following are the specifics of AePS:**

- AePS is a mechanism that allows an Aadhaar card holder to make transactions through an Aadhaar-linked bank account in the same way that a debit/credit card transaction does
- The transaction is completed by submitting the Aadhaar card number and biometric details at Points of Sale (PoS) or micro ATMs via any bank’s business correspondent using Aadhaar authentication
- The biometric data can be iris or fingerprint scan

- Users are not required to provide their bank account details to complete the transaction
- AePS enables users to transfer funds from one bank account to another
- AePS transactions are safe and secure because users must submit their biometrics in order to complete the transaction

What are the Benefits of AePS or Aadhaar Enabled Payment System?

The following are the advantages of AePS or Aadhaar enabled payment system for all segments of society:

- Aadhaar enabled payment system is easy to use
- It necessitates the submission of biometric data as well as the Aadhaar card number
- It empowers the underprivileged section of the society
- Users are not required to provide their bank details to complete the transaction
- It enables users to easily access their bank accounts using Aadhaar authentication
- AePS is completely safe as one needs to submit biometric data and Aadhaar number
- Micro PoS machines can be taken to remote villages to allow users to easily conduct transactions

Features of AePS

The following are the primary characteristics of an AePS facility:

- The transaction amount will only be deducted from the Aadhaar linked bank account
- The mechanism enables an Aadhaar card holder to perform basic banking transactions such as cash deposit, intrabank to interbank fund transfer, cash withdrawal, balance inquiry, and obtaining a mini bank statement via banking correspondent

What is required to use the AePS facility?

Following are the must-have requirements to use the AePS facility:

- An Aadhaar card should be linked with the bank account
- Aadhaar number
- Fingerprint biometric of the Aadhaar card holder
- Micro ATM

Objectives of AePS Service

Following are the objectives of AePS service:

- Customers can use the AePS system to access their Aadhaar-linked bank accounts to perform tasks including cash deposits, cash withdrawals, intrabank or interbank fund transfers, balance inquiries, and getting a mini statement.
- It simplifies the distribution of funds under various government programmes such as NREGA, Social Security pension, Handicapped Old Age Pension, and others.
- It contributes to the Indian government's and reserve bank's goal of encouraging payment electrification and increasing financial inclusion.
- Its goal is to lay a solid foundation for Aadhaar-based banking services.

How Does AePS Work?

You can obtain essential financial services by simply remembering 12 digit Aadhaar number. The Aadhaar number is linked to your bank account. To authenticate a transaction or use an AePS facility, you must use your fingerprint, which is authenticated with your Aadhaar. The bank will only process your transaction after the UIDAI authenticates your fingerprint. Assume a man claims to be Anvay and shows the Aadhaar number associated with Anvay's name. Anvay wants to make a transaction to pay for his purchases from a merchant. Hence, he must provide his fingerprint to verify the transaction; if the fingerprint matches, the bank will proceed with the transaction.

- As a result, a large number of facilitators are involved at any given time.
- The person who wishes to conduct the transaction.
- The intermediary (merchants/storeowners) or banking correspondent through which you desire to conduct the transaction
- The Aadhaar-enabled bank.
- UIDAI. For fingerprint authentication.
- NPCI, for transaction settlement.

What is AePS cash withdrawal limit?

NPCI has set the maximum transaction amount for a single AePS financial transaction at Rs. 10,000.

AePS Funds Transfer limit

The RBI does not impose any restrictions on AePS transactions. However, some banks have imposed a daily limit of Rs. 50,000 on the total number of transactions.

Charges for AePS transactions

AePS transactions are slightly more expensive than UPI transactions. AePS transactions can cost up to Rs. 15 per transaction. The transaction cost is distributed as follows:

- Although the UIDAI has not yet imposed any fees, it may do so in the future.
- The bank may charge up to 1% of the transaction. The minimum fee is Rs. 5 and the highest is Rs. 15.
- NPCI may levy a fee of 15 to 25 paise for settlement.

Currently, the Union government bears the cost of AePS payment until December 2019. It covers debit card, UPI, and AePS MDR fees. As a result, AePS transactions are currently free of charge.

Banking Services Offered by AePS

- Cash Deposit
- Cash Withdrawal
- Balance Enquiry
- Mini Statement
- Aadhaar to Aadhaar Fund Transfer
- Authentication
- BHIM Aadhaar Pay

Other Services offered by AePS

- eKYC
- Tokenization
- Aadhaar Seeding Status

Things to keep in mind while using AePS

Keep the following things in mind when using the AePS facility:

- A bank account must be linked to an Aadhaar number in order to use the AePS service
- PIN or OTP is required to complete the transaction
- Only the primary account can be used to make transactions if multiple accounts are linked to Aadhaar
- This facility is only available to Aadhaar-linked bank accounts

Digital payments related common frauds and preventive measures

With the emergence of the internet, there is a significant rise in digital payments. Most of the customers, across the globe, are probably online. More people are opting to shop online for items like clothes, furniture, cosmetics, shoes, fast-food, etc. that typically would have been purchased in-store.

Not only virtual shopping, but online financial investments have increased tremendously with the increase in the number of people opening online investment accounts. The internet is considered by investors as a primary instrument to research and trade securities, including stocks and bonds. Investors collect a lot of information with respect to the stock and make the decision to buy or sell. Online platforms are cheap and make it easy for them to buy or sell.

At the same time, the risk of fraudulent activities has increased too. With numerous customers making use of digital payment and storing the card details and other crucial information online, scammers can’t avoid taking advantage, resulting in the rapid growth of digital payment fraud.

What is digital payment fraud?

Digital payment fraud is any form of the fake or fraudulent transaction completed by a hacker or cyber-criminal. With the advancement of technology, Cyber Crime is also increasing. Through the internet, the attacker robs the person of funds, private merchandise, interest, or confidential details. These activities can be classified as unauthorized transactions, loss of merchandise, false refunds, etc.

Internet fraud in e-commerce is popular ever since e-commerce sites were introduced. Since companies figured out a way that consumers could securely purchase goods from them without actually visiting the physical store, criminals also have done their best to access and profit from that data available on the internet.

How does it happen?

Scammers have become skilled in illegally collecting data online. Hackers often pretend as legitimate people and contact the card owners asking for sensitive details and information. They then use several ways, as mentioned below, to interact and steal crucial data.

- Email
- Messages
- Illegal websites
- Phone calls
- Sending malicious software to smartphones

Cybercriminals often operate in teams to breach data security systems. They check for bugs or fixes that have not been updated in quite some time. Such loopholes make it easy for hackers to gain access around the firewall and acquire confidential information.

Types of digital payment fraud

Identity theft – This is not a new thing, since it also happens outside cyberspace. Typically, this type of fraud entails a cybercriminal stealing your personal information by spoofing your system. In order to perform illegal online payment transactions, the hacker then uses your data. Since the cybercriminal has all the essential details, they can bypass restrictions and firewalls on fraud detection.

The merchant on the e-commerce website might not realize that it is the hacker who is doing the transaction instead of the real user, as all the details are being provided.

Phishing – You would have come across numerous email subscriptions and websites that persuade you to opt for updates and notifications. In most cases, these sources would ask you to provide certain personal information, including your credit card details. If the email is not from a reliable source, your data will be compromised and used to carry out fraud e-commerce transactions. This is known as a phishing attack.

Merchant Identity Fraud – This involves a fraudster that builds a platform quite similar to that of the merchant account. The attacker then proceeds and imposes fake payments and fees on stolen credit cards. This whole operation is carried out in a quick way before the cardholders realize they are being cheated.

Pagejacking – At times, e-commerce websites are hacked by criminals who direct the customers to an unsecured network. This untrusted site can contain malware that can break webpage security systems and steal the customer’s funds.

Securities fraud – Speed, fast access, and anonymous activity, all provide a suitable atmosphere for securities and stock market fraud. This can happen in several ways.

The most common of all involves providing misleading or fake information on a specific stock to shoot up its price. Investors treat this information as genuine and start buying the stock, resulting in a price increase. By the time they realize that the information is fake, the stock price falls, and the investors lose their money.

Another way is to offer stock that simply does not exist. Online investors, surfing the internet for information, invest in such stocks without realizing they are being the victim of a scam and eventually end up losing their money.

Stock market fraud–With the advancement in technology and everything at our fingertips, there has been a rise in stock market scams too. Unknowingly, the investors are exposed to the immense risk of a criminal who uses their personal data and investment for illegal trades, leaving investors at a loss.

Before the investor realizes that he/she has lost the money to a scam, the criminal would have shut this activity and moved to another fraud.

There is an increase in the number of victims of stock market scams in Dubai. The scammer deceives the victim by fraudulent means to persuade the investor to surrender their capital or property.

Foreign exchange fraud – This is a trading technique used to deceive investors by misleading them that by investing in the forex market, they can expect to make a high profit.

Currency trading scams also lure customers through radio advertising, newspaper ads, or appealing internet pages.

There have been cases of forex trading frauds in Dubai, involving hundreds of victims. The scams involved transfers of foreign money meant to escape bank transaction charges and investments in different small businesses.

As part of forex investment scams in the UAE, multiple investors were persuaded into forex trading with a promise of making a high profit. The brokers refused to pay the investors at some point, customers then moved to the court in order to recover their capital.

Preventive measures

E-commerce firms have already begun to raise awareness regarding internet corrupt practices. Even though it is difficult to eradicate cybercriminals entirely, you can take certain measures to prevent internet fraud.

- Use a certified payment processor
- Be updated with recent trends in digital payment fraud
- Use tested antivirus software that runs regular checks
- Encrypt the transactions and emails containing confidential information
- Regularly change your login and passwords
- Regularly update network security systems

Depending on the severity of the case, you can also seek legal opinion for guidance and expert advice.

Reporting a cybercrime

Cybercrime can be extremely difficult to investigate as it breaches legal jurisdictions. In addition, a criminal may terminate one online fraud activity and start a new activity with a fresh approach even before it is noticed by the authorities. Having said that, cybercrime law enforcement officials are becoming more vigilant and dedicate more resources to respond to such threats.

You can report your case to the local law enforcement authority as soon as you realize you are a victim of such fraud. Even though it is not necessary, but it is ideal to keep evidence of the incident. This may include mail receipts, card receipts, phone number of the caller, messages, etc.