

MODULE 4

E-Security: Information System Security; Security on the Internet: Network and Website Security Risks, How Are Sites Hacked?, Security and E-mail, Network and Website Security; E-business Risk Management Issues: The Firewall Concept, Firewall Components; E-payment Systems: Digital Payment Requirements, Online Payment Categories; Digital Tokenbased E-payment Systems, Benefits to Buyers, Benefits to Sellers, Convenience, Credit Cards as E-payment Systems, Encryption and Credit Cards 266 The Mobile Payments; Classification of New Payment Systems: Smart Card Cash Payment System, Micropayment Systems, Properties of 2 Electronic Cash (E-cash), E-cash in Action, Using the Digital Currency, Operational Risk and E-cash, Legal Issues and E-cash; Customer Relationship Management: Converting Clicks to Customers, Managing Customer Value Orientation and Life Cycle, The Customer Retention Goal.

E-Security

Information System and Security

ET stands for Teletype Network. It is a **client/server application protocol** that provides access to virtual term

- Organizations increasingly depend on digital infrastructure due to advancing technology
- Ensuring system security has become a top priority.
- Over 60% of businesses experienced cyber attacks in the past year.
- Data breaches are among the most common and costly attacks.
- Cyber attacks can cause:

Loss of sensitive data

Financial damage

- Cyber security is not just a technical issue but a key business concern.

- Understanding information security systems is essential for everyone, not just IT professionals.

It helps:

Protect sensitive data

Build strong strategies against cyber threats.

What is Information System and Security?

An **information system** is a set of tools that perform certain operations within an organization. These operations include collection, processing, storage, and distribution of information to make key decisions. Information systems help organizations to achieve their goals by improving efficiency and supporting business operations by processing data and providing meaningful information.

which is provided The computer

Goals of Information System Security

The three major goals for any information security system to achieve are the key principles of the CIA triad. The [CIA triad](#) forms the foundation of any information security system:

Security Principle	Description
Confidentiality	Ensures that information is only accessible to those authorized to view it.
Integrity	Ensures that information remains unaltered and accurately represents its intended state.
Availability	Ensures that information is accessible when needed by authorized individuals.

Steps to form an Information System Security Framework

An organisation needs to frame a standard security structure to maintain the security of its information system. There should be a set of steps that must be followed to plan this framework and implement it.

Here is a breakdown of the **Information Security Framework** process in stages:

1. Identify

The first stage of the Information Security Framework focuses on understanding the organization's business, its goals, and the risks that might come up with managing its information and systems. In this stage they find out vulnerabilities, potential threats, and the sensitive information assets that need protection. Regular risk assessments are performed to estimate these risks.

Understanding the business context and requirements for the information systems.

Identifying critical information assets that need protection.

Regularly conducting risk assessments to find vulnerabilities and establish appropriate mitigation strategies.

For Example :

In a hospital the critical assets would be identified as patient records and risk assessment will be conducted to find the outdated software, data stored without encryption or proper backup, the IoT based digital equipment vulnerable to being targeted by the attackers etc.

2. Protect

The next stage involves putting up **safeguards** to protect the identified information and systems in the previous step. This includes firewalls and antivirus software, organizational policies, legal documents (like contracts and agreements), training and awareness. These methods are take care of during project development and internal operations.

Deploying technologies to secure information (e.g., antivirus, firewalls).

Implementing security policies and formal responsibilities.

Creating legal safeguards, such as contracts and agreements with suppliers.

For Example

Installation of protection mechanisms like firewalls, encrypting the critical data, and implement a strong authentication system for all the employees.

3. Detect

Actively monitoring of information systems to identify security incidents in real-time. By using detection tools and techniques, the organization can spot suspicious activities earlier. Regular monitoring is important to ensure the security and identify any potential risks.

Continuously monitoring network and system activities.

Using tools and resources to detect abnormal or suspicious behavior.

Analyzing and understanding the potential risks associated with detected incidents.

For Example:

Active monitoring tools like **Intrusion detection software** to look after the network traffic for unusual activities, like unauthorized access attempts to patient records, or critical devices equipped in the hospital.

4. Respond

Once a security incident has been detected, it is needed to respond quickly. This stage focuses on **minimizing the impact** of the incident by responding timely and correctly. This stage includes communication with relevant stakeholders, such as managers, staff, partners, or law enforcement, as well as implementing response measures. It also involves analyzing the situation to frame an effective response and looking for ways to improve the process.

- Ensuring a prompt and effective response to the incident.
- Informing relevant stakeholders about the breach and ongoing actions.
- Mitigating the impact of the incident and learning from the experience to improve future responses.

For Example:

After detecting unauthorized access, the hospital immediately **locks the suspicious account**, informs the relevant staff, and starts investigating the origin and cause of the breach.

4. Respond

Once a security incident has been detected, it is needed to respond quickly. This stage focuses on **minimizing the impact** of the incident by responding timely and correctly. This stage includes communication with relevant stakeholders, such as managers, staff, partners, or law enforcement, as well as implementing response measures. It also involves analyzing the situation to frame an effective response and looking for ways to improve the process.

- Ensuring a prompt and effective response to the incident.
- Informing relevant stakeholders about the breach and ongoing actions.
- Mitigating the impact of the incident and learning from the experience to improve future responses.

For Example:

After detecting unauthorized access, the hospital immediately **locks the suspicious account**, informs the relevant staff, and starts investigating the origin and cause of the breach.

- **Tools for Information System Security**
- **1. Authentication**
- **2. Access Control**
- **3. Encryption**
- **4. Backups**
- **5. Firewalls**

1. Authentication : Authentication is the process of verifying the identity of a user, device, or system before granting access to resources. It ensures that only authorized individuals can access sensitive information through methods such as passwords, biometrics, smart cards, or multi-factor authentication (MFA).

- **2. Access Control :** Access control is a security mechanism that regulates who can view, use, or modify information and system resources. It assigns permissions based on user roles and responsibilities, ensuring that users can access only the data necessary for their tasks.
- **3. Encryption :** Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) using cryptographic algorithms. It protects sensitive

information from unauthorized access during storage and transmission, ensuring data confidentiality and security.

- **4. Backups :** Backups are copies of important data stored separately from the original data. They help organizations recover information in the event of hardware failure, accidental deletion, cyberattacks, or natural disasters, ensuring business continuity and data availability.
- **5. Firewalls :** A firewall is a network security tool that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between trusted internal networks and untrusted external networks, helping to prevent unauthorized access and cyber threats.

What Is Network Security?

- Network security incorporates various technologies, processes, and devices into a broad strategy that protects the integrity, confidentiality, and accessibility of computer networks. Organizations of all sizes, industries, or infrastructure types require network security to protect against an ever-evolving cyber threat landscape.

Security Risks in Website

1. Injection

[Injection](#) or [SQL](#) injection is a type of security attack in which the malicious attacker inserts or injects a query via input data (as simple as via filling a form on the [website](#)) from the client-side to the server. If it is successful, the attacker can read data from the database, add new data, update data, delete some data present in the database, issue administrator commands to carry out privileged database tasks, or even issue commands to the [operating system](#) in some cases.

2. Broken Authentication

It is a case where the authentication system of the web application is broken and can result in a series of security threats. This is possible if the adversary carries out a brute force attack to disguise itself as a user, permitting the users to use weak passwords that are either dictionary words or common passwords like “12345678”, “password” etc.

3. Sensitive Data Exposure

As the name suggests, this means that sensitive data stored is leaked to malicious attackers. This information can include personal data like name, address, gender, date of birth, personal identification numbers like Aadhaar card number or SSN, etc.,

4. Insufficient Logging and Monitoring

This is the most common reason for most major [breaches](#) to occur. Since most organizations do not invest in monitoring and effective logging or responding in a timely manner to the threat, the attackers can easily break the security system and can operate till days.

How Websites Are Hacked

1. Malware and Backdoors

[Malware](#) is a type of malicious software that computer systems, often exploiting security weaknesses such as outdated software, insecure coding practices, or third-party integrations. Once infected, they can cause frequent [website crashes](#) and security breaches.

A [backdoor](#) is an access control software vulnerability that can allow attackers to gain unauthorized access to your website. These can be flaws in the code or malware infections, allowing attackers to mislead login procedures to hijack the site.

2. SQL Injection

An [SQL injection](#) (SQLi) is a type of cyber-attack where a hacker slips malicious code into a website's database to alter or steal confidential data.

The attacker usually manipulates text input fields, like those used for login or search functions, to send SQL commands to the database to trick it into performing an unauthorized action, like providing direct access to the system.

3. Brute Force Attacks

Brute force attacks are a trial-and-error method hackers use to decode encrypted data such as passwords. This is done by systematically checking all possible password combinations until the correct one is found. Attackers employ automated tools to generate password combinations.

4.Cross-Site Scripting (XSS)

Cross-site scripting is a security vulnerability that allows attackers to inject malicious scripts into web pages. It allows cybercriminals to steal user data, deface websites, or redirect visitors to harmful sites.

XSS attacks can occur in various forms, often exploiting vulnerabilities in user-generated content.

Common examples include:

Reflected XSS – malicious scripts are reflected back to the user’s web browser through URLs, error messages, or other dynamic content.

Stored XSS – scripts are injected into a website’s database and executed whenever the affected page is loaded.

DOM-based XSS – attackers inject scripts directly into a web page’s Document Object Model (DOM), exploiting vulnerabilities in JavaScript libraries or frameworks.

What Is Email Security?

- Email security is the framework of technologies, protocols, and policies designed to protect email communications from cyber threats while maintaining message confidentiality, integrity, and availability.
- Modern email security platforms deploy multi-layered defense mechanisms that combine traditional signature-based detection with advanced behavioral analytics and machine learning (ML) algorithms.
- These systems prevent unauthorized access resulting in [data breaches](#), detect and block malicious content, and ensure the privacy of sensitive information being transmitted.

What Is Email Security?

- Email security is the framework of technologies, protocols, and policies designed to protect email communications from cyber threats while maintaining message confidentiality, integrity, and availability.

- Modern email security platforms deploy multi-layered defense mechanisms that combine traditional signature-based detection with advanced behavioral analytics and machine learning (ML) algorithms.
- These systems prevent unauthorized access resulting in [data breaches](#), detect and block malicious content, and ensure the privacy of sensitive information being transmitted.

Why Is Email Security Important?

- Email security is important because it has become a business-critical imperative as cyber threats reach unprecedented scale. Email is widely known as the number-one threat vector for cyber-attacks. Meanwhile, cyber criminals are increasingly tweaking their tactics and techniques to exploit email vulnerabilities, with AI-powered attacks affecting about [seven in eight organizations](#) in the past year.

What is network security?

- Network security combines policies and technologies to protect systems and digital assets from unauthorized access, misuse, and disruption. By using layered defenses rather than a single control, it ensures data integrity and reliable performance across increasingly complex, distributed networks.

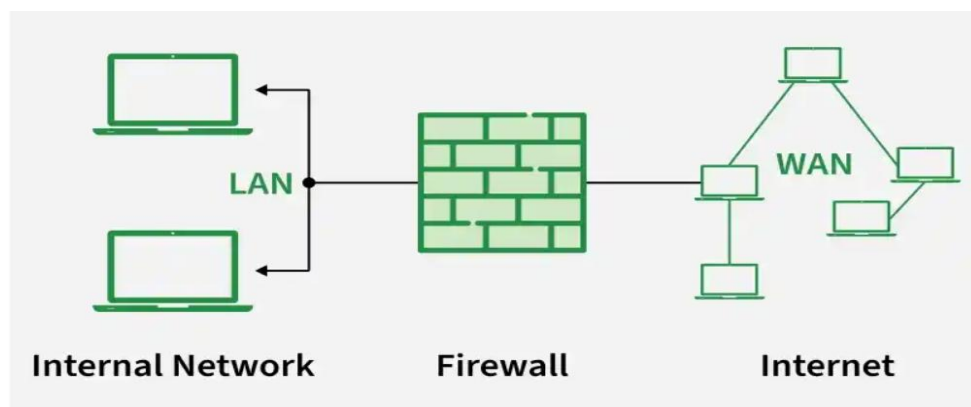
Why network security matters

- Enterprise networks support critical business operations and connect users, devices, applications, and data across on-premises infrastructure, cloud environments, and remote locations. At the same time, threat activity continues to evolve, and attackers increasingly target the network layer to move laterally, disrupt services.
- **Network security plays a central role in three areas:**
 - Threat and risk prevention, by reducing exposure and limiting the impact of attacks
 - Compliance and governance, by enforcing access controls, monitoring activity, and supporting audit requirements
 - Operational resilience, by helping organizations maintain availability and recover quickly during incidents.
- **Core properties of a secure network**

- The effectiveness of a network security program is measured against three foundational properties:
- **Confidentiality** ensures information and network resources are accessible only to authorized entities. Encryption, identity-based access controls, and secure authentication mechanisms help protect data.
- **Integrity** protects against unauthorized or accidental modification of data and network processes. Techniques such as cryptographic hashing, digital signatures, and validation checks help ensure data accuracy and trustworthiness.
- **Availability** ensures reliable access to network services and resources. Protections against denial-of-service attacks, redundancy, and resilient architectures help maintain uptime and performance.

E-business Risk Management Issues: The Firewall Concept, Firewall Components

- **Firewall** is a network security system, available as hardware or software, that monitors and controls incoming and outgoing traffic based on predefined rules. It acts like a security guard, filtering data packets to either:
 - **Accept:** Allow the traffic.
 - **Reject:** Block with an error response.
 - **Drop:** Block silently without response.



Importance

Prevent Unauthorized Access: Like a locked door with a guard, only trusted users and traffic are allowed through.

Block Malicious Traffic: Harmful data such as viruses, phishing attempts, or denial-of-service (DoS) attacks are stopped before reaching the system.

Protect Sensitive Information: Safeguards personal and business data from theft or accidental leaks.

Control Network Usage: Enforces policies such as parental controls, workplace restrictions, or government filtering.

Mitigate Insider Risks: Detects suspicious applications or data exfiltration attempts from within the network.

Working of Firewall

- A firewall inspects all incoming and outgoing traffic and decide whether to allow or block it.
- All data packets entering or leaving the network must first pass through the firewall.
- The firewall examines each packet against predefined security rules set by the organization.
- If the packet matches safe rules, it is allowed; if it is suspicious, blacklisted, or contains malicious content, it is blocked.
- Blocked or unusual traffic is recorded in logs, and real-time alerts may be generated for serious threats.
- Since it is not possible to define every rule, the firewall applies a default policy (accept, reject, or drop). Setting the default policy to drop or reject is considered best practice to prevent unauthorized access.
- **What are the different components**
- A **firewall** is a network security system that acts as a protective barrier between a trusted internal network and untrusted external networks like the internet. It monitors and controls incoming and outgoing network traffic based on predetermined security

rules, filtering data packets to allow or block them according to the organization's security policy.

- **Components of a Firewall System**

- **1.Perimeter Router :** The **perimeter router** provides the connection link between the internal network and external networks such as the internet.

- **2. Firewall**

- The **firewall** is the core security component that provides multiple levels of protection by monitoring and controlling traffic between different network zones.

- **3. Virtual Private Network (VPN) :** A **VPN** creates secure encrypted tunnels between remote networks or individual devices.

- **4. Intrusion Detection System (IDS) :**An **IDS** continuously monitors network traffic and system activities to identify, analyze, and respond to potential security threats

- **Components of a Firewall System**

- **1.Perimeter Router :** The **perimeter router** provides the connection link between the internal network and external networks such as the internet.

- **2. Firewall**

- The **firewall** is the core security component that provides multiple levels of protection by monitoring and controlling traffic between different network zones.

- **3. Virtual Private Network (VPN) :** A **VPN** creates secure encrypted tunnels between remote networks or individual devices.

- **4. Intrusion Detection System (IDS) :**An **IDS** continuously monitors network traffic and system activities to identify, analyze, and respond to potential security threats

- **Components of a Firewall System**

- **1.Perimeter Router :** The **perimeter router** provides the connection link between the internal network and external networks such as the internet.

- **2. Firewall**

- The **firewall** is the core security component that provides multiple levels of protection by monitoring and controlling traffic between different network zones.
- **3. Virtual Private Network (VPN)** : A VPN creates secure encrypted tunnels between remote networks or individual devices.
- **4. Intrusion Detection System (IDS)** :An IDS continuously monitors network traffic and system activities to identify, analyze, and respond to potential security threats

Architecture Type	Operation Level	Key Features
Packet Filter	Network Layer (Layer 3)	Examines packet headers, filters based on IP addresses, ports, and protocols
Circuit Filter	Session Layer (Layer 5)	Monitors TCP handshakes and connection states, validates session establishment
Application Level Filter	Application Layer (Layer 7)	Deep packet inspection, content filtering, application-specific security rules

Conclusion

A comprehensive firewall system integrates multiple security components including perimeter routers, firewalls, VPNs, and IDS to create layered defense mechanisms. The choice of firewall architecture – packet filtering, circuit filtering, or application-level filtering – depends on the organization's specific security requirements and performance considerations.

Digital Payment Regulations in India

Various regulatory authorities in India control the digital payment industry, including the RBI, the NPCI, and the Ministry of Electronics and Information Technology.

Reserve Bank of India and National Payments Corporation of India

The RBI regulates digital payment systems in India, such as electronic cash transfers, prepaid payment instruments, and card payments.

Payment and Settlement Systems Act, 2007

All digital payments in India, including those made using mobile wallets, prepaid cards, and online platforms, are governed under the [Payment and Settlement Systems Act, 2007](#).

Ministry of Electronics and Information Technology

MeitY is in charge of developing the country's digital infrastructure, which includes e-governance, digital literacy, and digital payments. It collaborates with other regulatory bodies and industry stakeholders to promote digital payment system adoption in India.

Pradhan Mantri Jan Dhan Yojana

With the introduction of new payment systems and the execution of various initiatives to promote digital payments, India's legislative framework for digital payments has undergone considerable changes in recent years.

Retail payments systems (RPS)

Cards continue to be the preferred payments instrument, along with cash. Although there has been a significant shift towards mobile and contactless payments, prepaid cards or SVFs are widely accepted.

Develop high-value payment systems (HVPS)

- HVPS plays a vital role in the overall financial infrastructure by ensuring settlement of payments obligations between banks. HVPS has come a long way from deferred net settlement (DNS) systems which settle transactions only at the end of each day to real-time gross settlement (RTGS) systems which settle transactions on a continuous basis
- **Financial inclusion**
- Financial inclusion has been able to bring unbanked population from primarily rural/semi-urban areas under the ambit of banking services. It has also given rural banking services an opportunity to become a part of mainstream banking.
- **What is payment methods?**
- Payment methods refer to the different ways people and businesses transfer and receive money for products and services. This includes the old-school cash and checks along with today's more advanced digital ways (credit cards, debit cards, mobile wallets, UPI, online bank transfers, etc.).
- **Different types of payment modes**
- In today's digital age, a plethora of payment modes cater to diverse consumer preferences. Let's explore some common ones:
-

1. Debit Card Payments:

Advantages: Convenient, widely accepted, linked to your bank account.

Disadvantages: Limited spending based on available funds.

2. Credit Card Payments: Advantages : Offers credit, rewards programs, and purchase protection.

Disadvantages: Can lead to debt if not managed responsibly.

3. Prepaid Cards: Advantages: Pre-funded, limits spending, good for budgeting.

Disadvantages: Limited spending power, may have fees.

4. Digital Wallets: Advantages: Convenient, contactless payments, often offer cashback.

Disadvantages: Security risks if not used cautiously.

5. Cash: Advantages: Widely accepted, no fees, privacy.

Disadvantages: Inconvenient to carry, risk of theft, limited tracking.

6. Autopay: Advantages: Automated bill payments, avoids late fees, saves time.

Disadvantages: Requires careful setup to avoid overdrafts.

Digital Token-based Electronic Payment System

A digital token-based electronic payment system is a financial technology (FinTech) solution that facilitates secure and efficient transactions using digital tokens rather than traditional currencies like cash or credit cards. These systems leverage blockchain technology or other cryptographic methods to create and manage digital tokens, enabling a variety of payment scenarios.

1. Digital Tokens: Digital tokens are units of value that represent real or virtual assets. These tokens are created, stored, and transacted electronically. They can represent various assets, such as:

Digital representations of physical assets (e.g., real estate, commodities).

Utility tokens that grant access or usage rights to a particular platform or service.

Security tokens that represent ownership in an asset, such as company shares.

2. Blockchain Technology: Many digital token-based payment systems are built on blockchain technology, a decentralized and immutable ledger. Blockchain ensures transparency, security,

and trust in transactions by recording every transaction in a tamper-resistant manner across a distributed network of nodes.

3.Smart Contracts: Smart contracts are self-executing agreements with predefined rules encoded on the blockchain. They automatically execute when certain conditions are met, enabling trustless and automated transactions.

Benefits to Buyers in Digital Entrepreneurship (Detailed Explanation)

Digital entrepreneurship means doing business using digital platforms such as websites, mobile apps, social media, and e-commerce portals. It provides many advantages to buyers (customers) because it makes purchasing easier, faster, and more convenient.

1. Convenience and Easy Access

Buyers can purchase products or services anytime and from anywhere using smartphones, laptops, or computers. They do not need to visit physical stores.

Example: A customer can order groceries online at midnight.

Benefits:

Saves time

No travel needed

Available 24/7

2. Wide Variety of Choices

Online platforms provide access to thousands of products from different brands and sellers in one place.

Example: A buyer can compare clothes, shoes, and electronics from many sellers on one website.

Benefits:

More options available

Easy to find desired products

Access to global brands

3. Price Comparison

Digital platforms allow buyers to compare prices of the same product across different websites.

Example: Comparing mobile phone prices on Amazon, Flipkart, and other websites.

Benefits:

Helps save money

Best deals can be selected

Transparent pricing

4. Lower Prices and Discounts

Online businesses often offer discounts, coupon codes, cashback, and festive sales.

Example: Big Billion Days, Great Indian Festival sales.

Benefits:

Affordable shopping

Seasonal offers

Cashback rewards

5. Customer Reviews and Ratings

Buyers can read reviews and ratings from other customers before purchasing.

Example: Before buying headphones, a buyer checks star ratings and comments.

Benefits:

Better decision making

Reduces risk of poor-quality products

Builds trust

Benefits to Sellers in Digital Entrepreneurship (Detailed Explanation)

Digital entrepreneurship means running a business through digital platforms such as websites, mobile apps, social media, and online marketplaces. It offers many advantages to sellers by helping them reach more customers, reduce costs, and grow faster.

1. Global Market Reach

Sellers can sell products or services to customers from different cities, states, and countries through the internet.

Example: A small handmade craft seller in Mysore can sell products across India using online platforms.

Benefits:

More customers

Increased sales opportunities

2. Low Startup Cost

Starting an online business often requires less investment than opening a physical store.

Example: A seller can start with an Instagram page or website instead of renting a shop.

Benefits:

No shop rent

Lower electricity and maintenance cost

Affordable business setup

3. 24/7 Business Operations

Online stores can accept orders anytime, even when the seller is sleeping.

Benefits:

Continuous sales

No time restrictions

More convenience for customers and sellers

4. Direct Customer Connection

Digital platforms allow sellers to interact directly with customers through messages, chats, email, and comments.

Benefits:

Better customer relationships

Quick feedback

Easy problem solving

5. Lower Marketing Cost

Digital marketing through social media, SEO, WhatsApp, and email is cheaper than TV, newspaper, or print advertising.

Example: Promoting products on Instagram Reels or Facebook Ads.

Benefits:

Cost-effective promotion

Targeted advertising

Higher return on investment

Convenience in E-Payment System

Convenience is one of the biggest advantages of an Electronic Payment (E-Payment) System. It means payments can be made quickly, easily, and anytime without using cash.

Global reach and accessibility

One of the most significant advantages of e-payment systems is their ability to transcend geographical boundaries. Unlike traditional payment methods that are often limited by location and banking hours, electronic payments operate 24/7 across different time zones and countries.

Lightning-fast transaction speeds

Speed is the most noticeable advantage of e-payment systems compared to traditional methods. While a check might take several days to clear and cash transactions require physical exchange, electronic payments are processed almost instantaneously.

Real-time processing benefits

The instant nature of e-payments provides immediate feedback to both parties involved in the transaction. Customers receive instant confirmation of their purchases, while merchants can immediately verify payment receipt.

Mobile payment revolution

The rise of mobile payment solutions has taken convenience to new heights. With services like digital wallets, QR code payments, and near-field communication (NFC) technology, consumers can complete transactions using just their smartphones.

Anytime and Anywhere Payment

Users can make payments 24/7 from any place using a mobile phone, laptop, or computer. There is no need to visit a bank or ATM.

Example: Paying electricity bills at midnight using a mobile app.

No Need to Carry Cash

People do not need to carry cash in their wallets, reducing the risk of losing money or theft.

Example: Paying in supermarkets by scanning QR code.

Automatic Bill Payments

Users can set auto-pay for electricity, phone recharge, subscriptions, and loans.

Example: Monthly Wi-Fi bill paid automatically.

Credit Cards as E-Payment Systems

A **Credit Card** is an electronic payment system issued by banks or financial institutions. It allows customers to buy goods and services without paying cash immediately. The bank pays the seller first, and the customer repays the amount later within the billing cycle.

Features of Credit Cards

1. **Cashless Payment** – Customers can make payments without carrying cash. It is easy and safe to use.
2. **Buy Now Pay Later** – Users can purchase products now and pay the bill later on the due date.

3. **Credit Limit** – Every card has a fixed spending limit decided by the bank. Customers can use the card within that limit.
4. **Online and Offline Use** – Credit cards can be used in shops, malls, hotels, and online websites.
5. **Security** – Transactions are protected using PIN, OTP, CVV, and fraud detection systems.

Advantages of Credit Cards

Convenient to Use – Payments can be made quickly anytime and anywhere.

Emergency Support – Helpful when immediate money is needed for urgent expenses.

Worldwide Acceptance – Accepted in many countries and online platforms.

Safe Transactions – Reduces the need to carry cash and provides secure payments.

Builds Credit Score – Timely bill payments improve the customer's credit history.

Special Offers – Users get discounts, cashback, travel benefits, and reward points.

How transaction encryption protects payment data

Transaction encryption is the process of **converting sensitive payment data into an unreadable format** to prevent unauthorized access during transmission. When a customer initiates a transaction—whether online or at a physical point-of-sale (POS)—their payment details are instantly encrypted, ensuring that even if the data is intercepted, it cannot be read or misused.

This encryption process is a critical layer of security in modern payment systems, helping businesses:

Protect cardholder information from cyber threats and fraud attempts

Comply with regulatory requirements like PCI DSS and GDPR

Prevent data breaches that could lead to financial and reputational damage

The steps involved in encrypting a transaction

1. Data entry and encryption initiation

1. When a customer enters their card details at checkout or taps their card on a payment terminal, the data is immediately encrypted at the point of entry.
2. Secure encryption algorithms scramble the payment details, converting them into unreadable ciphertext.

2. Transmission through the payment network

1. The encrypted transaction data is sent through a secure channel to the payment processor or acquiring bank.
2. Security protocols like **TLS (Transport Layer Security)** ensure that data remains protected during transmission.

3. Practical applications of encrypted transactions: Encryption is used across various industries and payment channels to **secure transactions and protect customer data**. Some real-world applications include:

4. **E-commerce payments** – When customers enter their card details online, the data is encrypted before being transmitted to the payment processor.
5. **Mobile wallets and NFC payments** – Apple Pay, Google Pay, and contactless payments use encryption and tokenization to secure transactions.
6. **Recurring payments and subscriptions** – Encrypted payment data ensures that stored card details remain protected when businesses process recurring transactions.
7. **Bank transfers and wire payments** – Encrypted end-to-end communication safeguards banking credentials and financial transfers from cyber threats.

Types of encryption in payments

Encryption in payments can be classified into three main types, each serving a unique function in securing transaction data.

Symmetric encryption

Symmetric encryption uses a single key for both encryption and decryption. This means that the same key is used to scramble and unscramble data, making the process fast and efficient.

How it works:

The payment data is encrypted using a shared key.

The receiving system uses the same key to decrypt the data and process the transaction.

Advantages:

Faster encryption and decryption

Requires less computational power, making it ideal for high-speed transactions

Asymmetric encryption

Asymmetric encryption uses two separate keys—a public key for encryption and a private key for decryption. This method is widely used in online payments and secure communications.

How it works:

A merchant's system encrypts payment data using a public key.

The receiving payment processor decrypts the data using a private key that only they control.

Advantages:

Enhanced security – Even if the public key is exposed, transactions remain protected because the private key is required for decryption.

Ideal for online payments where secure communication is critical.

Hash functions

Hash functions are used in payment security to ensure data integrity and prevent tampering. Unlike symmetric and asymmetric encryption, hash functions do not allow decryption—instead, they generate a unique, irreversible fingerprint of the original data.

How it works:

Payment data is passed through a **hashing algorithm**, which produces a unique hash value.

If the data is altered in any way, the hash value changes, alerting the system to possible fraud.

Advantages:

Prevents data tampering by ensuring transaction records remain unchanged.

Used in password storage and blockchain transactions for added security.

CLASSIFICATION OF NEW PAYMENT SYSTEMS

Smart Card Cash Payment System

A Smart Card is a plastic card with an embedded microchip that stores data and money electronically. It is used as a cash payment system to make payments without using physical cash. The chip securely stores user information, account details, and transaction data.

Features of Smart Card

Embedded Microchip – A smart card contains an embedded microchip that securely stores and processes information. The chip can hold personal, financial, or identification data.

Cashless Payment – Smart cards enable users to make payments electronically without carrying physical cash, making transactions more convenient and efficient.

Rechargeable – Many smart cards can be reloaded with money multiple times, allowing users to continue using the card without replacing it.

Fast Transactions – Smart cards process transactions quickly, reducing waiting time at payment counters, transportation systems, and service points.

Secure System – Smart cards provide high security through PIN protection, encryption techniques, and authentication mechanisms, reducing the risk of fraud.

Portable – They are small, lightweight, and easy to carry in wallets or pockets, making them convenient for everyday use.

Multi-purpose Use – A single smart card can be used for various purposes such as banking, shopping, transportation, access control, and identification..

Advantages of Smart Card

- Easy and convenient to use.
- Reduces need to carry cash.
- Secure and less chance of fraud.
- Saves transaction time.
- Can store multiple applications in one card.
- Durable and reusable.

Disadvantages of Smart Card

- Card may be lost or damaged.
- Requires machine/card reader.
- Initial issuing cost is high.
- Technical failure may interrupt payment.

- Forgotten PIN may create issues.

Examples of Smart Cards

- ATM Card
- Debit Card
- Metro Smart Card
- SIM Card

Types of Smart Cards

1. **Contact Smart Card** – Inserted into a card reader.
2. **Contactless Smart Card** – Tap or wave near a reader using NFC/RFID technology.

1. Contact Smart Card – In Detail

A Contact Smart Card is a type of smart card that has an embedded microchip and must be physically inserted into a card reader to complete a transaction. The metal contact plate on the card touches the reader terminals, allowing data and power transfer between the card and the machine.

How It Works

The user inserts the smart card into the card reader.

The reader supplies power to the chip.

The chip exchanges data with the system.

User enters PIN/password if required.

Transaction is authorized and completed.

Main Features

1. **Embedded Chip** – Stores account details, balance, and security data.
2. **Physical Contact Needed** – Must be inserted into a machine.
3. **Secure Transactions** – Uses PIN and encryption for safety.
4. **Reusable** – Can be used many times.
5. **Fast Processing** – Transactions complete quickly.

Uses of Contact Smart Card

1. **Banking Cards** – ATM, debit, and credit cards with chip.
2. **ID Cards** – Employee or student identity cards.
3. **Telephone Cards** – Used in prepaid calling systems.
4. **Healthcare Cards** – Store patient or insurance details.
5. **Access Cards** – Used to enter offices or secure areas.

Advantages

High security due to chip technology.

Stores more data than magnetic stripe cards.

Reliable and accurate transactions.

Difficult to duplicate.

Useful for many applications.

Disadvantages

Needs a card reader device.

Card contacts may wear out over time.

Slower than tap-based contactless cards.

Card damage can stop usage.

2. Contactless Smart Card

A Contactless Smart Card is a type of smart card that contains an embedded microchip and antenna. It does not need to be inserted into a machine. The card works by simply tapping or waving near a card reader using technologies like RFID (Radio Frequency Identification) or NFC (Near Field Communication).

It is widely used for payments, transportation, access control, and identification because it is fast and convenient.

How It Works

The user brings the card near the card reader.

The reader sends radio signals to the card.

The card chip exchanges data wirelessly.

Payment or verification is completed instantly.

Features of Contactless Smart Card

1. **Wireless Communication** – No physical contact is needed.
2. **Embedded Chip and Antenna** – Stores data securely.
3. **Fast Transaction Speed** – Payment is completed in seconds.
4. **Easy to Use** – Tap or wave near the reader.
5. **Secure System** – Uses encryption and authentication.
6. **Durable** – No damage from repeated insertion.
7. **Multi-purpose Use** – Can be used for travel, banking, and access systems.

Uses of Contactless Smart Card

1. **Banking Payments** – Tap-to-pay debit and credit cards.
2. **Metro/Bus Cards** – Used in public transport systems.
3. **Office Access Cards** – Used to enter buildings.
4. **Student ID Cards** – Attendance and identification.
5. **Parking Cards** – Used in parking systems.

Advantages of Contactless Smart Card

1. Very fast and convenient.
2. No need to carry cash.
3. Easy to use for small payments.
4. Secure transactions.
5. Less physical wear and tear.
6. Saves time in queues

Disadvantages of Contactless Smart Card

1. Requires special card reader.
2. Risk of unauthorized scanning if security is weak.
3. Can be lost or stolen.
4. Limited transaction range.
5. Initial setup cost is high

MICROPAYMENT

- A **micropayment** is a [financial transaction](#) involving a very small sum of money and usually one that occurs online.
- Several micropayment systems were proposed and developed in the mid-to-late 1990s, which were ultimately unsuccessful.
- A second generation of micropayment systems emerged in the 2010s.
- A micropayment is a small online transaction, often less than a dollar or even a fraction, with varying definitions by vendors.
- Micropayments enable efficient digital content distribution, including royalties, online tips, and in-game purchases.

What Is a Micropayment?

- Micropayments are small transactions or payments usually of less than a dollar—and, in some cases, only a fraction of a cent—that are mainly made online.
- Micropayments are seen as a way to leverage the internet to facilitate the immediate distribution of digital rights, royalties, in-game purchases, online tipping, and even to coordinate devices connected via the internet of things (IoT).

How Micropayments Work and Their Impact in Fintech

- The latest technology advancements have brought about more exposure and inclusion into the digital world.
- [Fintech](#), technology in finance, is an emergent sector that is focused on making financial products available to all consumers at a negligible price.
- These technological efforts are seeing consumers' costs diminish to as low as a few cents.
- The problem with such low fees is that they may not feasibly be processable through [credit card](#) companies and their traditional transaction fee-based system. Micropayment systems have emerged to meet those needs.

Practical Applications of Micropayments

- Micropayment platforms built for handling small [transactions](#) work in a number of ways.
- One way is for a seller or service provider to have an established account with a [third-party](#) micropayment provider who collects, stores, and distributes the payments made.
- Through a [digital wallet](#) managed by the provider, payments are stored until they accumulate to a larger amount, at which point they are then paid out to the recipient.
- For easier facilitation of payments, it is necessary for consumers to also set-up an account with the same micropayment provider.
- **The Role of Micropayments in Digital Purchases**
- A micropayment is mostly limited to the realms of digital payment.
- Making a \$0.99 purchase of a music CD with shipping and handling cost of \$25.00 may not make sense to an average consumer.
- But paying \$0.99 for the digital content of the same music album could be a more rational transaction for the buyer as no physical delivery is necessary.

Properties Of Electronic Cash (E-cash)

Monetary value:-

- Monetary value is present if the electronic cash is backed by hard currency, a bank-certified cashier's check or bank-authorized credit. When e-cash created by one bank is accepted by the others, reconciliation must occur without any problems.

Storable and Retrievable:-

- Electronic cash must be storable and retrievable. Remote storage and retrieval will allow users to exchange e-cash from office, home or while traveling. The cash could be stored on a remote computer's memory, e.g. smart cards, [electronic wallets](#).

Security:-

- Electronic cash should not be easy to alter or copy while being stored or exchanged. Procedures must be in place to verify that the electronic cash is spent only once i.e. double spending issue should be taken care of.

Working of an electronic cash system:-

- **Step 1:** A customer or merchant signs up with one of the participating banks or financial institutions.

- **Step 2:** The customer receives specific software to install on his or her computer. The software allows the customer to download "electronic coins" to his or her desktop. The software manages the electronic coins. The initial purchase of coins is charged against the customer's bank account or against a credit card.
- **Step 3:** When buying the services from a website that accepts e-cash, the customer simply clicks the "Pay with e-cash" button. The merchant's software generates a payment request, describing the items purchased, price, time, and date.
- **Step 4:** The customer can then accept or reject this request. When the customer accepts the payment request, the software residing on the customer's desktop subtracts the payment that is sent to the bank or financial institution of the merchant, and then is deposited to the merchant's account.

E-Cash in Action

Introduction

- **E-Cash (Electronic Cash)** is a digital form of money used for making payments through the internet or electronic devices. It works like physical cash but exists in electronic form. In digital entrepreneurship, e-cash helps businesses receive and make payments quickly, securely, and conveniently.

Meaning of E-Cash

- E-cash is money stored electronically in mobile wallets, prepaid cards, or bank-linked payment systems. Customers can use it to buy goods and services online without using physical cash.
- **How E-Cash Works in Digital Entrepreneurship**
- **Customer Registration**
A customer creates an account in a digital wallet or payment app such as Paytm, PhonePe, or Google Pay.
- **Adding Money/Linking Bank Account**
The customer adds money to the wallet or links a bank account / card.
- **Making Purchase**
The customer selects products or services from an online store or app.
- **Payment through E-Cash**
The payment is completed digitally using QR code scan, wallet balance, or UPI transfer.
- **Instant Confirmation**
Both customer and entrepreneur receive immediate payment confirmation.

Role of E-Cash in Digital Entrepreneurship

Role of E-Cash in Digital Entrepreneurship

Supports Online Businesses

E-commerce stores, freelancers, subscription services, and digital startups can receive payments online.

Faster Transactions

Payments are completed instantly, saving time.

Cashless Operations

Reduces dependence on physical cash handling.

Wider Customer Reach

Customers from different locations can pay easily.

Better Record Keeping

Every transaction is digitally recorded for accounting.

Advantages of E-Cash

1. Convenient and easy to use
2. Fast payment processing
3. Secure with PIN/OTP/biometric verification
4. Reduces cash theft risk
5. Useful for small and large transactions
6. Promotes 24×7 business operations

Limitations / Disadvantages

1. Requires internet or mobile network
2. Risk of cyber fraud if careless
3. Technical failures may delay payment
4. Some users may lack digital literacy

Real-Time Example

A small online clothing seller on Instagram accepts payments through Google Pay and PhonePe. Customers pay instantly, and the seller dispatches the order quickly.

Using The Digital Currency

Introduction

Digital currency is money available in electronic form and used for online or digital transactions. It does not exist as physical notes or coins. It is transferred through computers, smartphones, and digital networks. In digital entrepreneurship, digital currency helps businesses perform fast, secure, and cashless transactions.

Meaning of Digital Currency

Digital currency refers to a type of currency that is stored, managed, and exchanged electronically. It can be used to buy goods and services, transfer money, and make payments online.

Examples include:

Central Bank Digital Currency (CBDC) such as Digital Rupee

Cryptocurrencies like Bitcoin

Wallet-based balances used in digital systems

How Digital Currency is Used

1. Creating a Digital Wallet / Account

Users first create an account in a digital wallet or approved payment platform.

2. Adding Funds

Money is added from a bank account or received from another user.

3. Purchasing Products and Services

Customers use digital currency to buy products from e-commerce websites, apps, or online businesses.

4. Peer-to-Peer Transfers

Users can send money directly to another person instantly.

5. Business Payments

Entrepreneurs can pay suppliers, freelancers, and service providers digitally.

Advantages of Digital Currency

1. Fast and instant transactions
2. 24×7 payment availability
3. Lower transaction cost in many cases
4. Convenient and paperless system
5. Better transaction records
6. Supports online and global business

Disadvantages

1. Needs internet and devices
2. Risk of hacking or scams if security is weak
3. Technical failures may interrupt payments
4. Limited acceptance in some places

Real-Time Example

An online course creator accepts payments using Google Pay or Digital Rupee. Students pay instantly, and access is provided immediately.

Operational Risk

Meaning

Operational risk is the risk of loss resulting from internal failures, human errors, system breakdowns, fraud, or external disruptions that affect business operations.

Causes of Operational Risk

1. HumanError

Mistakes made by employees while processing payments, orders, or data.

2. SystemFailure

Server crashes, software bugs, network downtime, or payment gateway failure.

3. Fraud and cybercrime Hacking, phishing, identity theft, and unauthorized transactions.

4. Poor Internal Processes Weak controls, lack of procedures, or delayed responses.

- 5. External Events** Natural disasters, power failure, internet outage, or regulatory changes.

Effects of Operational Risk

1. Financial loss
2. Business interruption
3. Customer dissatisfaction
4. Loss of reputation
5. Legal penalties

Managing Operational Risk

1. Strong internal controls
2. Staff training
3. Data backup systems
4. Cybersecurity measures
5. Regular audits
6. Disaster recovery plans

E-Cash

Meaning

E-Cash (Electronic Cash) is a digital form of money used for online transactions. It works like physical cash but exists electronically.

How E-Cash Works

User creates wallet/account.

Adds money or links bank account.

Selects goods/services online.

Pays using digital wallet or instant transfer.

Merchant receives payment confirmation.

Examples: Paytm, PhonePe, Google Pay

Advantages of E-Cash

Fast payments

Convenient and cashless

24×7 transactions

How E-Cash Works

User creates wallet/account.

Adds money or links bank account.

Selects goods/services online.

Pays using digital wallet or instant transfer.

Merchant receives payment confirmation.

Examples: Paytm, PhonePe, Google Pay

Advantages of E-Cash

Fast payments

Convenient and cashless

24×7 transactions

Convert Clicks Into Customers

Convert Clicks Into Customers means turning website visitors, ad clicks, or social media users into **paying customers**. In digital business, many people may click on an advertisement or visit a website, but only some of them actually buy products or services. The process of changing visitors into buyers is called **conversion**.

It is an important goal in **digital entrepreneurship** because clicks alone do not generate profit. Sales and loyal customers create business growth.

1. Utilize pop-ups

Pop-ups are one of the most efficient methods of converting clicks into customers. By displaying a small message or offer at the moment a visitor arrives on your website, you can increase the chances of them taking action.

2. Use strong calls to action

A call to action (CTA) is a statement or image that urges the reader to take a specific course of action, such as “buy now” or “sign up here.” **CTAs should be clear,impossible to miss** with the sole intention of boosting your conversion rate

3. Create compelling landing pages

A landing page is the first page that a customer sees when they click on one of your ads or links. Landing pages should be designed with conversion in mind, which means that they should be direct and to the point.

There are a few key [things to keep in mind when creating landing pages](#).

4. Offer incentives

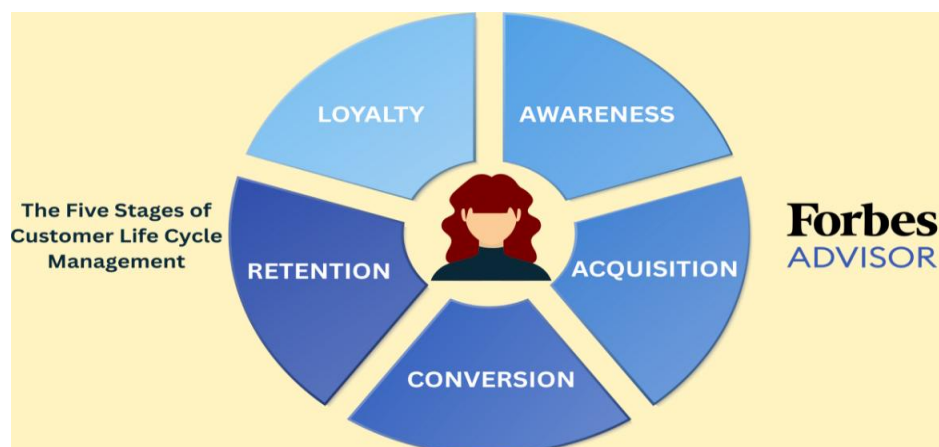
As an online business knows, one of the key metrics for success is conversion rate – the percentage of visitors who take the desired action, such as making a purchase. There are a number of ways to improve conversion rates, and one of the most effective is to offer incentives.

5. Make it easy to buy

No matter how great your product or service may be, if potential customers can't figure out how to purchase it, you're not going to make any money. That's why efficient methods of converting clicks into customers are so important.

What Is Customer Life Cycle Management (CLM)?

Customer life cycle management (CLM) is an approach taken by businesses to help them track and manage a customer's entire journey from potential customer to loyal patron. The cycle involves carefully managing each stage of a customer's journey to foster strong, long-lasting bonds that drive loyalty and business growth.



Customer Life Cycle Management Stages

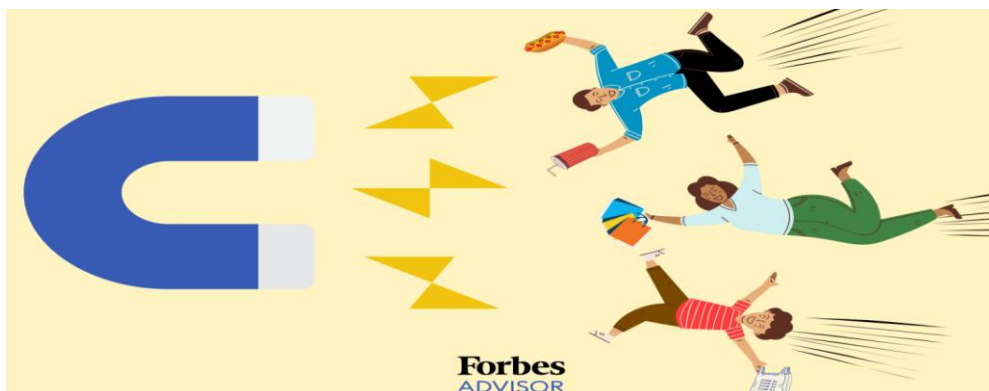
As mentioned earlier, the customer life cycle is broken down into five stages, each of which allows a business to track how each customer interacts with the brand. SMBs can use software, such as the [best CRMs for small businesses](#), to help track customer behaviors and to ensure they have the best possible brand experience.

1. Awareness



During this stage, a customer becomes aware of your brand due to your marketing efforts or through their own research. It's likely that a customer would have seen targeted ads on social media platforms such as TikTok, Instagram or Facebook, through your stellar search engine optimization (SEO) efforts, or print, radio or television ads. No matter what, your marketing efforts have paid off and you are now on the customer's radar.

2. Acquisition



As soon as that customer contacts you, whether through social media or via live chat on your website, your target has been acquired. The goal in this stage is to reel the customer in by offering information about your business and your products, maybe even some deals as well as customer support. The [best VPNs](#) are masters at this game by offering huge, hard-to-ignore deals for new customers.

3. Conversion



Congratulations! Your superpowered magnet or, if you're not an evil corporation, your ads help and you have closed the deal with a customer. Now, the task of turning that one-time customer into a loyal follower begins. In the conversion stage, it's important to determine customer behaviors, such as what touchpoint (social media, website, email list, etc.) was used, whether seasonal purchasing was a factor, what ad persuaded them and how they paid for your product. Knowing these metrics will help you start the customer retention process.

4. Retention



The hardest stage of the customer life cycle journey is retention. During this stage, you have to give your customers a reason to stick around. You need to ensure your business and offerings stand out from the crowd. You can increase your chances of retaining customers by displaying targeted ads that play on a customer's needs, wants and desires, by offering top-quality support, a reward program and by ensuring you offer deals that they simply cannot pass up.

6. Loyalty



The loyalty stage is where you turn a frequent customer into a loyal, lifelong fan of your business and products who then goes and tells the world about your brand. Whether they spread the word through social media or word of mouth, their love for your brand will help improve your chances of long-term success.

The Customer Retention Goal

Customer retention meaning Before we explain the importance of [customer retention](#), we must understand what exactly it is.

Customer retention is, put simply, a company's ability to turn buyers into repeat customers, preventing them from buying from a competitor. Long term customers are crucial for almost every type of business. From e-commerce retailers, where you want to keep existing customers engaged with your brand, to subscription-based companies where the number of retained customers you have directly impacts whether your business sinks or swims.

Why is customer retention important?

Of course, finding new customers is important and any business will want to grow and expand their [customer base](#) – but it shouldn't be at the expense of customer retention.

Keep business costs down

To start with, if you can keep your existing customers happy and ensure they come back for more, it's going to cost you less than continually having to find brand new customers. The Harvard Business Review found that acquiring a new customer can be between [five and 25](#) times more expensive than keeping an existing one.

Increase sales through upselling and cross-selling

It's easier to sell new products and services to existing customers than it is to prospects at the start of their journey with your brand. It's been found that existing customers are [50%](#) more likely than new customers to buy new products.

Improve your bottom line

When you focus on retention, you're likely to see an improvement in your business revenue. A study by [Bain & Co](#) found that increasing retention rates by as little as 5% can improve your revenue by 25-95%.

How to work out your customer retention rate

Your [customer retention rate](#) measures the number of customers your company retains over a given period, and it can be a useful metric to understand lifetime customer value.

Your retention rate is simply the inverse of your customer churn rate – so if you know that your churn rate is 60%, then your retention rate is 40%. Alternatively, if you don't know that figure, you can work out your retention rate using three key figures:

- Number of existing customers at the start of your chosen period (S).
- Number of total customers at the end of the period (E).
- Number of new customers added within the period (N).