Draft Study Material

JUNIOR CYBER SECURITY ASSOCIATE

JOB ROLE

Qualification Pack
G-04-IT-00351-2023-V1-NIELIT

SECTOR: IT-ITeS
Grades XI

विद्यया ऽ मृतमश्नुते

एन सी ई आर टी
NCERT

PSS CENTRAL INSTITUTE OF VOCATIONAL EDUCATION
(a constituent unit of NCERT, under Ministry of Education, Government of India)
Shyamla Hills, Bhopal- 462 002, M.P., INDIA
www.psscive.ac.in

Junior Cyber Security Associate

Grade – XI

Qualification Pack
G-04-IT-00351-2023-V1-NIELIT

PSS Central Institute of Vocational Education

A constituent unit of NCERT, Under Ministry of Education, Government of India
Shyamla Hills, Bhopal - 462 002, Madhya Pradesh, India

www.psscive.ac.in

DISCLAIMER

This material is only a reference study material and has been prepared by experts. Care has been taken to acknowledge the information with suitable references.

March, 2025

Published by:
Joint Director
PSS Central Institute of Vocational
Education, NCERT,
Shyamla Hills, Bhopal

CHIEF PATRON
Prof. Dinesh Prasad Saklani
Director
National Council of Educational
Research and Training (NCERT),
New Delhi

PATRON
Dr. Deepak Paliwal
Joint Director
PSS Central Institute of Vocational
Education, Bhopal

PROGRAMME COORDINATOR
Dr. Munesh Chandra
Professor (CSE), Head, ICT Centre
Department of
Engineering and Technology,
PSS Central Institute
of Vocational Education, Bhopal

PREFACE

The National Education Policy, 2020 emphasizes upon removing hard distinction between arts, science and commerce; and between curricular, co-curricular and extracurricular activities; and between vocational and general education. NEP focuses on flexible curricular structure and multidisciplinary learning. The secondary stage is for students aged between 14 and 18 and is divided into two phases: Phase 1 — Grades 9 and 10 and Phase 2 – Grades 11 and 12. The secondary stage for students aged 14-18 is divided into two phases, with the guidelines presented for grades 11 and 12. The National Curriculum Framework for School Education (NCFSE) 2023 advocates for choice-based courses, aiming to provide flexibility, remove separations between disciplines, and align with industry needs. Vocational education in the secondary stage will be an integral part of the educational system designed to provide students with practical skills and knowledge that directly prepare them for specific careers or trades. The focus should be on the holistic development of each child, addressing not only vocational skills but also social, emotional, and life skills. In schools, vocational courses are expected to align with the National Skill Qualifications Framework (NSQF) falling within NSQF levels 3 and 4. The NSQF is a quality assurance framework that organizes qualifications in a series of eight levels, in increasing order of complexity and competency. These levels are defined in terms of learning outcomes which are an explicit description of what a learner should know, understand and be able to do as a result of learning, regardless of whether these competencies were acquired through formal, non-formal or informal learning.

The NEP underscores the importance of vocational education, preparing students with practical skills aligned with industry needs. In the context of web development, this translates to equipping learners with not just theoretical knowledge but also hands-on experience. We should strive to provide comprehensive training that empowers individuals to tackle real-world challenges in the digital landscape.

Just as the NEP emphasizes the holistic development of students, our approach to web development should extend beyond technical skills. Let's prioritize the development of essential soft skills such as problem-solving, collaboration, and adaptability, ensuring that learners are well-rounded professionals capable of thriving in diverse environments.

I thank all other members for completing this task on time and in such an admirable way. I am also thankful to all the institutions and organisations which have generously extended their help and assistance in making this possible. As an organisation committed to reforming school education in Bharat and continuously improving the quality of all learning and teaching material that it develops, NCERT looks forward to critical comments and suggestions from all its stakeholders to further improve upon this textbook.

Professor Dinesh Prasad Saklani
Director
National Council of Educational Research and Training
New Delhi
April 2024

Foreword

Vocational Education and Training (VET) plays a significant role in preparing youth for relevant occupation and meeting the skill demand of the changing labour market. This is even more relevant, as India is witnessing accelerated youth population and the need for preparing skilled workforce for the growing economy. The strong partnership with the industry partners characterises India's National Shill Qualification Framework (NSQF], The Vocationalisation of Education in Schools under *Samagra Shiksha* by the Ministry of Education, Government of India is spearheading and catalysing the role of vocational education and training in equipping young people with skills.

The recent reforms through National Educational Policy (NEP) 2020 have focused on making VET system more coherent and flexible to both the needs of the labour market and social challenges. Improving the learning pathways and bridging the gap between vocational and general education and avoiding dead ends is another goal The ultimate goal is to ensure flexibility and responsiveness to the needs through education and training and to provide a strong framework for lifelong learning.

Reflecting on vocational education and training priorities, and recent developments in the system, priority has to be placed on developing vocational teachers of trainers to act as the link between education and training and employment. Preparing a cadre of professionally trained. vocational teachers is vital for imparting quality vocational education and developing skilled workforce in different sectors In this perspective, the PSS Central Institute of Vocational Education (PSSCIVE), Bhopal has introduced a 'Diploma in Vocational Education and Training' through distance mode, with the aim to develop a pool of trained vocational teachers or resource persons in spearheading the effective, Implementation of the scheme an vocationalisation of education in schools across India, The Diploma in VET is a one year programme, which will be taught in four blocks of tri-semester. It aims at providing the learners with the latest knowledge, skills and competencies in the field of vocational education and training Among others, the programme will also enable the learners to appreciate the ethical dimension of teacher professionalism in Vocational Education. The goal is to. equip the learners with a strong theoretical and practical understanding of VET while integrating ICT in their teaching.

I acknowledge the contributions of the material development team, reviewers and the support team for their contributions in the development of this self- learning material. We would welcome suggestions, which would help us to improve further the quality of this programme.

Wish you all the very best in this endeavor.

Dr. Deepak Paliwal
Joint Director
PSSCIVE, Bhopal

About the Textbook

“Junior Cyber Security Associate for class 11” is a concise yet comprehensive textbook designed to equip students with essential of cyber security. Through clear explanations and practical exercises, students learn the foundational concepts of cyber security, the cornerstones of cyber security. By engaging in hands-on projects, students gain practical experience in cyber security, network and operating systems, fostering confidence and proficiency in basic linux and windows commands and problem-solving.

This book provides a structured pathway for students to acquire valuable skills that are increasingly in demand. Whether students aim to pursue further education or enter the workforce, this textbook serves as a stepping stone to success in the dynamic field of cyber security analyst, network administrator, and system administrator. The book is divided into two units, the book meticulously covers every aspect of fundamentals of Network and Operating Systems and fundamentals of Cyber Security.

Throughout the textbook, emphasis is placed on identifying and addressing security vulnerabilities, network issues, system errors, ensuring that students develop the critical ability to build secure, stable, and efficient computing environments. Practical exercises and case studies accompany each chapter, providing hands-on experience and reinforcing theoretical concepts.

Dr. Munesh Chandra
Professor
Department of Engineering and Technology
PSSCIVE, NCERT, Bhopal

Textbook Development Team

1. Dr. Digvijay Singh Rathore, National Forensic Science University, Gandhi Nagar
2. Dr. Virendra Kumar Yadav, Indian Institute of Technology, Delhi
3. Mr. Desh Deepak Pathak, Directorate of Education, NCT, Delhi
4. Ms. Yogita Goyal, Gurukul The School, Ghaziabad
5. Ms. Soumya Trivedi, AKG Engineering College, Ghaziabad

MEMBER-COORDINATOR

Dr. Munesh Chandra,
PSSCIVE, NCERT, Bhopal

Acknowledgement

On behalf of team at the PSS Central Institute of Vocational Education (PSSCIVE), Bhopal we are grateful to the officials of the Ministry of Education, Government of India for the guidance and support at all times and levels.

We are obliged to the Director, NCERT for his care and leadership. We are indebted to the PAC NCERT for financial support.

We acknowledge the contributions of our colleagues at PSSCIVE and other experts for their academic support, untiring efforts and contributions in development of this material. The names of all the experts are acknowledged in the list of contributors.

The contributions made by the Administration and the supporting staff of PSSCIVE are duly acknowledged.

TEAM PSSCIVE

Table of Contents

Particular	Page No.
Unit -1 **Fundamentals of Network and Operating Systems**	**1-31**
Chapter-1 Introduction to Computer Networks, Its Types, and Benefits	2
Chapter-2 Networking Fundamentals and Protocol Models	13
Chapter-3 Introduction to Windows/Linux OS and its File System	23
Unit -2 **Fundamentals of Cyber Security**	**32-141**
Chapter-1 Introduction to Information Security	33
Chapter-2 Ethical Hacking and Cryptography	39
Chapter-3 Operating System Security and Access Control	46
Chapter-4 Introduction to Wireless Networks	52
Chapter-5 Introduction to Mobile Operating Systems – Android and iOS	61
Chapter-6 Web Application Protocols and Browser Security	68
Chapter-7 Social Media and Its Security	82
Chapter-8 Digital Payments and Their Security	101
Chapter-9 Introduction to Online Frauds in Banking	115
Chapter-10 Introduction to Cyber Crime and Cyber Law	126

Unit 1
Fundamentals of Network and Operating Systems

Chapter-1

Introduction to Computer Networks, Its Types, and Benefits

Arjun, a system engineer for the city's emergency response unit, was responsible for maintaining seamless communication across interconnected systems. The city's infrastructure relied on a structured computer network, integrating LANs, MANs, and WANs to facilitate resource sharing, real-time coordination, and centralized management.

A severe storm disrupted power and conventional communication channels, critically impacting emergency operations. The failure of key networking devices—including routers and switches—led to bottlenecks in data transmission. Arjun quickly assessed the situation and deployed repeaters to extend the signal range, reinforced firewalls to safeguard sensitive transmissions, and optimized data flow using a mesh topology to ensure redundancy.

With wired networks interruption, emergency teams relied on wireless communication (WWAN) via satellite and cellular networks to maintain operational continuity. The strategic integration of full-duplex Ethernet enabled high-speed, bidirectional communication, mitigating delays in rescue coordination.

Following the crisis, the city implemented hybrid topologies for enhanced fault tolerance, integrating secure gateways to manage inter-network communication. Arjun's swift intervention reinforced a fundamental principle: a robust network is not merely an infrastructure—it is a critical component of disaster resilience.

Are you familiar with the terms mentioned above? Let's try to understand them one by one.

A computer network is a structured interconnection of multiple computing devices(computers) that enables resource sharing (printer, scanner, etc), data communication, and centralized management. These networks play a crucial role in modern computing by facilitating seamless device interaction across diverse geographical locations. At its core, a network consists of nodes (computers, servers, or mobile devices) and communication channels (wired or wireless media). These components function using standardized protocols (predefined rules and conventions) such as TCP/IP, facilitating reliable and error-free data transmission. A detailed discussion on TCP/IP will follow in the upcoming chapters; for now, it is essential to understand that TCP/IP serves as the standard protocol for data communication.

Networks vary in size, topology, and communication protocols. The Internet is the largest example, linking millions of systems worldwide. Essential components include:

- **Nodes:** Computing devices like computers, servers, and mobile devices.
- **Communication Medium:** Wired (Ethernet, fiber optics) or wireless (Wi-Fi, Bluetooth). Simply put, a wired cable in a network is a physical connection that helps transfer data between computers, routers, and other devices. It provides a stable and fast internet connection. Examples include Ethernet cables, fiber optic cables, and coaxial cables.
- **Protocols:** Standardized communication rules (e.g., TCP/IP, UDP, HTTP).
- **Networking Devices:** Switches, routers, firewalls, and modems ensure seamless connectivity and data transfer.

1.1 Types of Computer Networks

Computer networks are categorized based on their size, coverage area, and purpose. The major types include:

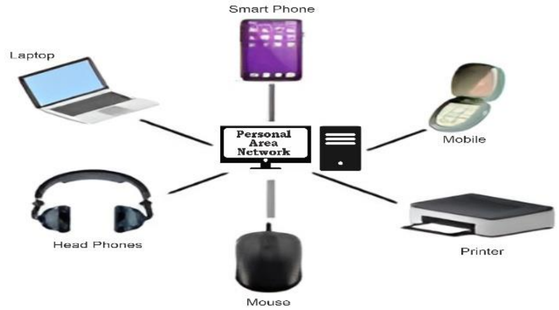
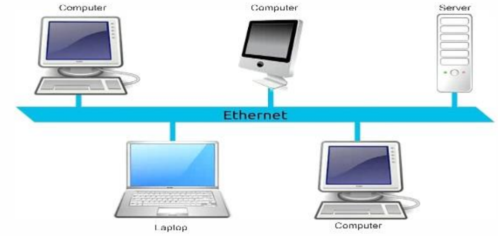
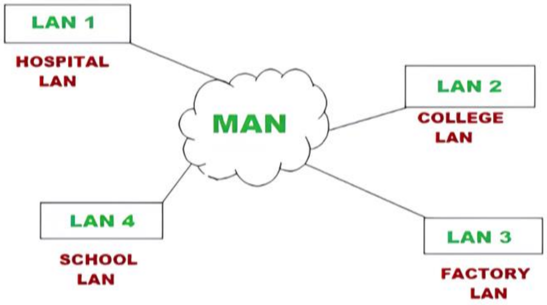
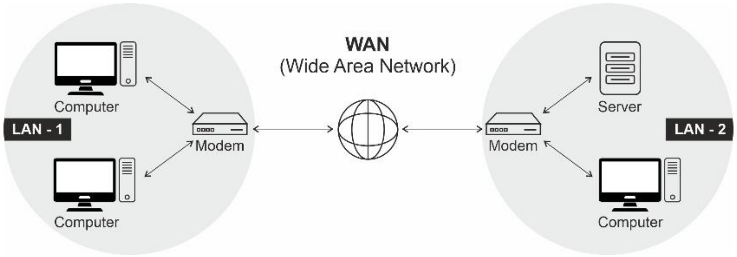
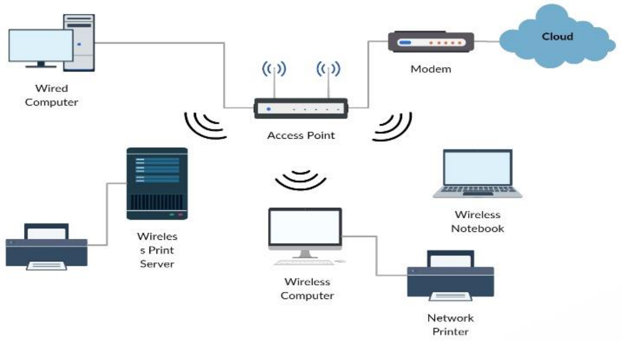
Personal Area Network ● **Personal Area Network (PAN):** Covers a very short range. The smallest network is used for personal devices like smartphones, smartwatches, and laptops (e.g., Bluetooth, infrared connections).	 Smart Phone Laptop Personal Area Network Mobile Head Phones Printer Mouse
Local Area Network (LAN): ● A high-speed network covering a small area, such as homes, offices, or schools. It uses Ethernet or Wi-Fi for communication.	 Computer Computer Server Ethernet Laptop Computer
Metropolitan Area Network ● **Metropolitan Area Network (MAN):** A network that connects multiple LANs within a city, often used by businesses, government agencies, or cable TV providers (e.g., cable TV networks).	 LAN 1 HOSPITAL LAN MAN LAN 2 COLLEGE LAN LAN 4 SCHOOL LAN LAN 3 FACTORY LAN
Wide Area Network ● **Wide Area Network (WAN):** A large-scale network covering vast distances, such as the Internet, which connects multiple cities or countries via leased lines, satellites, or fiber optics.	 WAN (Wide Area Network) Computer LAN - 1 Modem Computer Server LAN - 2 Modem Computer
Wireless Networks ● **Wireless Networks (WLAN, WWAN):** Supports mobility and remote communication (e.g., Wi-Fi, cellular networks).	 Wired Computer Modem Cloud Access Point Wireless Notebook Wireles s Print Server Wireless Computer Network Printer

Table 1.1: Types of Computer Networks

1.2 Benefits of Computer Networks

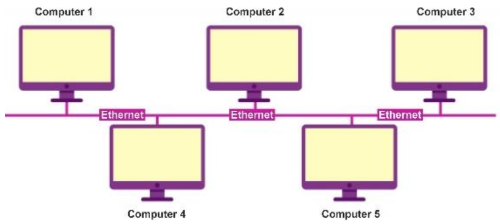
Some of the benefits of Computer Networks include:

1. **Efficient Resource Sharing:** Networks enable multiple users to access shared resources such as printers, storage devices, and applications, reducing redundancy and costs.
2. **Seamless Communication:** Facilitates real-time data exchange through emails, messaging, video conferencing, and VoIP services, improving collaboration.
3. **Centralized Data Management:** Ensures organized storage, easy retrieval, and secure backups, minimizing data loss and enhancing accessibility.
4. **Improved Security and Access Control:** Enables authentication mechanisms, firewalls, and encryption to regulate access and protect sensitive information.
5. **Scalability and Flexibility:** Supports the expansion of infrastructure, allowing new devices and users to integrate seamlessly without major modifications.
6. **Cost Efficiency:** Reduces hardware expenses and operational costs by utilizing centralized resources and cloud-based solutions.

1.3 Illustration of Topologies Used in Networking

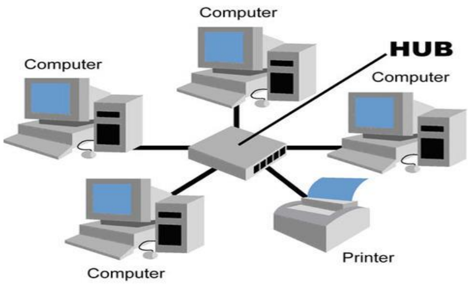
Network topology defines the structural layout of devices in a network. Common topologies include:

1. Bus Topology



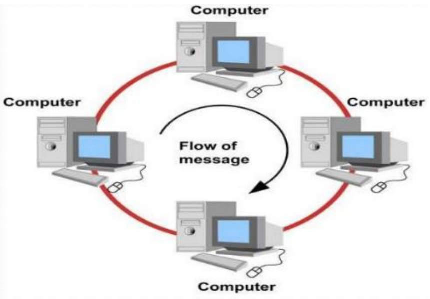
Bus topology is a simple and cost-effective network structure where all devices are connected to a single central cable, known as the backbone. This backbone serves as the main communication channel, allowing data to be transmitted in both directions. Each device (node) taps into this central cable to send and receive data. Bus topology is cost-effective and easy to install, making it suitable for small networks with minimal cabling. However, it has a single point of failure, limited scalability, and is prone to data collisions, which can degrade performance as more devices are added. This makes it less reliable for larger and high-traffic networks.

2. Star Topology:



Star topology is a widely used network structure where all devices are connected to a central hub or switch, which manages data transmission. It offers high reliability, as a failure in one device does not affect the entire network. However, it depends on the hub's functionality—if the hub fails, the entire network goes down. It is scalable, easy to manage, and commonly used in modern LANs.

3. Ring Topology:



Ring topology is a network structure where devices are connected in a circular manner, with data traveling in one or both directions. Each device acts as a repeater, forwarding data to the next node until it reaches its destination. It ensures efficient data transmission with minimal collisions but is vulnerable to failure if a single node malfunctions, unless a dual-ring or fault-tolerant mechanism is implemented.

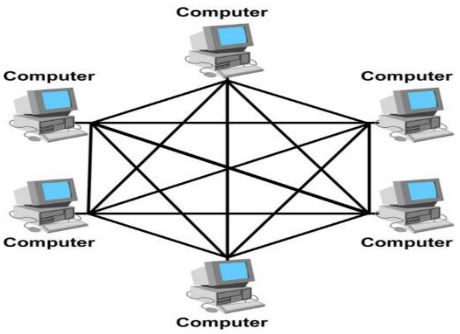
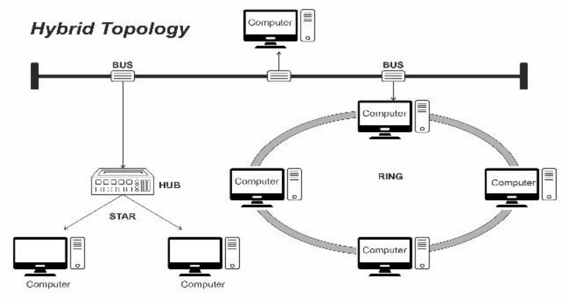
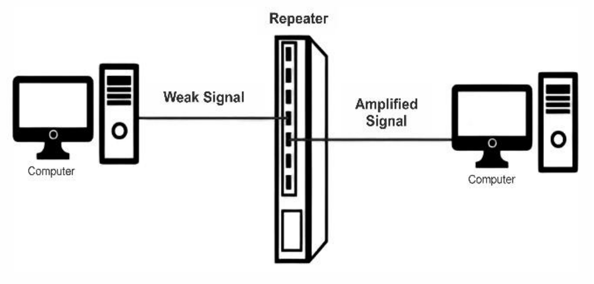
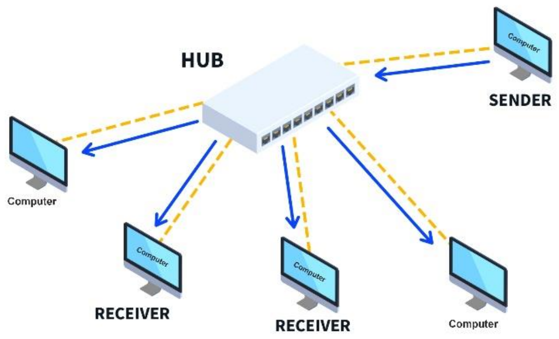
4. Mesh Topology: Mesh topology is a highly reliable network structure where each device is interconnected with every other device, ensuring multiple communication paths. This redundancy enhances fault tolerance, as data can take alternative routes if a connection fails. While it offers excellent reliability, security, and efficient data transmission, its complex setup and high cabling costs make it less practical for large-scale implementations.	 Computer Computer Computer Computer Computer Computer
5. Hybrid Topology: Hybrid topology is a combination of two or more network topologies, such as **star-bus, star-ring, or mesh-star**, designed to optimize performance, scalability, and fault tolerance. It inherits the strengths of individual topologies, offering flexibility and reliability, but can be complex and costly to implement due to increased cabling and configuration requirements, making it suitable for large-scale enterprise networks.	 Hybrid Topology Computer BUS BUS Computer HUB STAR RING Computer Computer Computer Computer Computer

Table 1.2: Topologies Used in Networking

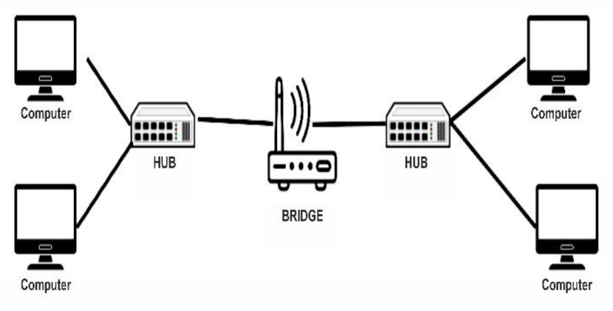
1.4 Networking Devices Overview

Several networking devices facilitate data transmission and communication:

Repeater A repeater is a network device that regenerates and amplifies signals to extend the range of data transmission. It is used in wired and wireless networks to prevent signal degradation over long distances. When data travels through a network, the signal weakens due to distance and interference. A repeater receives this weak signal, amplifies it, and retransmits it at full strength to the next segment of the network.	 Repeater Weak Signal Amplified Signal Computer Computer
Hub A hub is a basic networking device that connects multiple computers in a network and transmits data to all connected devices, regardless of the destination. It operates at the physical layer of the OSI model and does not filter or manage traffic. Hubs are cost-effective and simple, but lead to network congestion and collisions due to unnecessary data broadcasting. While once common in small networks, they are now largely replaced by more efficient switches, which offer better traffic management and performance.	 HUB SENDER Computer Computer RECEIVER Computer RECEIVER Computer Computer

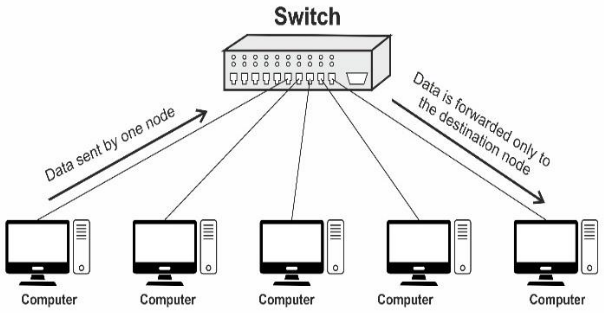
Bridge

A bridge is a networking device that connects and filters traffic between two or more LAN segments, improving network efficiency. It operates at the data link layer (Layer 2) and uses MAC addresses to forward or block data, reducing congestion. Bridges enhance performance by segmenting traffic, preventing unnecessary data flow. Unlike repeaters, they analyze data before forwarding. Commonly used in large networks, bridges help in network expansion while maintaining seamless communication and reducing collisions between connected segments.



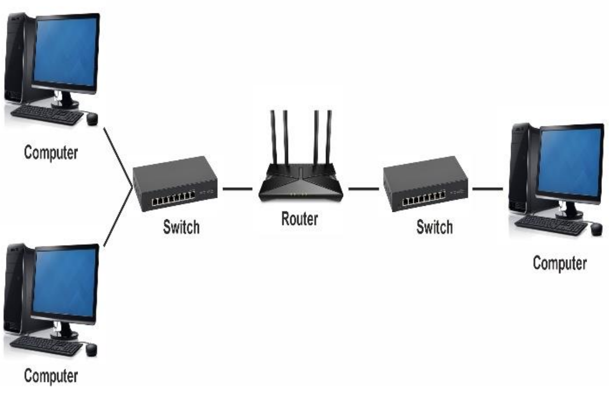
Switch

A switch is an intelligent networking device that connects multiple devices within a LAN and efficiently manages data traffic. It operates at the data link layer (Layer 2), using MAC addresses to forward data only to the intended recipient, reducing congestion. Unlike hubs, switches improve network performance by enabling simultaneous data transfers. Advanced switches also function at Layer 3 (network layer) for routing. They enhance speed, security, and scalability, making them essential for modern enterprise and home networks.



Router

A router is a networking device that directs data packets between different networks, enabling internet connectivity and efficient communication. It determines the best path for data transmission using IP addresses and routing protocols. Routers enhance security with firewalls, support multiple devices, and enable network segmentation. They connect LANs to WANs, ensuring seamless data flow. Unlike switches, routers operate at the network layer, making intelligent forwarding decisions. Essential for both home and enterprise networks, routers optimize performance, security, and scalability.



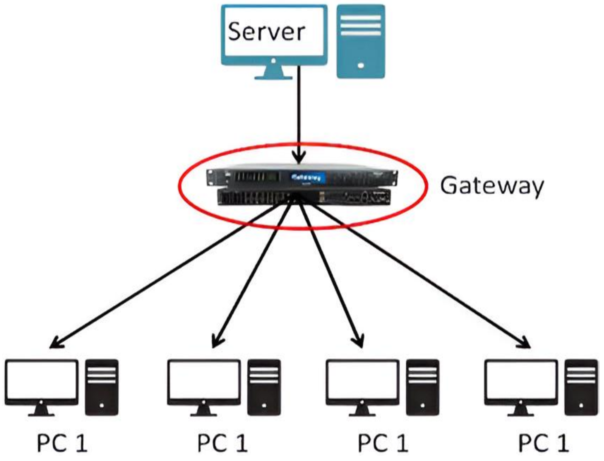
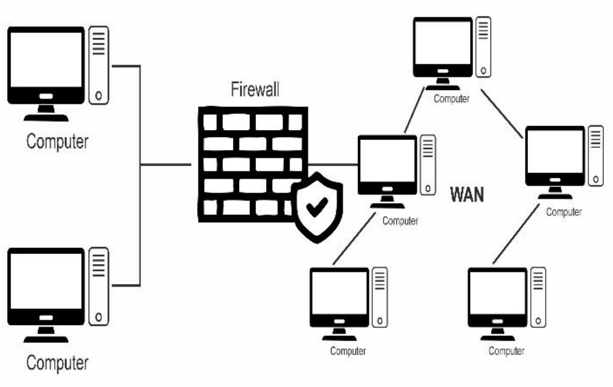
Gateway A gateway is a network device that connects different networks using different communication protocols, enabling seamless data transfer. It translates data formats, manages protocol conversions, and ensures compatibility between networks like LANs, WANs, or the Internet. Gateways operate at multiple layers, including network and application layers, and can function as firewalls, routers, or proxy servers. They are essential for secure, efficient cross-network communication, particularly in enterprise environments, cloud computing, and Internet-of-Things (IoT) applications.	
Firewall: A firewall is a security device or software that monitors and controls incoming and outgoing network traffic based on predefined rules. It acts as a barrier between trusted and untrusted networks, preventing unauthorized access and cyber threats. Firewalls can be hardware-based, software-based, or cloud-based, filtering data packets to block malware, hackers, and suspicious activities. They are essential for network security, ensuring data protection, privacy, and controlled access to sensitive resources in both personal and enterprise environments.	 Computer Computer Firewall Computer Computer WAN Computer Computer Computer

Table 1.3: Networking Devices Overview

1.5 Transmission Modes, Ethernet, and Transmission Media Classification

1.5.1 Transmission Modes: Transmission modes define how data flows between devices in a network.

Simplex:

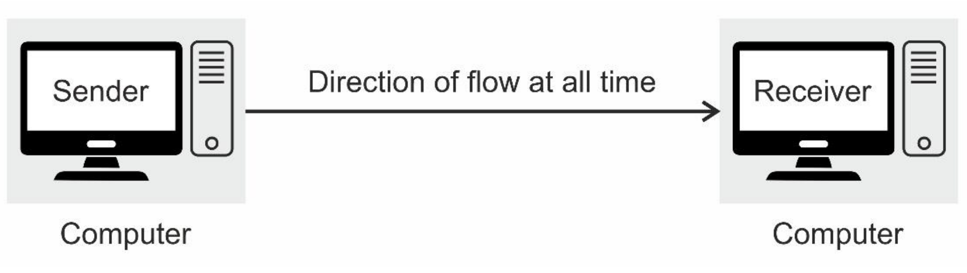


Fig: 1.1. Simplex

Half-Duplex:

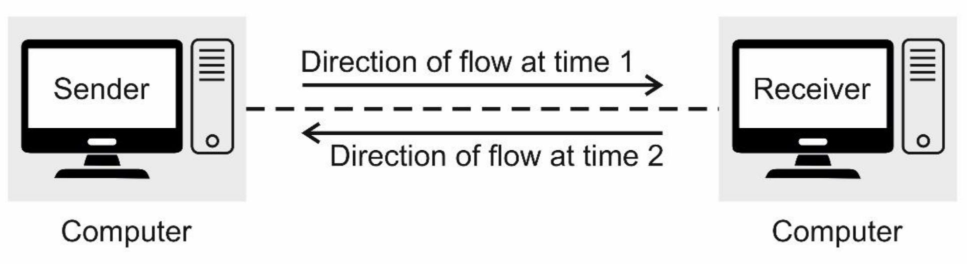


Fig: 1.2. Half-Duplex

Full-Duplex:

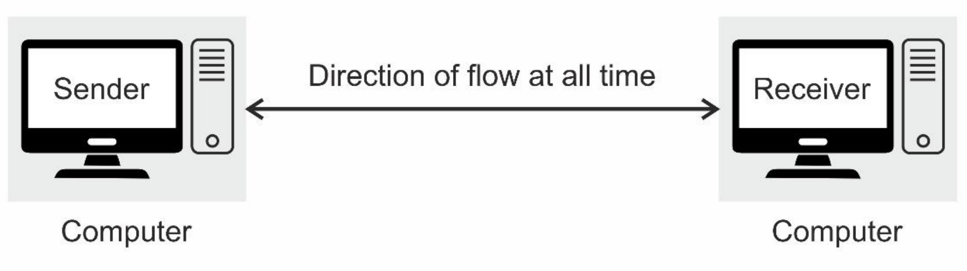


Fig: 1.3. Full-Duplex

- **Simplex:** Unidirectional communication (e.g., radio broadcasting). Simplex transmission is a one-way communication mode where data flows in a single direction without feedback or response. It is used in applications like radio broadcasting, TV transmission, and keyboard-to-monitor communication. While efficient for continuous data flow, it lacks two-way interaction, making it unsuitable for applications requiring real-time feedback or user response.

- **Half-Duplex:** Bidirectional but one at a time (e.g., walkie-talkies). Half-duplex communication allows data transmission in both directions but only one at a time. A device must wait for the other to finish before sending data. It is used in walkie-talkies, legacy Ethernet, and two-way radios, offering simple and efficient communication but with increased delays compared to full-duplex, where simultaneous transmission is possible.

- **Full-Duplex:** Full duplex is a communication mode where data flows in both directions simultaneously, allowing continuous two-way transmission without delays. This enhances efficiency and speed, commonly used in Ethernet, telecommunication, and modern networking devices. Unlike half duplex, it eliminates data collision, ensuring smoother communication in high-speed networks like fiber optics and full-duplex Wi-Fi systems.

1.5.2 Ethernet:

Ethernet is a widely used wired networking technology that enables high-speed data transfer within LANs. It manages data transmission and minimizes collisions. Ethernet supports various speeds, from 10 Mbps to 400 Gbps, using twisted-pair, fiber optic, or coaxial cables. Its reliability, scalability, and standardized protocols make it the backbone of modern wired networking, ensuring seamless and efficient communication across connected devices.

Fig: 1.4. Ethernet

Ethernet standards include:

- 10BASE-T (10 Mbps)
- 100BASE-TX (Fast Ethernet, 100 Mbps)
- 1000BASE-T (Gigabit Ethernet, 1 Gbps)

1.5.3 Transmission Media Classification:

- **Wired Media:** Includes twisted pair cables, coaxial cables, and fiber optics, offering reliable and high-speed data transfer.

Fig: 1.5. Wired Media

- **Wireless Media:** Includes radio waves, microwaves, and infrared, supporting flexible communication but susceptible to interference.

A thorough understanding of these concepts is essential for designing and maintaining efficient and scalable network infrastructures.

ASSESSMENT
Multiple Choice Questions

1. What is the primary function of a computer network?
   a) Running multiple operating systems
   b) Connecting devices for resource sharing and communication

c) Enhancing hardware performance
d) Increasing internet speed

2. Which of the following is NOT a type of computer network?
a) LAN
b) WAN
c) RAM
d) PAN

3. What is the standard protocol used for data communication in computer networks?
a) HTTP
b) UDP
c) TCP/IP
d) FTP

4. In a **bus topology**, all devices are connected to:
a) A central hub
b) A central switch
c) A single communication backbone
d) A mesh network

5. Which network topology offers **high fault tolerance** due to multiple paths between nodes?
a) Star topology
b) Bus topology
c) Mesh topology
d) Ring topology

6. What is the role of a **repeater** in a network?
a) Connecting different networks
b) Filtering traffic between network segments
c) Regenerating and amplifying signals to extend transmission distance
d) Assigning IP addresses to devices

7. Which device is responsible for directing data packets between different networks?
a) Switch
b) Hub
c) Router
d) Repeater

8. What is an advantage of **full-duplex transmission** over half-duplex transmission?
a) Data can flow in both directions simultaneously
b) It prevents network security threats
c) It requires fewer network resources
d) It is cheaper to implement

9. Which type of network typically covers a **city-wide area** and connects multiple LANs?
a) PAN
b) LAN
c) MAN
d) WAN

10. **Fiber optic cables** are classified under which type of transmission media?
a) Wired Media
b) Wireless Media

c) Optical Media
d) Magnetic Media

Fill-in-the-blanks

1. A computer network consists of _______ (such as computers and servers) and _______ (such as wired or wireless connections).
2. The main protocol used for reliable communication in networks is _______.
3. A _______ is a network type that covers a small geographical area like a home, office, or school.
4. In _______ topology, all devices are connected to a single communication backbone.
5. A switch operates at the _______ layer of the OSI model and forwards data to the intended recipient using MAC addresses.
6. _______ topology ensures multiple communication paths between devices, improving fault tolerance.
7. A _______ is used to regenerate and amplify weak signals in a network to extend data transmission over long distances.
8. The two types of transmission media are _______ (such as fiber optics) and _______ (such as Wi-Fi and Bluetooth).
9. A router uses _______ addresses to determine the best path for data transmission between networks.
10. A firewall is used to monitor and control _______ traffic, ensuring security and preventing unauthorized access.

True/False questions

1. A Local Area Network (LAN) typically spans multiple cities and countries.
2. In a Bus topology, if the main communication cable fails, the entire network stops functioning.
3. A repeater is used to block unauthorized access to a network.
4. A firewall can be implemented as both hardware and software for network security.
5. In a Full-Duplex transmission mode, data can be sent and received simultaneously.
6. The Internet is an example of a Wide Area Network (WAN).
7. Ethernet is a wireless networking technology used for long-distance communication.
8. A bridge is a networking device that connects two or more LAN segments and filters traffic.
9. A Hybrid topology is formed by combining different network topologies to optimize performance.
10. TCP/IP is an outdated protocol that is no longer used in modern networks.

Short-Answer Questions

1. What is the primary purpose of a computer network?
2. Name any two types of computer networks based on size.
3. What does TCP/IP stand for?
4. How does a repeater help in a network?
5. Mention one advantage and one disadvantage of the Bus topology.
6. What is the function of a firewall in a network?
7. Differentiate between Simplex and Full-Duplex transmission modes.
8. Why is Ethernet widely used in wired networks?
9. What is the role of a router in networking?
10. Which network topology connects all devices to a central hub?

Answer Key

Multiple Choice Questions

1. b, 2. c, 3. c, 4. c, 5. c, 6. c, 7. c, 8. a, 9. c, 10. a

Fill-in-the-blanks
1. devices, transmission media, 2. TCP, 3. LAN, 4. bus, 5. data link, 6. Mesh, 7. repeater, 8. wired, wireless, 9. IP, 10. network

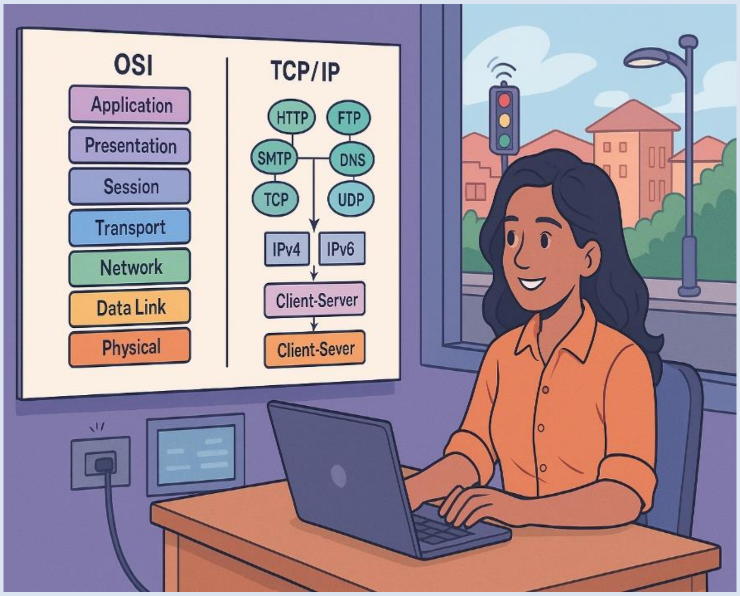
True/False questions
1. False, 2. True, 3. False, 4. True, 5. True, 6. True, 7. False, 8. True, 9. True, 10. False

Chapter-2

Networking Fundamentals and Protocol Models

In a smart coastal town named Nasik, a young network technician named Meera was newly appointed to the city's technology council. Her role was to upgrade the town's outdated communication systems to support upcoming smart initiatives like IoT-based traffic lights and automated water management systems.

On her first day, Meera started with the basics of networking, reviewing how data moves through networks using protocols and standardized models. Her mentor explained the importance of the OSI and TCP/IP models, which serve as blueprints for how devices communicate across vast and varied networks.



As Meera configured devices, she recalled the seven layers of the OSI model, each with a distinct role: The Physical layer for cabling and signals, Data Link layer for MAC addressing and switches, Network layer for routing through IP addresses, and Transport layer ensuring reliable data transmission through TCP or fast delivery with UDP. The Session, Presentation, and Application layers ensured user sessions were established, data was formatted, and applications like browsers or email clients worked seamlessly.

One day, during a town-wide firmware update, several IoT devices failed to sync. Meera traced the problem to mismatched protocol settings at the transport layer. She demonstrated how protocols like HTTP, FTP, SMTP, and DNS functioned within the TCP/IP stack, and reconfigured the devices to ensure each protocol communicated at its proper layer.

She also set up IP addressing schemes, distinguishing between IPv4 and IPv6, and configured DNS services to resolve domain names quickly. Her work with the client-server model helped devices request and receive data reliably, even under high load.

Meera implemented encapsulation and de-encapsulation to visualize how data packets are wrapped with protocol information at each layer and unwrapped at the receiving end. She emphasized the use of port numbers and the importance of ensuring secure and reliable communication using proper configurations.

By the month's end, Nasik had a robust and modern network infrastructure. Meera's deep understanding of networking fundamentals and protocol models had not only resolved technical issues but also educated her team about the layered approach of modern communication systems. She had proven that understanding the structure behind the scenes is key to building and maintaining a future-ready network.

Meera grasped these concepts—are you ready to explore some exciting ones yourself?

2.1 Introduction to OSI and TCP/IP Protocol Models

Communication between computer systems across networks is governed by a set of rules known as protocols. Two of the most prominent protocol models used in computer networking are the OSI Model and the TCP/IP Model.

2.1.1 Open Systems Interconnection (OSI) Model

The OSI model is a conceptual framework developed by the International Organization for Standardization (ISO). It standardizes the functions of a telecommunication or computing system into seven distinct layers, from physical transmission to application services:

1. **Physical Layer –** The Physical Layer is the first and lowest layer in the OSI model. This layer is responsible for the physical transmission of data over media. In simple words, one can think of it as the foundation of a building — everything else is built on top of it. It is responsible for physically sending data from one computer to another. This means turning digital data (1s and 0s) into signals that can travel through wires, fiber optic cables, or wireless (radio) waves. It defines the actual hardware components involved in data transfer, such as cables, connectors, hubs, and repeaters. One of its key roles is to manage the data transmission rate, ensuring that data is sent at a speed both devices can handle (e.g., 100 Mbps or 1 Gbps). The layer also handles synchronization, ensuring that the sender and receiver are properly timed to correctly interpret the signals. Additionally, it defines the network topology, which refers to how devices are physically connected (like star or bus layout), and the transmission mode, determining the direction of communication—whether it's one-way (simplex), two-way but one at a time (half-duplex), or two-way simultaneously (full-duplex). Overall, the Physical Layer forms the foundation of any network by enabling the actual movement of data in the form of signals.

2. **Data Link Layer** – The Data Link Layer is the second layer of the OSI model, sitting just above the Physical Layer. It is responsible for reliable data transfer between two directly connected devices on the same network. It takes raw bits from the Physical Layer and groups them into frames, adding important information like source and destination MAC addresses. One of its key roles is error detection and correction, ensuring that data is not corrupted during transmission. It also handles flow control to prevent a fast sender from overwhelming a slow receiver. The layer is divided into two sublayers: Logical Link Control (LLC), which manages communication and error handling, and Media Access Control (MAC), which controls how devices access the shared medium. Devices like network switches operate at this layer. In short, the Data Link Layer ensures that data is sent accurately and efficiently between devices on the same local network.

3. **Network Layer** – The Network Layer is the third layer of the OSI model. Its main job is to move data between different networks. It decides the best path for data to travel from the sender to the receiver, even if they are far apart. This process is called routing. The Network Layer also adds logical addresses, like IP addresses, to the data so that it knows where to go. It can break large data into smaller pieces if needed, and reassemble them at the destination. Common protocols used at this layer include IP (Internet Protocol) and ICMP (Internet Control Message Protocol).

4. **Transport Layer** – The Transport Layer is the fourth layer of the OSI model and is responsible for delivering data reliably from one computer to another. It ensures that messages are

complete, in order, and error-free. This layer breaks large messages into smaller pieces (called segments) and reassembles them at the destination. It also handles error checking and retransmission if data is lost. Two common protocols used here are TCP (which is reliable and connection-based) and UDP (which is faster but doesn't guarantee delivery). In simple terms, the Transport Layer acts like a delivery service that makes sure your data arrives correctly.

5. **Session Layer** – The Session Layer is the fifth layer of the OSI model. Its main job is to start, manage, and end communication sessions between two devices. Think of it like a coordinator that keeps track of who is talking to whom and when. It ensures that data from one application doesn't get mixed up with data from another. This layer also manages tasks like login sessions, session recovery if a connection is lost, and synchronization using checkpoints.

6. **Presentation Layer** – The Presentation Layer is the sixth layer of the OSI model. Its main job is to prepare data so that the Application Layer can understand it. It acts like a translator between different systems by converting data formats, such as from text to images or from one file format to another (e.g., .doc to .pdf). It also handles encryption and decryption for secure data transfer, and compression to reduce file sizes for faster transmission. In short, the Presentation Layer ensures that data sent from one computer is properly formatted, secure, and readable by the receiving computer.

7. **Application Layer** – The Application Layer is the top layer of the OSI model and is closest to the user. It provides the interface between the user and the network. This layer allows software applications to communicate over the network using services like email (SMTP), web browsing (HTTP/HTTPS), file transfer (FTP), and more. It does not perform the actual data transfer but prepares and presents the data in a way that other layers can use. It also manages things like user authentication and data formatting. In simple terms, the Application Layer makes network communication possible for programs we use every day.

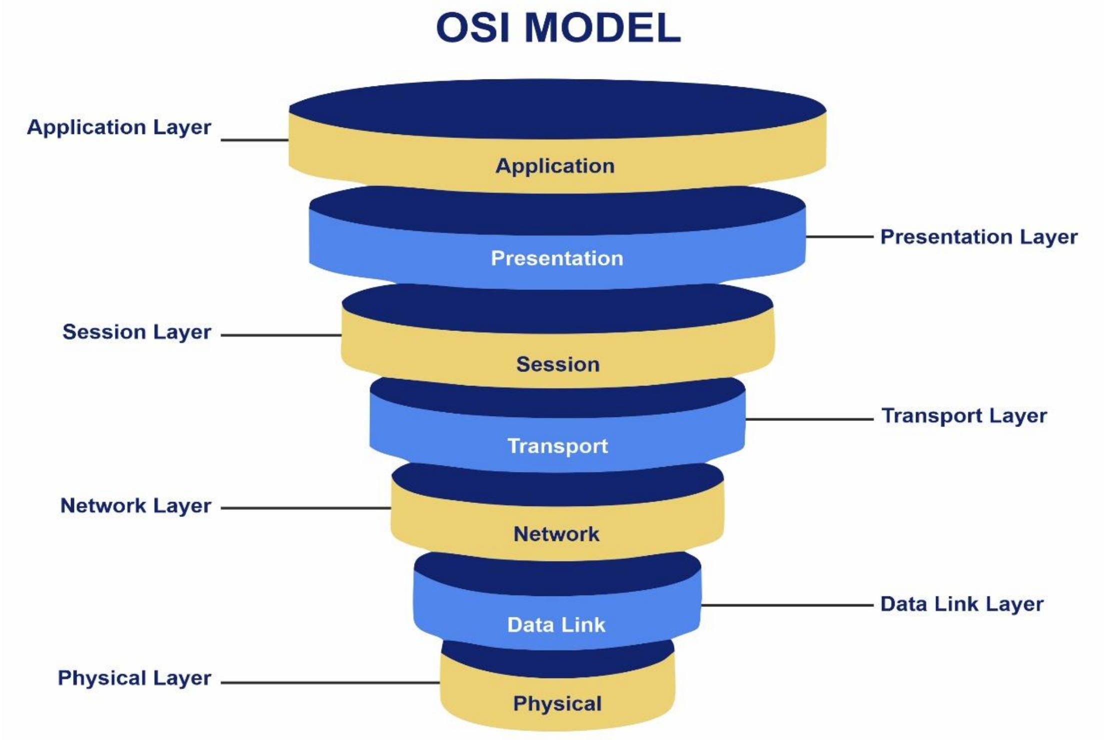


Fig: 2.1 Illustration of a OSI Model

2.1.2 TCP/IP Protocol Suite

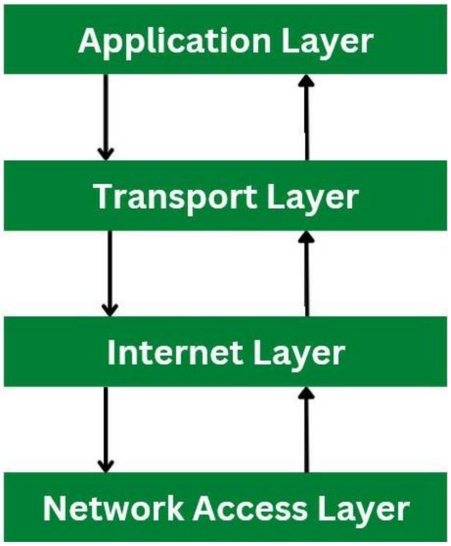


Fig: 2.2 Illustration of a TCP/IP MODEL

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is the foundational suite of protocols used in the Internet. It consists of **four layers**:

1. **Application Layer** – Combines the OSI application, presentation, and session layers (e.g., HTTP, SMTP, DNS).

2. **Transport Layer** – Offers end-to-end communication using protocols like TCP (reliable) and UDP (unreliable).

3. **Internet Layer** – Responsible for logical addressing and routing (e.g., IP, ICMP).

4. **Network Access Layer** – Combines the OSI data link and physical layers, dealing with hardware addressing and media transmission.

The TCP/IP model is more practical and widely adopted than the OSI model, especially in real-world Internet architecture.

2.2 Illustration of Port Numbers, Common TCP & UDP Ports

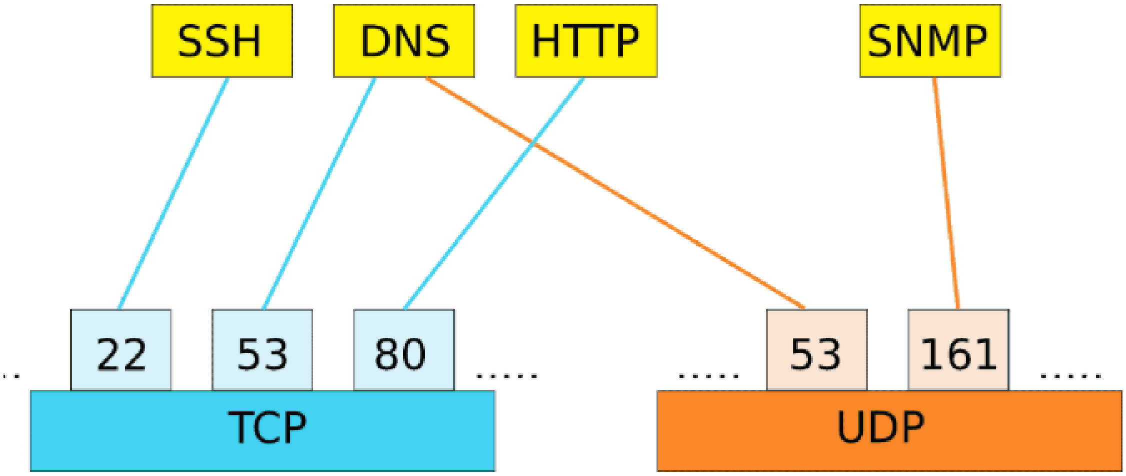


Fig: 2.3 Illustration of Port Numbers, Common TCP & UDP Ports

In TCP/IP networking, port numbers identify specific processes or network services on a host. They are part of the Transport Layer and help in multiplexing communication streams between applications.

- Port numbers range from 0 to 65535.
    - 0–1023: Well-known ports (reserved for common services)
    - 1024–49151: Registered ports
    - 49152–65535: Dynamic/private ports

Common TCP Ports/Common UDP Ports

Port Number	Protocol	Description
20, 21	FTP	File Transfer Protocol (Data, Control)
22	SSH	Secure Shell
23	Telnet	Remote Login (Insecure)
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System (also uses UDP)
80	HTTP	Web traffic (insecure)
110	POP3	Post Office Protocol (email)
143	IMAP	Internet Message Access Protocol
443	HTTPS	Secure HTTP
3389	RDP	Remote Desktop Protocol

Table 2.1: Common TCP Ports/Common UDP Ports

Each port acts as a communication endpoint for a specific process, allowing multiple network services to operate simultaneously on a single machine.

2.3 Introduction to RIR, Registries, and IANA

The assignment and management of IP addresses and autonomous system (AS) numbers are handled by global and regional organizations.

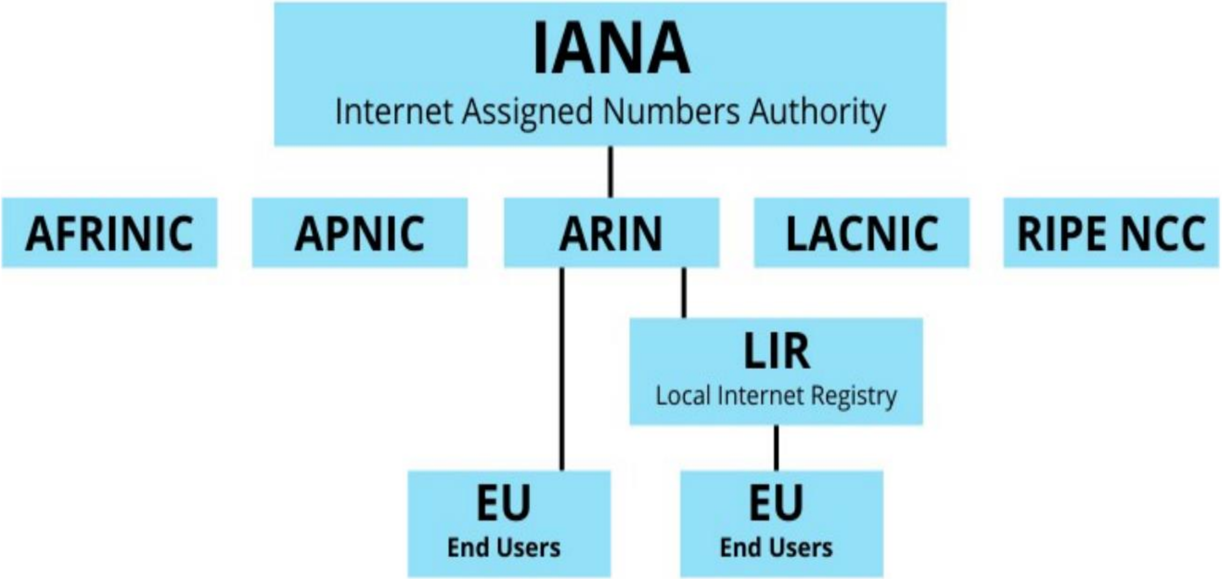


Fig: 2.4 Illustration of RIR, Registries, and IANA

2.3.1 IANA (Internet Assigned Numbers Authority)

IANA, under the oversight of ICANN (Internet Corporation for Assigned Names and Numbers), is responsible for:

- ***IP address space allocation**:* IP address space allocation means giving out IP addresses to devices so they can connect and communicate on a network or the internet. A global organization called IANA manages all IP addresses and gives big blocks to regional groups (RIRs). These groups then give smaller blocks to internet providers and companies. There are two main types of IP addresses: public (used on the internet) and private (used inside homes or offices). This system makes sure every device has a unique address and can send and receive data properly. It also helps organize and manage internet traffic efficiently.
- ***DNS root zone management:*** DNS root zone management is about controlling the top level of the Domain Name System (DNS), which helps convert website names (like www.google.com) into IP addresses (e.g., 192.168.1.1). At the very top of the DNS is the root zone. It contains the list of top-level domains (TLDs) like .com, .org, .net, and country codes like .in or .uk. The Internet Assigned Numbers Authority (IANA), managed by ICANN, is responsible for maintaining the root zone. They make sure that when someone types a website name, the DNS system knows where to start looking. In short, DNS root zone management keeps the "phonebook" of the internet's top-level addresses accurate and updated so the rest of the DNS system works smoothly.
- ***Protocol parameter assignment:*** Protocol parameter assignment involves assigning specific values to different aspects of internet communication to ensure devices can communicate effectively. This includes assigning port numbers for services (e.g., port 80 for HTTP), protocol numbers to distinguish between communication types (like TCP or UDP), and other standard values used in networking. Managed by organizations like IANA, this process ensures that global internet systems follow consistent rules, allowing devices and applications to work together seamlessly across the internet.

IANA delegates the distribution of IP address blocks to Regional Internet Registries (RIRs).

2.3.2 RIR (Regional Internet Registries)

RIRs manage, distribute, and register IP address allocations within specific global regions. There are five major RIRs:

RIR	Region Covered
ARIN	North America
RIPE NCC	Europe, the Middle East, and parts of Central Asia
APNIC	Asia-Pacific
LACNIC	Latin America and the Caribbean
AFRINIC	Africa

Table 2.2: Regional Internet Registries

These registries allocate address blocks to Internet Service Providers (ISPs), data centers, universities, and other organizations.

2.4 IP Addressing, Classes, and Addressing Scheme Overview

An **IP address** is a unique identifier assigned to each device connected to a network. There are two versions of IP addresses:

- **IPv4**: 32-bit address (e.g., 192.168.1.1). IPv4 (Internet Protocol version 4) is the most commonly used system for giving unique addresses to devices on a network, like computers, phones, or servers. It uses a set of four numbers separated by dots, like 192.168.0.1, and each number can be between 0 and 255. This address helps data know where to go when sent over the internet. IPv4 can support around 4.3 billion unique addresses, but as more devices connect, these addresses are running out. That's why a newer version called IPv6 is also being used. In simple terms, IPv4 works like a digital home address for your device.

- **IPv6**: 128-bit address (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv6 (Internet Protocol version 6) is the newer version of the IP address system used to identify devices on the Internet. It was created because the older system, IPv4, started running out of addresses. IPv6 uses longer addresses (like 2001:0db8:85a3:0000:0000:8a2e: 0370:7334), which means it can give more unique addresses, enough for every person and device in the world to have many. It is also more secure, faster in routing, and supports modern internet needs better than IPv4. In simple terms, IPv6 helps keep the internet running smoothly as more and more devices connect every day.

2.4.1 IP Address Classes (IPv4)

IPv4 addresses are divided into five classes based on the **first octet**:

Class	Range	Default Subnet Mask	Usage
A	1.0.0.0 – 126.0.0.0	255.0.0.0	Large networks
B	128.0.0.0 – 191.255.0.0	255.255.0.0	Medium-sized networks
C	192.0.0.0 – 223.255.255.0	255.255.255.0	Small networks
D	224.0.0.0 – 239.255.255.255	N/A	Multicasting
E	240.0.0.0 – 255.255.255.255	N/A	Experimental/Research

Table 2.3: IP Address Classes

Note: 127.0.0.0 is reserved for loopback testing (e.g., 127.0.0.1)

2.4.2 Basic IP Addressing Scheme

An IP addressing scheme is a way to give every device on a network its own special number, called an IP address, so it can send and receive information. Just like every house has a unique address, every computer or phone on the internet needs one too. This address has two parts, one that shows which network it's on, and one that shows which device it is. There are different groups called classes (like Class A, B, and C) based on the size of the network. Some IP addresses are used for the internet (public), and some are just for inside homes or schools (private). This system helps all devices talk to each other without confusion.

To determine the network and host portions, subnet masks are used. For example: Let's take an example of an IP address 10.0.5.22, which belongs to Class A. Class A IP addresses range from 1.0.0.0 to 126.0.0.0, and the default subnet mask for Class A is 255.0.0.0. With this subnet mask, the first part of the IP address (the first number, 10) represents the Network ID, while the rest (0.5.22) represents the Host ID. So, in this case, the Network ID is 10.0.0.0, and the Host ID is 0.5.22. This means that all devices with the same Network ID (10.0.0.0) belong to the same network, but each device has a unique Host ID to identify itself.

Proper IP addressing is critical for network design, routing, and communication between devices. Don't worry, if we find some concept that seems to be difficult this time. In higher studies, we will get deeper insights into these concepts.

Summary:

This chapter introduced the fundamental models and addressing mechanisms that govern modern networking. Understanding the OSI and TCP/IP layers helps in designing, troubleshooting, and securing networks. A clear grasp of port numbers, addressing schemes, and the role of organizations like IANA and RIRs is essential for managing and expanding network infrastructure.

Practical Activity 2.1

Objective:

To understand the concepts of the OSI and TCP/IP models, explore network commands (Netstat), learn about IANA and RIR, and practice IP configuration and troubleshooting using videos or simulators.

Tools & Platform Needed:

- Computer/Laptop with Windows/Linux OS
- Internet connection
- Access to simulation tools like Cisco Packet Tracer or videos
- Command-line terminal (CMD or Terminal)
- Access to educational videos on IANA, RIRs

Procedure:

Part 1: OSI & TCP/IP Models (Simulation/Video)

1. Watch a video or use a simulator to understand the 7 layers of the OSI model and 4 layers of the TCP/IP model.
2. Identify real-world protocols and devices working at each layer (e.g., HTTP at Application, IP at Network).
3. Create a small network in Cisco Packet Tracer (PCs, Switch, Router).
4. Simulate packet transfer between two PCs and observe how data passes through layers.

Part 2: Netstat Command

5. Open Command Prompt or Terminal.
6. Type netstat and observe all active connections.
7. Use netstat -a, netstat -n, and netstat -r to understand different outputs.
8. Interpret which ports and protocols are being used.

Part 3: IANA & RIR (Video Demonstration)

9. Watch a short video explaining IANA (Internet Assigned Numbers Authority) and RIRs (Regional Internet Registries).
10. Note how IP addresses and domains are managed regionally (e.g., APNIC, ARIN, RIPE NCC).

Part 4: IP Configuration & Troubleshooting

11. Use ipconfig (Windows) or ifconfig (Linux) to view your device's IP setup.
12. Use ping, tracert, and nslookup to test network connections.
13. Troubleshoot issues (e.g., no internet, incorrect gateway) and document your steps.

ASSESSMENT

Multiple Choice Questions

1. What is the main responsibility of the Physical Layer in the OSI model?
   a) Data formatting and encryption
   b) Ensuring reliable data transfer
   c) Physical transmission of data
   d) Routing data across networks

2. Which protocol is responsible for reliable, connection-based data transfer in the Transport Layer of the OSI model?
   a) UDP
   b) TCP
   c) IP
   d) DNS

3. Which layer in the OSI model is responsible for translating data formats and handling encryption?
   a) Session Layer

b) Application Layer
c) Presentation Layer
d) Transport Layer

4. In the TCP/IP model, which layer is responsible for routing and logical addressing?
a) Internet Layer
b) Transport Layer
c) Network Access Layer
d) Application Layer

5. What is the main role of port numbers in TCP/IP networking?
a) To identify the physical address of devices
b) To manage network traffic
c) To identify specific processes or network services
d) To allocate IP addresses

6. Which of the following is a common protocol used at the Transport Layer?
a) HTTP
b) DNS
c) TCP
d) FTP

7. What is IANA responsible for?
a) Assigning IP addresses to local networks
b) Managing domain names
c) IP address space allocation and DNS root zone management
d) Providing web browsing services

8. Which organization manages the distribution of IP address blocks to regional groups?
a) ICANN
b) RIR
c) IANA
d) DNS

9. Which class of IPv4 addresses is used for large networks?
a) Class B
b) Class A
c) Class C
d) Class D

10. In the IPv4 addressing scheme, which of the following addresses is reserved for loopback testing?
a) 127.0.0.0
b) 192.168.0.1
c) 10.0.0.1
d) 255.255.255.0

Fill in the blanks

1. The ________ layer in the OSI model is responsible for the transmission of raw data as electrical signals over physical media like cables and radio waves.
2. The ________ layer in the OSI model ensures reliable communication between two devices on the same network and adds error detection and correction mechanisms.
3. ________ (Transmission Control Protocol) is a protocol used in the ________ layer to provide reliable, connection-oriented data transfer.

4. The ________ layer in the OSI model is responsible for managing and controlling the dialog between two devices, such as establishing, maintaining, and terminating sessions.
5. The ________ layer is responsible for formatting and encrypting data for the application layer in the OSI model, and also for data compression.
6. The ________ layer in the TCP/IP model is responsible for routing data packets and logical addressing using IP addresses.
7. ________ (User Datagram Protocol) is a connectionless protocol used in the ________ layer of the TCP/IP model that does not guarantee the delivery of packets.
8. The range from ________ is reserved for ________ ports, which are used by essential network services like HTTP, FTP, and SSH.
9. The ________ (Internet Assigned Numbers Authority) manages the global distribution of ________ address blocks and ensures the proper operation of the DNS system.
10. ________ addresses in IPv4 range from ________ to ________ and are typically used for ________ networks.

True/False questions

1. The OSI model has 7 layers, while the TCP/IP model has only 4 layers.
2. UDP provides error recovery and ensures reliable data delivery, like TCP.
3. A MAC address is a physical address assigned to a device's network interface card (NIC).
4. The application layer of the OSI model is responsible for routing packets across networks.
5. HTTPS uses port 443 by default for secure communication over the web.
6. The data link layer adds both source and destination IP addresses to a packet.
7. In IPv4, the IP address 127.0.0.1 is commonly known as the loopback address.
8. DNS translates domain names into IP addresses.
9. Switches operate at the network layer of the OSI model.
10. FTP (File Transfer Protocol) is used to send emails.

Short-Answer Questions

1. What is the primary function of the DNS (Domain Name System) in networking?
2. Name the four layers of the TCP/IP model.
3. What is the purpose of using IP addresses in computer networks?
4. Which protocol is used to transfer files between computers over a network?
5. What is the difference between a switch and a hub?
6. Define MAC address and mention one characteristic that makes it unique.
7. Which port number is typically used for HTTP?
8. Why is the 127.0.0.1 IP address important?
9. Name one protocol used at the application layer of the OSI model.
10. What is the key difference between TCP and UDP?

Answer Key

Multiple Choice Questions

1. c, 2. b, 3. c, 4. a, 5. c, 6. c, 7. c, 8. b, 9. b, 10. a

Fill-in-the-blanks

1. Physical, 2. Data Link, 3. TCP, Transport, 4. Session, 5. Presentation, 6. Internet, 7. UDP, Transport, 8. 0 to 1023, well-known, 9. IANA, IP, 10. Private, 10.0.0.0, 10.255.255.255, internal

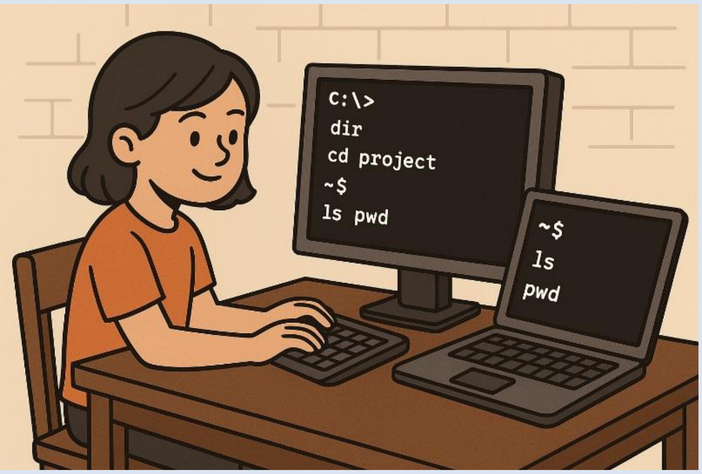
True/False questions

1. True, 2. False, 3. True, 4. False, 5. True, 6. False, 7. True, 8. True, 9. False, 10. False

Chapter-3

Introduction to Windows/Linux OS and its File System

Riya was working on a school project when her computer suddenly stopped responding. Curious and calm, she restarted it and saw a black screen with a blinking cursor. Instead of panicking, she remembered that her teacher once showed her the command line utility.



```
C:\>
dir
cd project
~$
ls pwd
```

```
~$
ls
pwd
```

She typed a few basic commands in Windows, like dir to see the files and cd to open her project folder. On her brother's Linux laptop, she used ls and pwd to check files and paths. Riya realized that both systems had different ways to organize files, but they both followed a structure called a file system. Thanks to her curiosity and the command line, she fixed the issue and saved her project.

Her friends were amazed and wanted to learn the magic too!

Introduction to Windows and Linux Operating Systems

An Operating System (OS) is system software that acts as an interface between the user and the computer hardware. It manages system resources and allows users to interact with the machine easily.

- **Windows OS**

  Windows is a type of software called an Operating System (OS). It helps you use your computer by showing everything on the screen in a simple and easy way using icons, folders, buttons, and menus.

Think of Windows as the manager of your computer. It helps you:

- Open and use apps like Paint, Word, or games
- Save your files and folders
- Connect to the internet
- Play music and videos
- Use a mouse and keyboard easily

It's called Windows because it shows different programs and files in boxes called "windows" on the screen. Example: When you turn on your computer and see the desktop with icons, and click on the Start button to open things—that's all part of Windows!

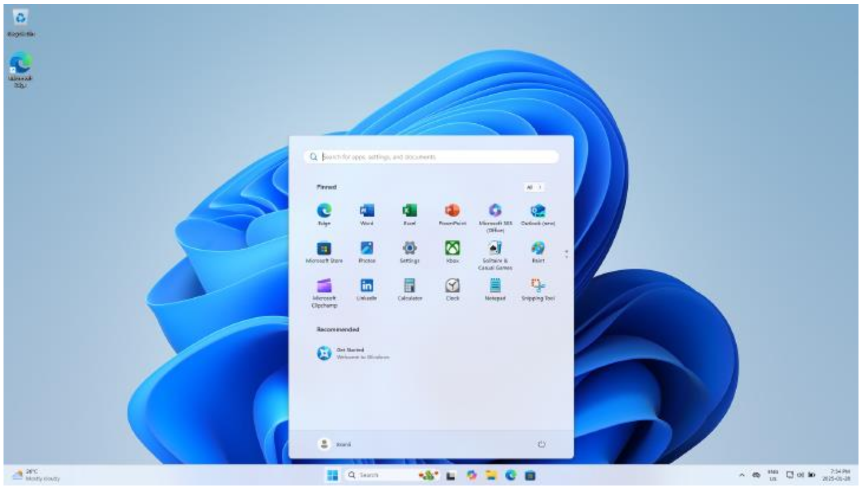


Fig: 3.1 Windows Operating System (OS)

- **Linux OS**
  Linux is also a type of Operating System (OS) like Windows, but it works a bit differently. It helps the computer run apps, manage files, and connect to the internet.

What makes Linux special is that:

- It is free to use, and anyone can change or improve it.
- It is used mostly in servers, school labs, tech companies, and even in mobile phones (like Android).
- It is very safe and secure from viruses.

Linux often uses a command line (text-based screen) to give instructions, but many versions also have desktops with icons and menus, just like Windows. Example: If you have ever seen someone using Ubuntu, Kali Linux, or Linux Mint, they are using a version of the Linux OS.

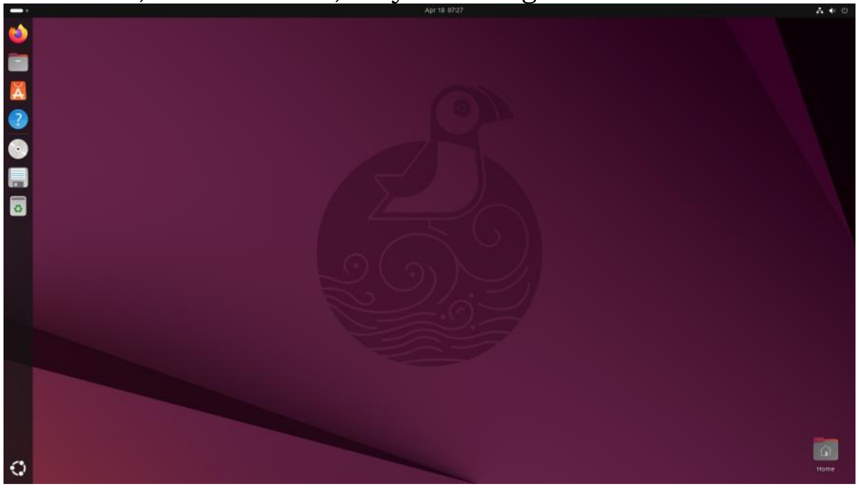


Fig: 3.2 Linux operating system

3.1 Windows vs Linux – A Simple Comparison

Table: Comparison

Feature	**Windows**	**Linux**
Cost	Paid (comes with a license)	Free and open-source

User Interface	Easy, graphical with icons and menus	Also graphical, but often uses commands too
Usage	Used mostly in homes, offices, and schools	Used in servers, coding, and tech systems
Security	More likely to get viruses	Very secure, fewer viruses
Customization	Less customizable	Highly customizable by users
File System	Uses NTFS, FAT32	Uses ext3, ext4
Example Versions	Windows 10, Windows 11	Ubuntu, Fedora, Kali Linux

Table 3.1: Comparison table of Windows vs Linux

3.2 File System in Windows and Linux

3.2.1 Windows File System

Imagine your computer is like a big library, and the Windows File System is the way this library is organized, so you can easily find, store, and manage all your files.

- The computer has drives like C:, D:, or E: – think of them like bookshelves.
- Each drive contains folders (like drawers), and inside those folders, you keep your files (like papers).
- **Folders** = Boxes to keep things organized
  Files = Your documents, photos, videos, etc.
-

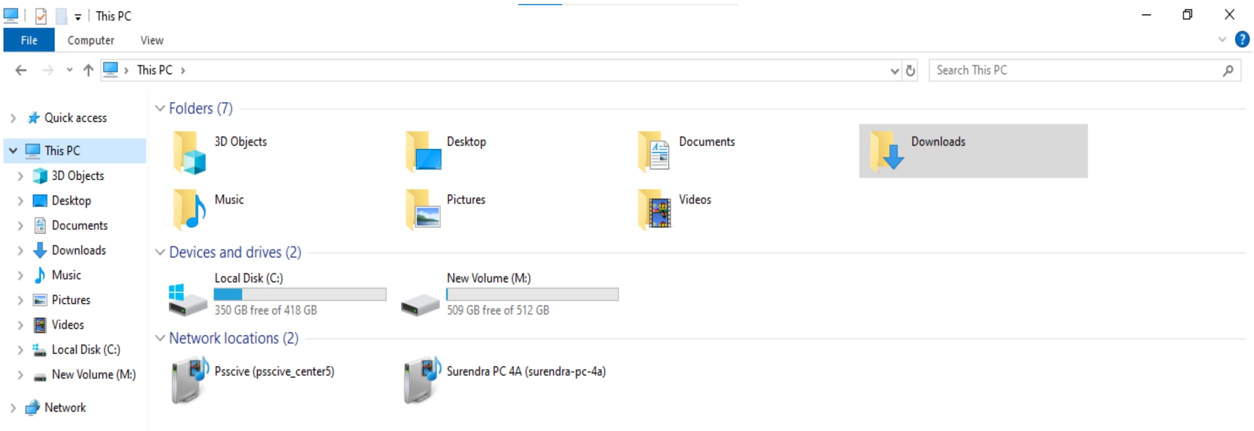


Fig: 3.3 File system in the window operating system

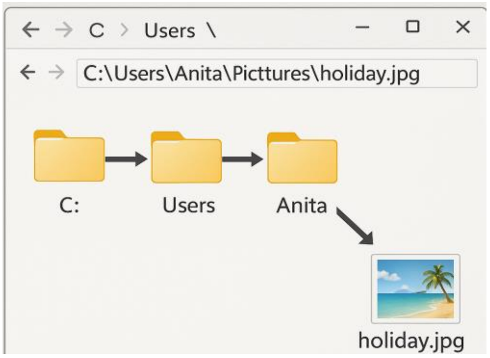


Fig. 3.4 File system

Example:
C:\Users\Anita\Pictures\holiday.jpg
This means:
→ Go to C drive → Open 'Users' folder → Open 'Anita' → Then 'Pictures' → Find the file holiday.jpg

3.2.2 Types of Windows File Systems

FAT32 and NTFS are two types of file systems used by Windows to store and organize files. FAT32 is older and works well for USB drives and memory cards, but it has a limit—it can't store files bigger than 4GB. NTFS is newer and more powerful. It is used by most computers today because it can handle large files, keeps data more secure, and allows you to set permissions (like who can open or change a file). NTFS is better for hard drives, while FAT32 is still useful for portable devices.

3.2.3 Important Features of Windows File System

Feature	**Simple Meaning**
Drives	Like shelves (C:, D:) to keep files
Folders	Used to group files (like school folders for subjects)
Extensions	Tell what kind of file it is (.jpg, .mp4, .docx)
Hidden Files	Files you don't see unless you ask Windows to show them
Recycle Bin	Temporary place for deleted files (you can restore them)
File Permissions	Control who can open/edit/delete a file (in NTFS)

3.2.3 Why File System Important?

- Keeps everything organized
- Helps Windows find and open files quickly
- Protects your data from getting lost or damaged

3.2.4 Linux File System

The Linux file system is like a big tree where everything is stored in folders (called directories). At the top is the root folder, written as "/", and all other folders grow from it, just like branches. Some important folders are as follows:

- /home – where users keep their files (like Documents or Pictures).
- /bin – has programs and commands that the system uses.
- /etc – stores settings and system files.
- /dev – has files for devices like your mouse or keyboard.
- /tmp – a place for temporary files that are deleted automatically.

In Linux, everything is treated as a file—even folders and connected devices!

3.3 Overview of Command Line Utility

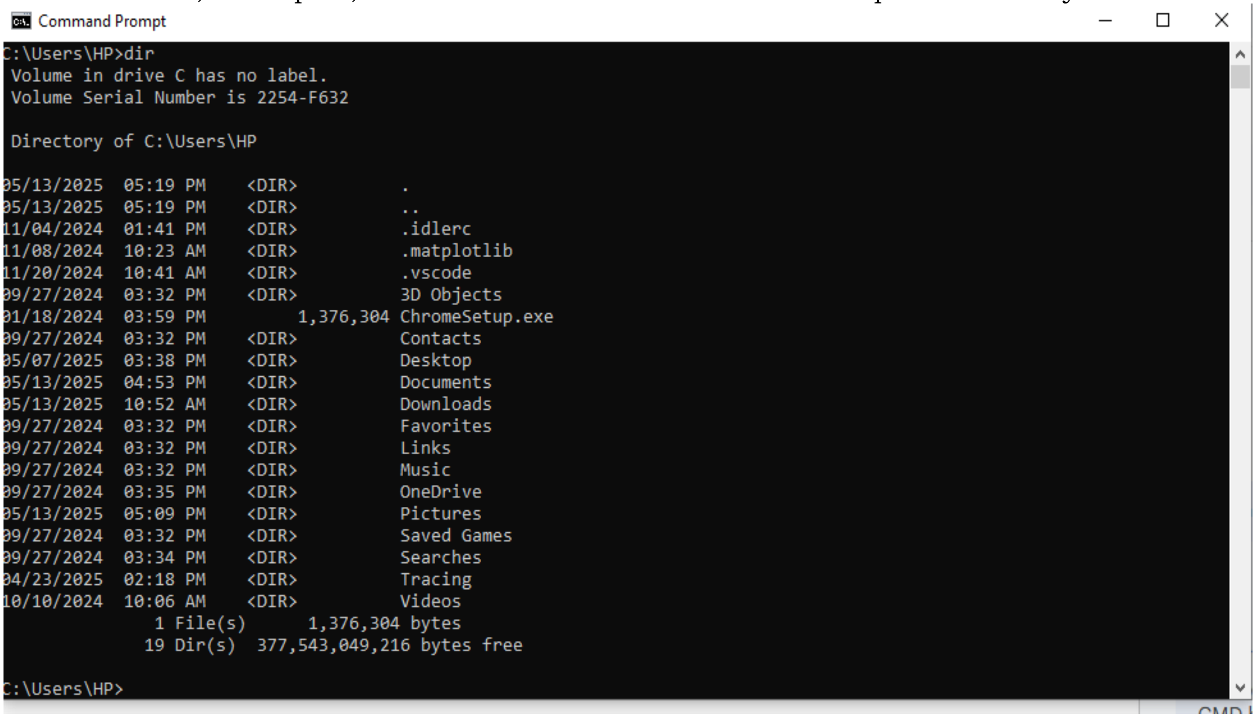
A command-line utility is a tool that lets you talk to the computer by typing commands instead of clicking with a mouse. It's like giving instructions using text. This is also called the command line interface (CLI).
Here's what we should know:

- In Windows, the command line tool is called Command Prompt (cmd) or PowerShell.
- In Linux, the tool is called Terminal or Shell.

With the command line, you can:

- Open files and folders
- Copy or delete files
- Install or run programs
- Check your system information
- And much more — all just by typing!

It might look like a black screen with white text, but it's a powerful tool used by system administrators, developers, and advanced users to control the computer efficiently.



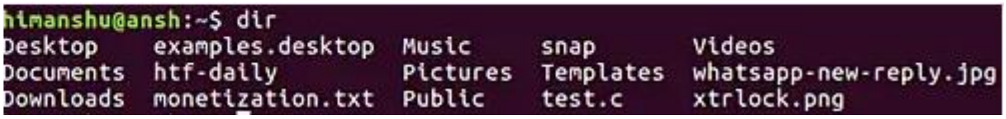
```
:\Users\HP>dir
 Volume in drive C has no label.
 Volume Serial Number is 2254-F632

 Directory of C:\Users\HP

05/13/2025  05:19 PM    <DIR>          .
05/13/2025  05:19 PM    <DIR>          ..
11/04/2024  01:41 PM    <DIR>          .idlerc
11/08/2024  10:23 AM    <DIR>          .matplotlib
11/20/2024  10:41 AM    <DIR>          .vscode
09/27/2024  03:32 PM    <DIR>          3D Objects
01/18/2024  03:59 PM         1,376,304 ChromeSetup.exe
09/27/2024  03:32 PM    <DIR>          Contacts
05/07/2025  03:38 PM    <DIR>          Desktop
05/13/2025  04:53 PM    <DIR>          Documents
05/13/2025  10:52 AM    <DIR>          Downloads
09/27/2024  03:32 PM    <DIR>          Favorites
09/27/2024  03:32 PM    <DIR>          Links
09/27/2024  03:32 PM    <DIR>          Music
09/27/2024  03:35 PM    <DIR>          OneDrive
05/13/2025  05:09 PM    <DIR>          Pictures
09/27/2024  03:32 PM    <DIR>          Saved Games
09/27/2024  03:34 PM    <DIR>          Searches
04/23/2025  02:18 PM    <DIR>          Tracing
10/10/2024  10:06 AM    <DIR>          Videos
               1 File(s)      1,376,304 bytes
              19 Dir(s)  377,543,049,216 bytes free

:\Users\HP>
```

Fig: 3.5 Command Prompt in Windows



```
himanshu@ansh:~$ dir
Desktop    examples.desktop  Music     snap       Videos
Documents  htf-daily         Pictures  Templates  whatsapp-new-reply.jpg
Downloads  monetization.txt  Public    test.c     xtrlock.png
```

Fig: 3.6 Command Prompt in Linux

3.3.2 Basic Commands in Windows and Linux

Basic Windows Commands

Command	**What it Does**	**Example**
dir	Shows files and folders in the current folder	dir
cd	Changes the current folder	cd Documents
mkdir	Makes a new folder	mkdir SchoolWork
del	Deletes a file	del notes.txt
copy	Copy a file	copy notes.txt D:\backup
cls	Clears the screen	cls
exit	Closes the command prompt	exit

Table 3.2: Basic Commands in Windows

Basic Linux Commands

Command	What it Does	Example
ls	Lists files and folders	ls
cd	Changes directory	cd /home/user/Documents
mkdir	Creates a new folder	mkdir Homework
rm	Removes a file	rm oldfile.txt
cp	Copy a file or folder	cp file.txt /home/user/
clear	Clears the terminal screen	clear
exit	Exits the terminal	exit

Table 3.3: Basic Commands in Linux

Summary

- Windows and Linux are two different types of operating systems, each with unique file systems.
- The Command Line Interface (CLI) is a powerful tool for managing files and directories efficiently.
- Knowing basic commands helps you control the system without relying on the graphical interface.

Practical Activity 3.1

Objective:
Learners will demonstrate their understanding of file systems, file permissions, and common file management operations on both Windows and Linux.

Tools & Platform Needed:

- Smartphone/computer with internet access
- Windows or Linux operating system
- Terminal (Linux) or Command Prompt (Windows)

Procedure:
Step 1: Form Groups (3–4 students)
Encourage collaboration by forming small groups, which will help each member understand the topics through discussion and sharing insights.

Step 2: Assign Tasks (Choose from the following)

1. **Demonstration of File Systems (Windows / Linux)**
   - Windows: Navigate through the file system using File Explorer. Locate different file types (e.g., .txt, .exe, .jpg) and determine their default file associations.
   - Linux: Open the terminal and navigate through the file system using commands like ls, cd, pwd, and explore directories like /home, /etc, /usr.

2. **Configuring Permissions (Read, Write, and Execute)**
   - Windows: Modify permissions on a file/folder through the **Properties > Security** tab. Demonstrate how to assign read, write, and execute permissions to different users or groups.
   - Linux: Use ls -l to display file permissions and chmod to change file permissions. Perform the following tasks:
     - Allow the user to write to a file.
     - Remove the execute permission from a file.
     - Add execute permission for the owner using chmod.

3. **Using the sudo Command & Working with Hard/Soft Links (Linux)**
   - Linux: Demonstrate how to use sudo for administrative tasks (e.g., sudo apt update).
   - Show the creation of hard and soft (symbolic) links using commands like ln and ln -s.

Step 3: Complete the Activity Tasks

- **Windows Users**: Show examples of changing file permissions and navigating the file system.
- **Linux Users**: Create hard and soft links, change file permissions using chmod, and execute sudo commands.

Step 4: Note Key Learning Points:

- **File System (Windows/Linux)**: How directories and files are structured in both Windows and Linux.
- **File Permissions**: The importance of setting the correct file permissions to protect sensitive data.
- **Sudo Command**: How sudo enhances security by allowing users to perform administrative tasks with elevated privileges.
- **Hard and Soft Links**: The difference between hard links (same inode) and soft links (symbolic links).

Step 5: Group Presentations

- Each group will present 3 main takeaways from the practical activity.
- Share screenshots showing:
  - Navigating the file system.
  - Configuring file permissions.
  - Using the sudo command.
  - Creating hard and soft links.

Step 6: Submit a Summary

Each group will submit a summary (approx. 200-300 words) discussing how these activities improve understanding of file management and security practices. The summary should include:

- Key learning points.
- Practical applications in real-life scenarios (e.g., managing file permissions on personal computers, using sudo for system updates).

How does this activity enhance personal or digital information safety.

ASSESSMENT

Multiple Choice Questions

1. Which of the following is a file system used by Windows?
A. ext4
B. FAT32
C. NTFS
D. Both B and C

2. What does the command dir do in the Windows Command Line?
A. Deletes files
B. Displays the current directory path
C. Lists files and folders
D. Changes directory

3. Which command is used to list files in a Linux directory?
A. list
B. ls
C. dir
D. show

4. In Linux, what does the command pwd show?
A. Password
B. Print working directory
C. Present working data
D. Protected window

5. Which of the following is not a Linux command?
A. cd
B. mkdir
C. copy
D. rm

6. The NTFS file system supports which of the following features?
A. File compression
B. File encryption
C. Large file support
D. All of the above

7. What is the full form of FAT in FAT32?
A. File Allocation Table
B. Fast Access Technology
C. File Architecture Tool
D. None of the above

8. What is the key difference between Windows and Linux?
A. Windows is open-source
B. Linux is closed-source
C. Windows uses GUI by default, Linux often uses CLI
D. Both use the same file system.

9. Which command is used to create a new folder in Windows?
A. mkdir
B. newfolder
C. mkfolder
D. createdir

10. Which of these is an advantage of using the command line?
A. Slower operation
B. Less control over the system
C. Faster for advanced users
D. Requires high-end graphics

Fill in the Blanks

1. The full form of NTFS is _______________.
2. In Windows, the command to create a new directory is _______________.
3. The Linux command to remove a file is _______________.
4. In Linux, the command pwd stands for _______________.
5. FAT32 stands for _______________.
6. The command line utility in Windows is called _______________.

7. A Linux file system that is widely used is called _______________.
8. In Windows, _______________ command lists files and directories.
9. The file system used by default in most Linux distributions is _______________.
10. The command to clear the screen in Windows CLI is _______________.

True or False

1. NTFS allows file encryption and compression.
2. FAT32 supports very large files over 4GB.
3. The Linux command ls is used to list directory contents.
4. The command cd is used to create a directory.
5. Windows and Linux use the same file systems.
6. Linux is commonly used through a graphical interface only.
7. The rm command deletes files in Linux.
8. cls is used to clear the screen in Windows CMD.
9. mkdir works in both Windows and Linux for making directories.
10. cp is the Linux command for copying files.

Answer Key

Multiple Choice Questions

1. D, 2. C, 3. B, 4. B, 5. C, 6. D, 7. A, 8. C, 9. A, 10. C

Fill-in-the-blanks

1. New Technology File System, 2. mkdir, 3. rm, 4. Print Working Directory, 5. File Allocation Table 32, 6. Command Prompt, 7. ext4, 8. dir, 9. ext4, 10. cls

True/False questions

1. True, 2. False, 3. True, 4. False, 5. False, 6. False, 7. True, 8. True, 9. True, 10. True

Unit 2

Fundamentals of Cyber Security

Chapter-1

Introduction to Information Security

Riya and the Cyber Trap

Riya was a smart student who loved using her laptop to study and play games. One day, she received an email saying she had won a new smartphone. Excited, she clicked the link and entered her personal details. Soon after, strange things started happening—her social media account was hacked, and her photos were leaked.

Her teacher, Mr. Verma, explained that Riya had become a victim of phishing and identity theft. He taught her about the CIA Triad—Confidentiality, Integrity, and Availability—and how to stay safe online. Riya learned to use strong passwords, install antivirus software, and never click unknown links again.

Let’s we all learn these interesting concepts.

Information security is all about protecting important data from being accessed, changed, or destroyed by unauthorized people. It’s like locking up your things in a safe place to keep them secure and private. In the digital world, this means securing your computer, mobile phone, and any other device that holds personal information.

Information security ensures that our digital information remains confidential, intact, and available only to those who are authorized to access it. This is important because today, many things we do are online, like shopping, social media, and banking. If our information is not secure, hackers or cybercriminals could steal it and cause harm.

1.1 Key Terms in Information Security

- **Data**: Information that is stored in a computer or online. It could be anything — your name, photos, passwords, or messages.
- **Cybersecurity**: The practice of protecting computers, networks, and data from unauthorized access, attacks, or damage.
- **Hacker**: A person who tries to break into computer systems without permission, usually to steal or damage data.
- **Firewall**: A software or hardware tool that blocks unwanted access to your computer or network, like a security guard at a gate.

- **Antivirus**: A program that scans your computer to find and remove harmful software like viruses.
- **Malware**: Short for "malicious software", this is harmful software like viruses, worms, or spyware that can damage or steal your data. Think of it like a virus that makes your computer sick — it can delete files, slow things down, or send your data to someone else.
- **Phishing**: A trick where hackers send fake emails or messages to steal your personal information, like passwords or bank details.
- **Password**: A secret word or code used to access a computer, app, or account. A strong password helps keep your data safe.
- **Encryption**: A way of turning data into a secret code so that only the right person can read it, like writing a message in a secret language.
- **User Authentication**: A way to check if someone is allowed to access a system, usually done using usernames and passwords.
- **Spyware**: Software that secretly watches what you do on your computer and sends that information to someone else.
- **Virus**: A harmful program that spreads from one computer to another and can damage files or slow down the system.
- **Backup**: A copy of your data saved somewhere safe (like a USB or cloud) so you don't lose it if something goes wrong.
- **Access Control**: A way to limit who can see or use data or devices. Only certain people get permission.
- **Two-Factor Authentication (2FA)**: A security method that asks for two things before letting you in, like a password *and* a code sent to your phone.

1.2 Why is Information Security Important?

Information security is important because we rely heavily on data and technology in our daily lives. Whether it's keeping personal details safe or ensuring that online services function correctly, protecting information helps prevent problems like:

- **Data theft**: When hackers steal personal or financial data.
- **Identity theft**: When someone impersonates you using your private information. In simple words, Identity theft is when someone steals your personal information, like your name, address, Aadhaar number, or bank details, and pretends to be you. They might use this information to open bank accounts, take loans, or buy things in your name without your knowledge. It's like someone wearing a mask to act like you and misuse your identity.
- **Cyberattacks**: Malicious actions that try to damage or steal information from computers and networks.

So, securing information helps avoid these risks and ensures that we can trust the systems and devices we use every day.

1.3 The CIA Triad: The Three Pillars of Information Security

One of the key concepts in information security is the CIA Triad. It stands for Confidentiality, Integrity, and Availability. These three principles are the foundation of protecting data in any system or organization.

1. **Confidentiality:** This means keeping information private. Only authorized people should have access to certain data. For example, your password, bank details, and personal messages should be kept confidential. Think of it as locking up your diary in a secret place so no one else can read it.
2. **Integrity:** This means making sure the data is accurate and not tampered with. If someone changes or corrupts the data, it can cause problems, like a wrong bank balance or a lost assignment. Integrity ensures that the data stays correct and reliable over time.
3. **Availability:** This means making sure the information is accessible to authorized people when they need it. For example, when you want to access your email or social media accounts, you should be able to do so without delays or system crashes. Availability ensures that the information and systems are always running and accessible to those who need them.

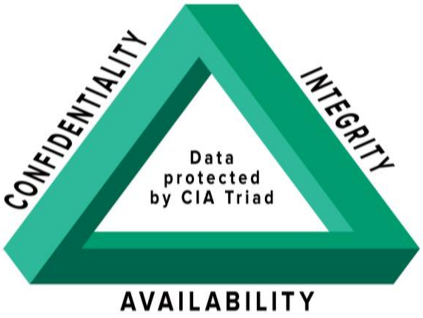


Fig: 1.2 Illustration of CIA Triad

Summary

This chapter introduces the concept of Information Security, which means protecting data from unauthorized access, changes, or loss. It explains the CIA Triad: Confidentiality (keeping data private), Integrity (keeping data accurate), and Availability (making sure data is accessible when needed). Key terms like Malware (harmful software), Phishing (fake messages to steal information), and Identity Theft (someone misusing your details) are also explained. The chapter highlights the importance of Cybersecurity, which is all about using safe practices and tools to protect computers and networks. Overall, it teaches how to stay safe in the digital world.

Practical Activity 1.1

Objective:

Learners will demonstrate the application of Information Security through a simulator or educational video.

Tools & Platform Needed:

Smartphone/computer with internet access, educational simulator/video platform (e.g., Cyber Safety simulators, Cyber security games, YouTube educational videos).

Procedure:

Step 1. Form small groups (3–4 students) to encourage collaboration.

Step 2. Choose one of the following information security themes:

- Strong password creation
- Phishing detection
- Two-factor authentication
- Access control and file permissions

Step 3. Watch an assigned educational video or use a free simulator like:

- Cyber Safety demos
- YouTube videos on information security basics

Step 4. Complete the activity shown (e.g., creating secure passwords, identifying fake emails).

Step 5. Note key learning points such as:

- How to recognize a phishing attack
- How strong passwords improve security
- What 2FA means and how it adds protection

Step 6. Each group presents 3 main takeaways, screenshots, and an example of how they will apply this in real life.

Step 7. Submit a summary highlighting how this improves personal or digital information safety.

Practical Activity 1.2

Objective:

Learners will understand and demonstrate the CIA Triad (Confidentiality, Integrity, Availability) using a simulator or video-based explanation.

Tools & Platform Needed:

Computer/tablet, internet access, animation/simulation tool (e.g., Curriculum simulator, Cybersecurity videos, PowerPoint-based CIA triad models).

Procedure:

Step 1. Divide students into pairs or small groups.

Step 2. Watch a short educational video or presentation explaining the CIA Triad.

Recommended YouTube keywords:

- "CIA Triad for beginners"
- "Cyber Security CIA Triad explained"

Step 3. Observe the three key concepts:

- Confidentiality: Protecting data from unauthorized access
- Integrity: Ensuring data is not changed or tampered with
- Availability: Ensuring data is available when needed

Step 4. Use a simulator (or guided teacher-led demo) to simulate these scenarios:

- Login attempts showing confidentiality breach
- File tampering examples for integrity
- Server downtime example for availability

Step 5. Discuss real-life examples for each (e.g., WhatsApp encryption = confidentiality, checksum = integrity).

Step 6. Each group creates a mini-presentation (3 slides max) explaining the CIA Triad with examples and screenshots, or drawings.

Step 7. Submit the group work and reflect on how CIA concepts help keep information secure in everyday life.

Assessment

Multiple Choice Questions:

1. What does the 'C' in the CIA Triad stand for?
   A. Cybersecurity
   B. Communication
   C. Confidentiality
   D. Control

2. What is the main purpose of Information Security?
   A. Speeding up the internet
   B. Protecting data from theft or damage
   C. Playing online games safely
   D. Creating computer programs

3. Which of the following is a type of malware?
   A. Firewall
   B. Virus
   C. Antivirus
   D. Browser

4. What does 'Integrity' in the CIA Triad mean?
   A. Hiding information from others
   B. Keeping data correct and unchanged
   C. Making data unavailable
   D. Encrypting passwords

5. If someone sends a fake email to steal your bank details, what is it called?
   A. Hacking
   B. Phishing
   C. Debugging
   D. Downloading

6. Which one of these is an example of identity theft?
   A. Someone using your internet
   B. Someone using your computer
   C. Someone pretending to be you online
   D. Someone is fixing your phone

7. What does 'Availability' mean in the CIA Triad?
   A. Making sure data is hidden
   B. Making sure data is accurate
   C. Making sure data is reachable when needed
   D. Making sure data is colorful

8. Which one of the following is used to protect your computer from malware?
   A. Video player
   B. Calculator
   C. Antivirus
   D. Keyboard

9. What is the full form of CIA in Information Security?
   A. Confidentiality, Integrity, Availability
   B. Control, Internet, Access
   C. Cybersecurity, Information, Application
   D. Computer, Integrity, Accuracy

10. Which one of the following is NOT a good security habit?
   A. Using strong passwords
   B. Clicking on unknown links
   C. Installing antivirus
   D. Logging out after use

Fill in the blanks:

1. The main goal of information security is to protect __________ from being stolen, changed, or lost.
2. The CIA Triad stands for Confidentiality, Integrity, and __________.
3. A __________ is a harmful software that can damage or steal data from your computer.
4. __________ means only authorized people can access the data.
5. __________ ensures that data is correct and not changed by someone who shouldn't.
6. If someone pretends to be you online and uses your details, it is called __________ __________.
7. A good way to protect your information is to use strong __________ that are hard to guess.
8. __________ means the data should be available to users when needed.
9. Clicking on unknown links from emails or messages can lead to a __________ attack.
10. An __________ program helps in detecting and removing viruses from your system.

True and False

1. Information security is only important for businesses, not for individuals.
2. The "C" in CIA Triad stands for Confidentiality.
3. Integrity in information security means making sure data is safe and not changed without permission.
4. Availability means hiding data from everyone, even authorized users.
5. Viruses and worms are types of malware.
6. Identity theft happens when someone uses your personal information without permission.
7. A strong password should include only your name and birthdate.
8. Phishing is a safe method of collecting emails from friends.
9. Antivirus software can help protect your computer from malware.
10. Keeping software updated helps improve information security.

Short answer questions:

1. What is information security?
2. What does the CIA Triad stand for in information security?
3. What is the meaning of confidentiality in the CIA Triad?
4. Why is integrity important in information security?
5. How does availability help users in accessing data?
6. What is malware? Give one example.
7. Define identity theft in simple words.
8. What is the purpose of using antivirus software?
9. How can we create a strong password?
10. Why is it important to update software regularly?

Answer Key

Multiple Choice Questions

1. C, 2. B, 3. B, 4. B, 5. B, 6. C, 7. C, 8. C, 9. A, 10. B

Fill-in-the-blanks

1. data, 2. Availability, 3. virus, 4. Confidentiality, 5. Integrity, 6. Identity theft, 7. Passwords, 8. Availability, 9. Phishing, 10. antivirus

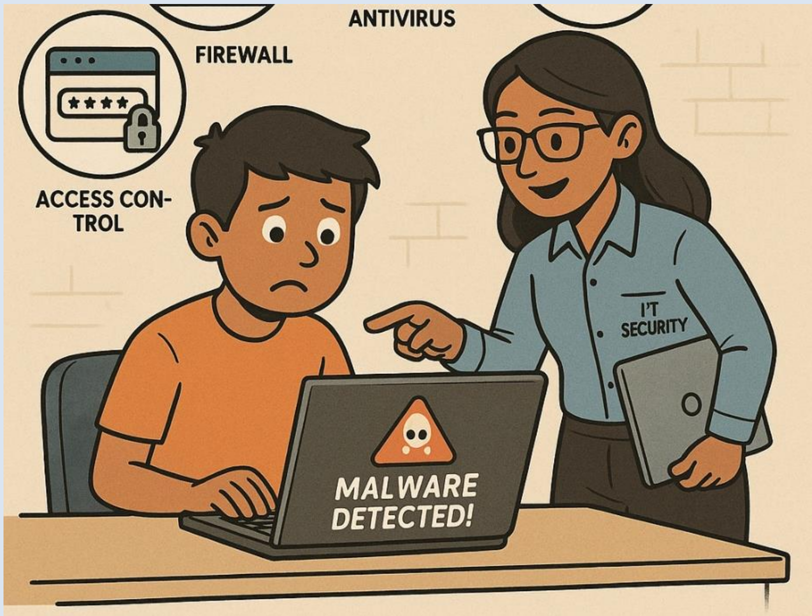
True/False questions

1. False, 2. True, 3. True, 4. False, 5. True, 6. True, 7. False, 8. False, 9. True, 10. True

Chapter-2

Ethical Hacking and Cryptography

Aryan was a bright student who enjoyed working with computers. One day, a virus made all the school computers crash. Unsure of what to do, Aryan turned to his sister Meera, an ethical hacker, for help. Meera explained that ethical hackers are like digital bodyguards—they protect systems from harmful hackers. She also introduced Aryan to cryptography, a method of locking messages with secret codes so that only the right people can read them. Aryan found it fascinating and began learning how to protect important data. Inspired, he dreamed of becoming a cyber defender to guard against online dangers.



Now, let's begin learning the things that made Aryan so excited!

2.1 Hacking

Hacking is the act of finding and using weaknesses or loopholes in computer systems, networks, or software. Sometimes, people hack to steal information, damage data, or disrupt services without permission. This type of hacking is illegal and harmful. However, not all hacking is bad; some people use hacking skills to help improve security. These helpful hackers are called ethical hackers, and they are allowed to test systems to find and fix problems before bad hackers can take advantage. In short, hacking means trying to break into a digital system, either for harmful or helpful purposes, depending on the hacker's intention.

2.1.1 Ethical Hacking

Ethical hacking is the process of testing computer systems, networks, or software to find security weaknesses—but with permission and for a good purpose. Ethical hackers, also called "white-hat hackers," use the same tools and techniques as malicious hackers, but they do it legally and responsibly. Their goal is to identify and fix problems before someone with bad intentions can exploit them. Companies and governments often hire ethical hackers to protect important data and systems. In simple words, ethical hacking helps make the digital world safer by staying one step ahead of cybercriminals.

Who uses Ethical Hacking?

- Governments, Banks; Schools, Big companies. They hire ethical hackers to make sure their systems are safe.

2.1.2 Types of Hacking

Type	**Role**
White-hat	Good hackers. Help protect systems.
Black-hat	Bad hackers. Steal or damage data.
Grey-hat	In-between. Sometimes break rules, but don't always have bad intentions.

2.1.3 Why Ethical Hacking is Important

Imagine your school has an online exam system. If a hacker breaks in and changes marks, that's serious! An ethical hacker would test the system first to stop that from happening.

Ethical hacking is important because it helps protect individuals, organizations, and governments from cyberattacks. In today's digital world, everything from bank accounts and personal data to hospital systems and online classes runs on computers and the internet. Hackers often try to break into these systems to steal information or cause damage. Ethical hackers, also called "white-hat hackers," use their skills to think and act like bad hackers, but in a safe and legal way. They look for weaknesses in systems before the bad guys do and help fix them. This keeps our data secure, protects privacy, and ensures that important services keep running without interruption. In short, ethical hacking is like having a friendly security guard who finds and fixes problems before trouble begins.

What they do?

Ethical hackers, also known as white-hat hackers, are professionals who help protect computer systems from cyber-attacks. They carefully test networks, websites, and software to find any weaknesses that could be used by malicious hackers. Using legal methods and special tools, they try to break into systems—just like a real hacker would—but with permission. After finding the security problems, they report them to the organization and suggest ways to fix them. Their main goal is to improve safety, prevent data loss, and keep sensitive information secure from cyber threats.

2.1.4 Common tools used

Ethical hackers use a variety of tools to test and secure systems. Here are some commonly used ones:

1. **Nmap (Network Mapper):** Used to scan networks and find open ports and devices connected to the network.
2. **Wireshark:** A network analyzer that captures and studies data traveling over a network.
3. **Metasploit:** A powerful tool used to test system vulnerabilities by simulating real cyber-attacks.
4. **Burp Suite:** Used mainly for testing the security of web applications, especially for finding weaknesses in websites.
5. **Kali Linux:** A specialized operating system filled with many hacking and security tools, often used by ethical hackers.
6. **John the Ripper:** A password cracking tool used to check the strength of passwords and understand how does this activity enhances personal or digital information safety.
7. **Aircrack-ng:** A tool used to test the security of wireless networks.

These tools help ethical hackers find and fix problems before real hackers can exploit them.

2.2 Introduction to Cryptography

Cryptography is the science of protecting information by changing it into secret code. Only people with the right key can read it.

Cryptography is important because it helps keep our information safe and private. It is like using secret codes to protect data from being read or changed by unauthorized people. Whether you are sending a message, shopping online, or using a banking app, cryptography ensures that your information is secure. It helps in:

- **Protecting personal data** like passwords, bank details, and health records.
- **Securing online transactions** so that hackers can't steal money or information.
- **Maintaining privacy** by making sure only the intended person can read the message.
- **Building trust** in digital systems, websites, and apps by keeping communication secure.

Without cryptography, the digital world would be very unsafe. Some everyday examples are as follows:

- WhatsApp uses end-to-end encryption
- Websites with https:// are using cryptography
- ATMs and credit cards also use it to protect data

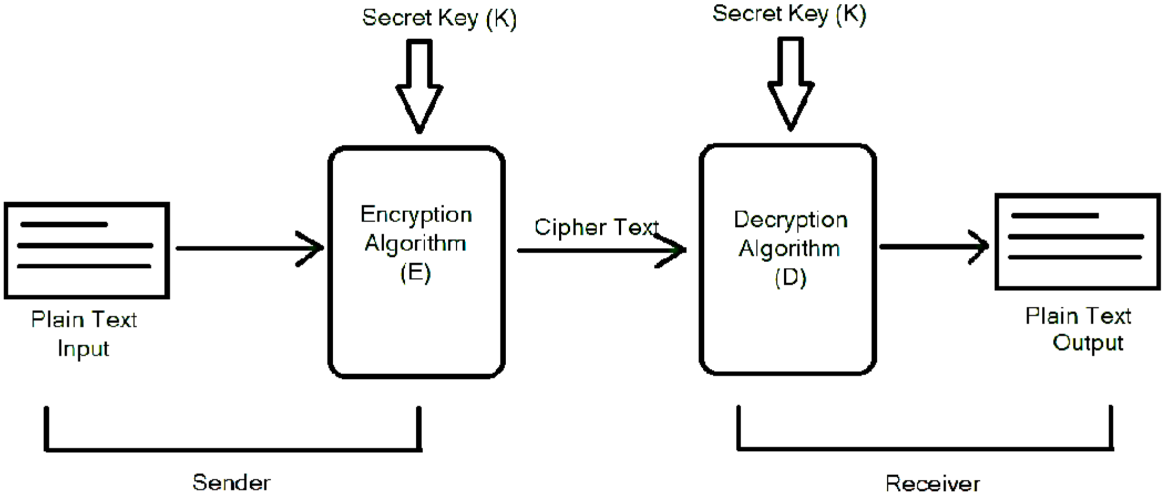


Fig: 2.1 Illustration of Cryptography

2.1.1 Common Terms

Some important terms used in cryptography are as follows:

Plaintext: This is the original, readable message or data before it is encrypted. Example: A simple message like "Hello".

Ciphertext: This is the unreadable, coded version of the message after encryption. Example: "1z@8x!" instead of "Hello".

Encryption: The process of turning plaintext into ciphertext using a key. It keeps the data safe from unauthorized access.

Decryption: Turning ciphertext back into readable plaintext using a key.

Key: A secret code used for encryption and decryption. It can be the same or different depending on the type of cryptography.

Algorithm: A step-by-step method or formula used to encrypt or decrypt data. Example: AES, RSA, SHA-256.

Digital Signature: A way to verify that a message or document hasn't been changed and is from a trusted sender.

Hashing: A method to convert data into a fixed-length value. It's one-way—once hashed, you can't get the original data back.

2.1.2 Types of Cryptography

Symmetric Key Cryptography

Symmetric Key Cryptography is a method of protecting information where the same key is used for both encrypting (converting the original message into a secret code) and decrypting (converting the code back into the original message). It's like using a single key to lock and unlock a treasure box. This method is simple and fast, making it suitable for many applications where speed is important. However, both the sender and the receiver must have the same secret key, and keeping this key safe becomes very important. If the key is stolen, anyone can read the secret messages.

- In this type, the same key is used to lock (encrypt) and unlock (decrypt) the message.
- It's fast and best for securing large amounts of data.
- Example: AES (Advanced Encryption Standard)

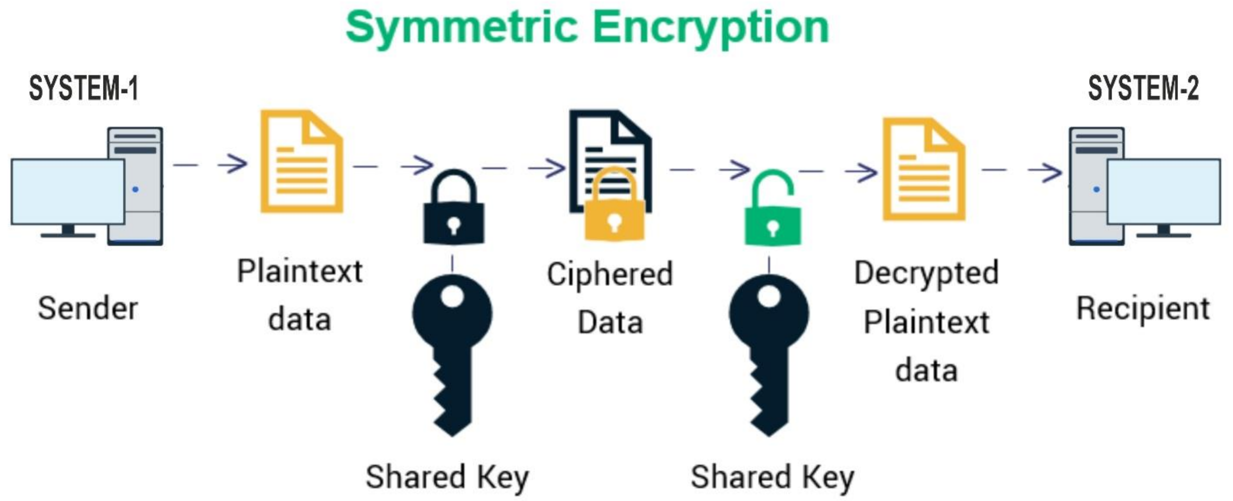


Fig: 2.2 Symmetric Key Cryptography

Asymmetric Key Cryptography

- This uses two keys: a public key to encrypt the data and a private key to decrypt it.
- It is more secure and is often used in emails or online payments.
- Example: RSA (Rivest–Shamir–Adleman)

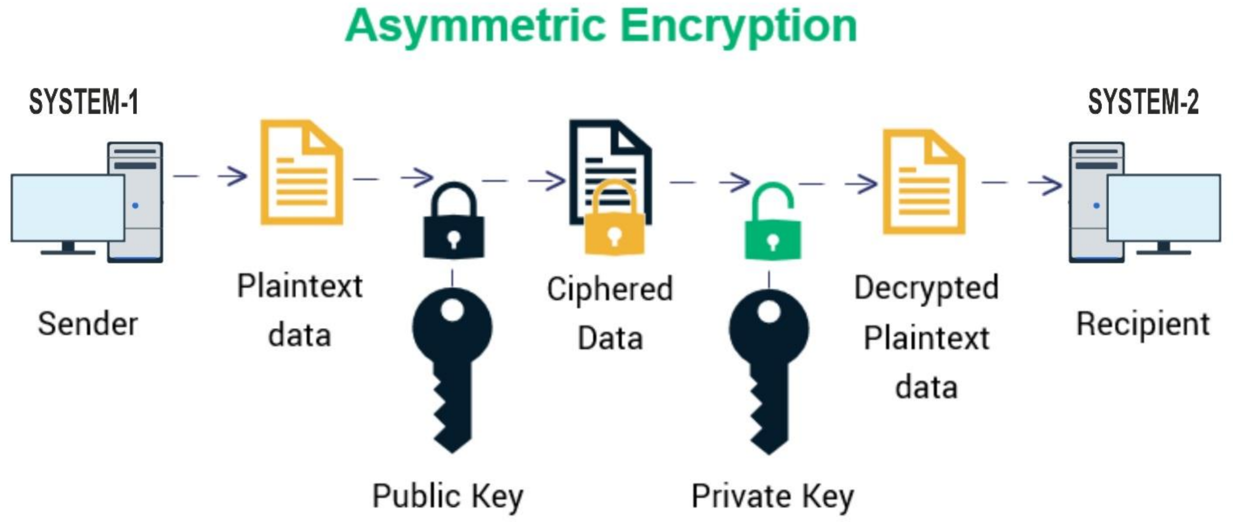


Fig: 2.3 Asymmetric Key Cryptography

Hash Functions

- This doesn't use any key. It converts data into a fixed-size string called a hash.
- It is mainly used to check data integrity, like passwords or downloaded files.
- Example: SHA-256

Each type of cryptography has a specific use and helps protect information in different ways.

Summary

- Ethical hacking helps protect computers and networks.
- White-hat hackers are good hackers who find and fix problems.
- Cryptography is used to keep data safe by converting it into secret codes.
- Two main types: symmetric (same key) and asymmetric (public/private keys).
- We use cryptography daily in apps, websites, banking, and more.
- Good hackers work to stop bad hackers!
- Cryptography = Secret codes + Keys
- Our digital world is safer because of these technologies.

Practical Activity 2.1

Objective:

To demonstrate the use of network monitoring tools (e.g., Wireshark) to observe data packets and analyze types of data transferred over a network.

Tools & Platform Needed:

Laptop/PC with internet access, Wireshark installed (or similar tools like Fiddler or GlassWire), secure network connection (school Wi-Fi or hotspot), and teacher supervision.

Procedure:

Step 1. Students will be divided into groups of 2–3.

Step 2. The teacher demonstrates how to install and launch Wireshark.

Step 3. Once opened, students will select the active network interface (e.g., Wi-Fi) and start capturing packets.

Step 4. Perform simple online activities (open a website, send a message, or refresh an app) to see live network traffic.

Step 5. Stop capturing after 2–3 minutes and filter results using protocols like HTTP, TCP, or DNS.

Step 6. Students will analyze the packet details, such as:

- Source & destination IPs
- Protocol used
- Size of data packets
- Type of request (GET, POST, etc.)

Step 7. Discuss which types of data are visible and how unsecured traffic can be a risk. Step 8. Each group creates a simple report with screenshots, examples of protocols, and one lesson learned about network data visibility and security.

Practical Activity 2.2

Objective:

To perform encryption and decryption of messages using online or offline tools and understand how data is protected.

Tools & Platform Needed:

Any browser-enabled device, online tool like https://www.cryptii.com, or offline software like VeraCrypt, Notepad++ plugin, or Python script (teacher-assisted).

Procedure:

Step 1. Students will work in pairs. One plays the sender, the other the receiver.

Step 2. Open an online encryption tool (like Cryptii) and write a short message (e.g., "My data is secure").

Step 3. Select a method of encryption (e.g., Caesar cipher, Base64, or AES if supported).

Step 4. Encrypt the message and copy the encoded result.

Step 5. Share the encrypted text with their partner, who will paste it in the tool and use the same key/method to decrypt it.

Step 6. The decrypted message should match the original. If not, troubleshoot and correct the settings.

Step 7. Discuss:

- What is encryption?
- Why is it important in online communication?
- What if someone intercepts the message without the key?

Step 8. Each pair documents their steps, screenshots, type of encryption used, and how encryption keeps digital information safe.

Assessment

Multiple Choice Questions

1. What is the main goal of ethical hacking?
   A) To steal data
   B) To harm systems
   C) To find and fix security flaws
   D) To create viruses

2. Which of the following is a tool used by ethical hackers?
   A) MS Paint
   B) Wireshark
   C) VLC Media Player
   D) Google Chrome

3. Which key is kept secret in Asymmetric Key Cryptography?
   A) Public key
   B) Shared key
   C) Private key
   D) Password

4. What does the "C" in CIA Triad stand for?
   A) Cryptography
   B) Confidentiality
   C) Communication
   D) Certificate

5. In Symmetric Key Cryptography, the same key is used for:
   A) Only encryption
   B) Only decryption
   C) Both encryption and decryption
   D) None of the above

6. Which of the following is NOT the purpose of cryptography?
   A) To secure data
   B) To hide data from hackers
   C) To speed up the internet
   D) To protect privacy

7. Ethical hackers are also known as:
   A) Black hat hackers
   B) Script kiddies
   C) White hat hackers
   D) Cyber criminals

8. Which of these is a type of encryption method?
   A) File Explorer
   B) RSA
   C) Photoshop
   D) Firewall

9. What does encryption do to a message?
   A) Deletes it
   B) Makes it unreadable to unauthorized users
   C) Sends it faster
   D) Copies it

10. Which of the following helps secure communication online using public and private keys?
    A) Notepad
    B) Antivirus
    C) Asymmetric encryption
    D) Printer

Fill in the Blanks

1. Ethical hackers are also known as ____________ hat hackers.
2. The main goal of ethical hacking is to ____________ and fix security weaknesses.
3. ____________ is the science of writing and solving secret codes.

4. In symmetric key cryptography, the ____________ key is used for both encryption and decryption.
5. The CIA Triad stands for Confidentiality, ____________, and Availability.
6. In asymmetric encryption, there are two keys: a ____________ key and a private key.
7. A common tool used for network analysis by ethical hackers is ____________.
8. Encryption helps to keep information safe from ____________ users.
9. ____________ is the process of converting plain text into an unreadable form.
10. In asymmetric encryption, the ____________ key is kept secret by the owner.

True or False Statements

1. Ethical hackers always work without permission to test system security.
   Cryptography helps in keeping information secure and private.
2. A black hat hacker is the same as an ethical hacker.
3. Encryption is a method of converting plain text into unreadable code.
4. Asymmetric key cryptography uses two different keys.
5. Symmetric cryptography is faster than asymmetric cryptography.
6. Ethical hackers help in finding and fixing security loopholes.
7. A firewall is a tool commonly used by ethical hackers.
8. In asymmetric cryptography, the same key is used for both encryption and decryption.
9. Data integrity means that information has not been altered or tampered with.

Answer Key

Multiple Choice Questions

1. C, 2. B, 3. C, 4. B, 5. C, 6. C, 7. C, 8. B, 9. B, 10. C

Fill-in-the-blanks

1. white, 2. find, 3. Cryptography, 4. same, 5. Integrity, 6. public, 7. Wireshark, 8. unauthorized, 9. Encryption, 10. private

True/False questions

1. False, 2. True, 3. False, 4. True, 5. True, 6. True, 7. True, 8. False, 9. True

Chapter-3

Operating System Security and Access Control

Ravi was a curious student who loved using his computer for school projects and gaming. One afternoon, while playing his favorite game, he noticed something strange—his computer was slow, and files were disappearing. Worried, he turned to his older cousin, Priya, for help.

Priya, who worked as an IT security specialist, quickly realized that Ravi's computer had been infected by malware. "This is why securing your operating system is so important," she explained. She taught Ravi about OS security and how hackers could break into systems if the security wasn't strong.

She showed Ravi how she used special tools to protect her computer, like firewalls and antivirus software, which stopped the bad software from doing harm. She also explained how access control worked: only authorized users could access certain files and settings. "It's like having a secret password to protect your most valuable belongings," she said.

Priya helped Ravi set up strong passwords and enabled encryption on his files to make sure even if someone tried to hack in, they wouldn't be able to read his data. Ravi was amazed at how simple yet powerful these tools were. He promised to always stay aware of his computer's security and even started learning more about protecting his data.

As Priya left, she said, "Remember, keeping your computer secure is not just about stopping viruses—it's about controlling who can access your information. And with the right tools, you can keep your computer safe from many dangers."

Ravi, now more aware of the importance of OS security, couldn't wait to explore more ways to protect his digital world. Let's dive in and explore together.

3.1 Introduction to Operating System Security

Operating System (OS) security refers to the measures and practices taken to protect the operating system of a computer from unauthorized access, attacks, and data breaches. Since the OS controls everything in a computer, including the hardware and software, it is a crucial element in ensuring the overall security of a system.

In simple terms, if the OS is compromised, the whole computer becomes vulnerable. Therefore, OS security is essential to protect sensitive information, personal data, and to prevent any malicious activities such as viruses, malware, or hackers.

3.1.1 Key Components of OS Security

User Authentication

The first line of defense in OS security is ensuring that only authorized users can access the system. This is achieved through methods such as passwords, PIN codes, and biometric systems (like fingerprints or face recognition).

Access Control

Access control helps in determining who can access what on a computer. It controls permissions for files, folders, applications, and other system resources. Only authorized users are granted access based on their roles (like Admin or User).

Security Policies

These are rules and guidelines that dictate how an OS and the system it runs on should be used. Security policies help ensure that users and administrators follow best practices to keep the system secure.

Encryption

Encryption converts data into an unreadable format, so even if someone accesses your data, they cannot understand it without the correct key. It's like locking your data with a secret code that only you or an authorized person can unlock.

3.1.2 Access Control in Detail

Access control is a way to ensure that only authorized users and processes can access specific resources on the computer, such as files, applications, or even the hardware. The most common methods of implementing access control in operating systems are:

Discretionary Access Control (DAC)

In DAC, the owner of the resource (like a file or folder) has the discretion to decide who can access it. The owner can allow or deny access to other users based on their preferences.

Mandatory Access Control (MAC)

In MAC, the operating system itself determines access permissions based on a set of rules. These rules cannot be changed by users. It's more rigid and ensures a higher level of security.

Role-Based Access Control (RBAC)

In RBAC, users are given access based on their roles within an organization. For example, an administrator has more access than a regular user. This method helps manage access efficiently in large organizations.

3.2 Introduction to Security Tools for Windows OS

Windows OS provides a variety of built-in tools to enhance system security. These tools help protect users from threats and ensure that unauthorized activities are prevented.

Windows Defender Antivirus

Windows Defender is a built-in antivirus program that protects against malware, viruses, spyware, and other harmful software. It constantly runs in the background and scans the system for threats.

Windows Firewall

The firewall helps block unauthorized access to your system over the network. It monitors incoming and outgoing traffic to ensure that no malicious or unauthorized connection can harm the computer.

BitLocker

BitLocker is a tool that encrypts the entire drive on your computer, ensuring that all your files and data are secure. Even if your computer is stolen, the encrypted data remains protected.

User Account Control (UAC)

UAC helps prevent unauthorized changes to your computer. It asks for permission whenever a program tries to make changes to the system that could affect its operation.

Security Update and Patch Management

Keeping your Windows OS updated with the latest security patches is essential. Windows Update automatically installs updates that fix vulnerabilities and bugs that could be exploited by hackers.

3.2.1 How OS Security Works in Simple Terms

Let's think of an operating system like a house. The house has rooms (files, data, and programs), and the door is the access point. The key to the door is your password.

- **Authentication:** Just like you need a key to enter a house, your computer needs authentication (like a password or fingerprint) to let you in. If you don't have the key, you can't enter.
- **Access Control:** Inside the house, you may have different rooms for different purposes. The owner (or admin) decides who gets to enter which room. Only trusted people can access sensitive rooms (files or programs).
- **Protection from External Threats:** To keep unwanted visitors away (hackers or viruses), you have a lock on the door (Windows Firewall), security cameras (Windows Defender), and even alarm systems (BitLocker encryption).

Together, these tools and strategies ensure that only the right people can access the right resources, and your data is protected from external threats.

Summary

It covers the significance of securing operating systems against potential cyber threats and unauthorized access, emphasizing the need for strong security measures. The chapter introduces different tools used to ensure the security of the Windows operating system, detailing how they protect against malware, unauthorized access, and data breaches. Key concepts such as user authentication, permissions, and encryption are explained to help students understand the role of OS security in safeguarding systems. By the end of the chapter, students will gain a basic understanding of how to keep their operating systems secure and the importance of access control.

Practical Activity 3.1

Objective:

To demonstrate the use of security tools such as Antivirus, Firewall, and BitLocker to protect a computer system.

Tools & Platform Needed:

Computer or laptop (Windows), Antivirus software (e.g., Windows Defender), Windows Firewall, BitLocker (if available), internet access.

Procedure:

Step 1. The teacher explains what each tool does:

- **Antivirus**: Detects and removes malware.
- **Firewall**: Blocks unauthorized access.
- **BitLocker**: Encrypts your hard drive for security.

Step 2. Students work in pairs. Each pair will explore the security tools installed on the computer.

Step 3. Open Windows Security and check the status of Antivirus and Firewall:

- Go to Settings > Update & Security > Windows Security.
- Click on Virus & Threat Protection to view antivirus status.
- Click on Firewall & Network Protection to view firewall settings.

Step 4. If BitLocker is available (on Pro or Edu editions), explore it via Control Panel > BitLocker Drive Encryption (do not turn it on without teacher supervision).

Step 5. Discuss:

- What threats do these tools defend against
- How automatic updates keep antivirus effective
- Why encryption adds an extra layer of safety

Step 6. Prepare a short group report or slide summarizing what each tool does, with screenshots and one real-life example of its use.

Practical Activity 3.2

Objective:

To demonstrate Windows Firewall settings through a video or simulation, and understand how it controls network access.

Tools & Platform Needed:

Computer/laptop, internet connection, projector or screen, YouTube video or school-provided simulation (e.g., "Windows Firewall Settings Explained").

Procedure:

Step 1. The teacher plays a video/simulation showing how to access and modify Windows Firewall settings.

Suggested keyword: *"How to Use Windows Defender Firewall to Block or Allow Programs"*

Step 2. Students observe and note down the steps:

- How to open the Firewall via **Control Panel or Settings**
- Viewing current network settings
- Allowing or blocking an app through the firewall
- Turning the firewall on/off (with caution)

Step 3. Discuss how firewall rules are created and how they protect against network threats.

Step 4. In pairs, students simulate the steps (without applying risky changes), like checking which apps are allowed through the firewall.

Step 5. Each group documents:

- What settings are visible
- What options are available for public vs. private networks
- What could happen if the firewall is turned off

Step 6. Submit a reflection or presentation slide explaining how the Windows Firewall helps protect your device and data from unauthorized access.

Answer Key

Multiple Choice Questions

1. What is the primary purpose of operating system security?
   A) To speed up the computer's performance
   B) To protect the computer from unauthorized access and threats
   C) To manage hardware resources
   D) To improve software performance

2. Which of the following is a common type of access control used in OS security?
   A) Encryption
   B) Multi-factor authentication
   C) Access control lists (ACL)
   D) All of the above

3. What does the term "least privilege" refer to in access control?
   A) Allowing users to access all system resources
   B) Limiting user permissions to the minimum needed for their role
   C) Allowing users to modify system settings
   D) Granting administrative rights to all users

4. Which Windows security tool helps to protect against malware and malicious software?
   A) Windows Firewall
   B) Windows Defender
   C) Task Manager
   D) Control Panel

5. Which of the following is a method of securing communication between users and the operating system?
   A) Biometric authentication
   B) Usernames and passwords

C) Virtual Private Network (VPN)
D) All of the above

6. What does the principle of "Defense in Depth" refer to?
   A) Using only a single security measure for protection
   B) Layering multiple security measures to protect the system
   C) Ensuring strong passwords are used
   D) Monitoring user activity

7. Which of these is an example of biometric authentication?
   A) Username and password
   B) Fingerprint scan
   C) PIN code
   D) CAPTCHA

8. What is a firewall used for in OS security?
   A) To manage files and folders
   B) To block unauthorized access to a computer network
   C) To run antivirus software
   D) To speed up internet connections

9. In Windows OS, which tool is commonly used for checking system performance and resource usage?
   A) Task Manager
   B) Command Prompt
   C) Windows Explorer
   D) Disk Cleanup

10. Which of the following access control methods is primarily used for ensuring that only authorized users can access sensitive information?
    A) File permissions
    B) User roles and policies
    C) Encryption
    D) All of the above

Fill in the Blanks

1. The process of verifying the identity of a user before allowing access is called __________.
2. __________ is the Windows tool that provides real-time protection against viruses and malware.
3. In access control, the rule of __________ privilege means giving users the minimum level of access necessary to do their job.
4. A __________ is used to monitor and control incoming and outgoing network traffic based on security rules.
5. The list that defines which users or system processes are granted access to objects is called __________.
6. __________ authentication uses something the user is, such as a fingerprint or facial recognition.

True & False

1. Operating system security helps protect computers from unauthorized access.
2. A password is not considered a part of authentication.
3. Access control decides who can access what part of a computer system.
4. Firewalls are used to increase the internet speed.
5. Windows Defender is a built-in security tool in Windows OS.
6. Only administrators can use access control settings.

7. Biometric security uses things like fingerprints or facial recognition.
8. OS security has nothing to do with viruses.
9. Encryption is used to make files readable to everyone.
10. Using strong passwords improves your computer's security.

Short Answer Questions

1. What is the role of an operating system in computer security?
2. What is access control?
3. Name any two tools used for OS security.
4. Why are strong passwords important?
5. What is biometric authentication?
6. What is the function of a firewall?

Answer Key

Multiple Choice Questions

1. B, 2. D, 3. B, 4. B, 5. D, 6. B, 7. B, 8. B, 9. A, 10. D

Fill-in-the-blanks

1. Authentication, 2. Windows Defender, 3. Least, 4. Firewall, 5. Access Control List (ACL), 6. Biometric

True/False questions

1. True, 2. False, 3. True, 4. False, 5. True, 6. False, 7. True, 8. False, 9. False, 10. True

Chapter-4

Introduction to Wireless Networks

Riya was excited to use her new tablet at home. She connected to a neighbor's open Wi-Fi and started browsing. The next day, her device was behaving strangely—apps were crashing, and some files disappeared. Worried, she told her older cousin, Aarav, who was studying computer science. Aarav explained that using an unsecured Wi-Fi network is risky. Anyone can access your data or even control your device!

He showed Riya how to connect safely by using secured networks with strong passwords and taught her about encryption and firewalls. Riya learned how wireless networks work and how important it is to protect them.
From that day on, she never connected to an unknown Wi-Fi and even helped her parents set a strong password at home.

4.1 Introduction

A wireless network allows devices like mobile phones, laptops, and tablets to connect to the internet or other devices without using wires. Instead of cables, these networks use radio signals or infrared to transmit data.
Wireless networks are used in homes, schools, offices, airports—almost everywhere!
But, just like unlocked doors, wireless networks without security can be dangerous. Hackers can easily steal data or harm your device if your network is not protected.

4.1.1 Types of Wireless Networks

There are different types of wireless networks based on how far the signals can travel.

- ***Personal Area Network (PAN)***: A Personal Area Network (PAN) is a small network used for connecting devices within a very short range, usually within 10 meters. It allows personal devices such as smartphones, tablets, laptops, smartwatches, and wireless earphones to communicate with each other without using cables. PANs are mostly wireless and are commonly used at home, in cars, or on-the-go to share files, stream music, or sync data between devices.

Key Points:

- PAN covers a very small range (typically a few meters).
- Commonly uses Bluetooth, Infrared (IR), or USB for connectivity.
- Designed for personal use, not for large-scale networking.
- Useful for file sharing, internet tethering, and device synchronization.

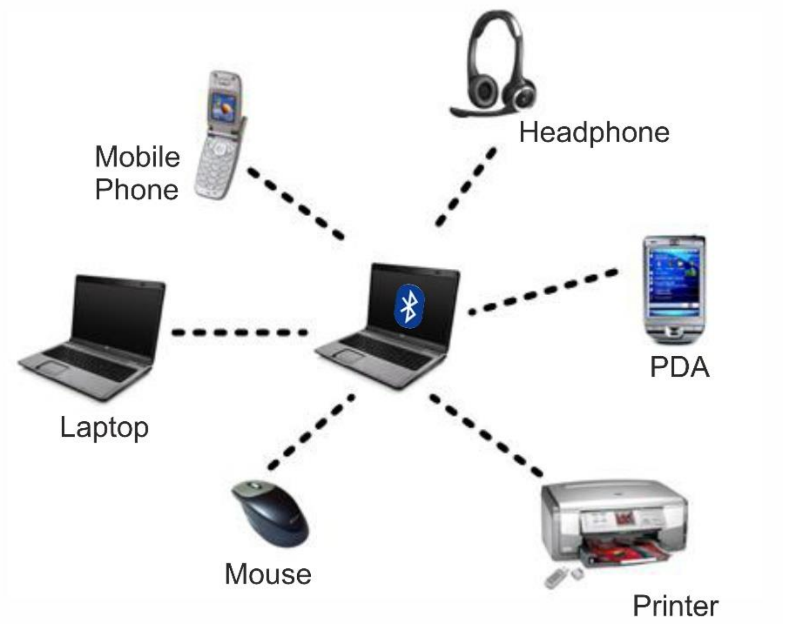


Fig: 4.1 Example of a Personal Area Network (PAN) showing wireless communication between a smartphone, smartwatch, and wireless earphones via Bluetooth.

- ***Local Area Network (LAN):*** A Local Area Network (LAN) is a network that connects computers and other devices within a limited area such as a home, school, office building, or campus. It allows users to share resources like files, printers, internet connections, and software applications. LANs are faster and more secure compared to wider networks because they are confined to a small geographic area and usually managed by a single organization. LANs can be wired (using Ethernet cables) or wireless (using Wi-Fi). In a wired LAN, devices are connected through switches, routers, and cables. In a wireless LAN, devices use Wi-Fi signals to connect to a central access point. LANs are commonly used in schools for sharing documents and internet, in offices for collaborative work, and in homes to connect multiple devices to a single internet source.

Key Points:

- Covers a small physical area (like one building).
- Offers high-speed data transfer.
- Allows resource sharing among connected devices.
- Easier to manage and secure than larger networks.

Suggested Figure Caption:

A Local Area Network (LAN) setup connecting computers, printers, and mobile devices within an office environment.

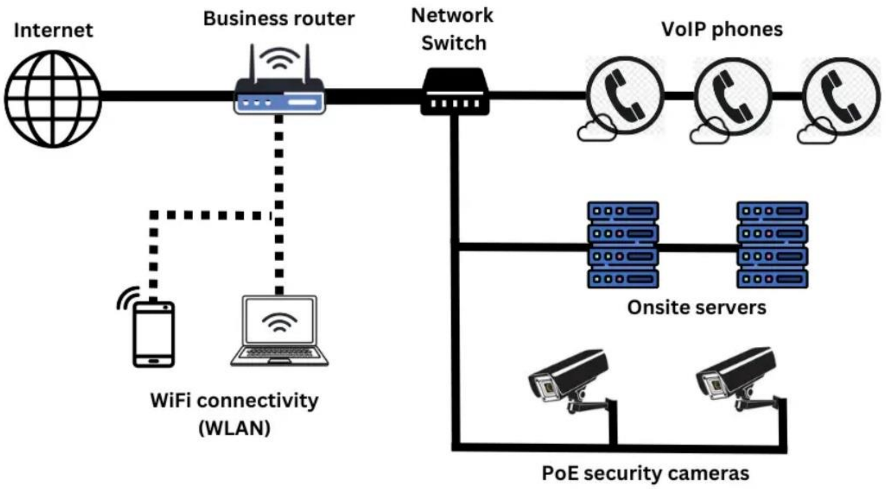


Fig: 4.2 Local Area Network (LAN) setup connecting computers, printers, and mobile devices within an office environment.

- ***Metropolitan Area Network (MAN)***
  A Metropolitan Area Network (MAN) is a network that spans a large city or a group of nearby cities. It is larger than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN). A MAN connects multiple LANs within a city to form a bigger network, allowing communication and data sharing between schools, businesses, government offices, and other organizations located across the city.
  MANs are often established using high-speed fiber optic cables or wireless microwave transmissions. They are managed by telecom providers or government agencies and usually support faster data speeds than WANs but cover shorter distances. A good example of a MAN is the network used by a city's public transportation system or a group of hospitals within a metro area that share medical records and services.

Key Features:

- Covers a city or a metropolitan area.
- Connects multiple LANs together.
- Faster and cheaper than WANs.
- Often managed by service providers.

Suggested Figure Caption:
A Metropolitan Area Network (MAN) linking different offices and institutions across a city using high-speed connections.

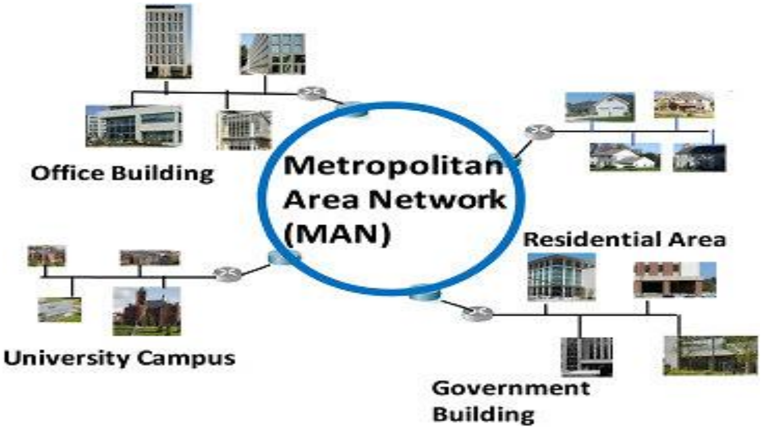


Fig: 4.3 Metropolitan Area Network (MAN) linking different offices and institutions across a city using high-speed connections

- ***Wide Area Network (WAN)***

A Wide Area Network (WAN) is the largest type of network, covering vast geographical areas, such as countries or continents. It connects multiple LANs and MANs over long distances. The internet is the most well-known example of a WAN, linking millions of computers and devices around the world.

WANs use public networks like telephone lines, satellite links, or undersea cables to transfer data. Since the distance is much greater than in LANs or MANs, WANs often require special devices such as routers, switches, and modems. These networks are mostly managed by Internet Service Providers (ISPs) or large organizations.

WANs are essential for global communication, enabling emails, video conferencing, file sharing, and access to cloud services. Although they may experience slower speeds and higher costs than local networks, WANs are necessary for modern businesses and services that operate in different regions.

Key Features:

- Covers large areas like countries or continents.
- Connects multiple LANs and MANs.
- Uses public and private transmission systems.
- Vital for global communication and internet access.

Suggested Figure Caption:

A Wide Area Network (WAN) connecting different countries and continents through satellites, undersea cables, and telecom infrastructure.

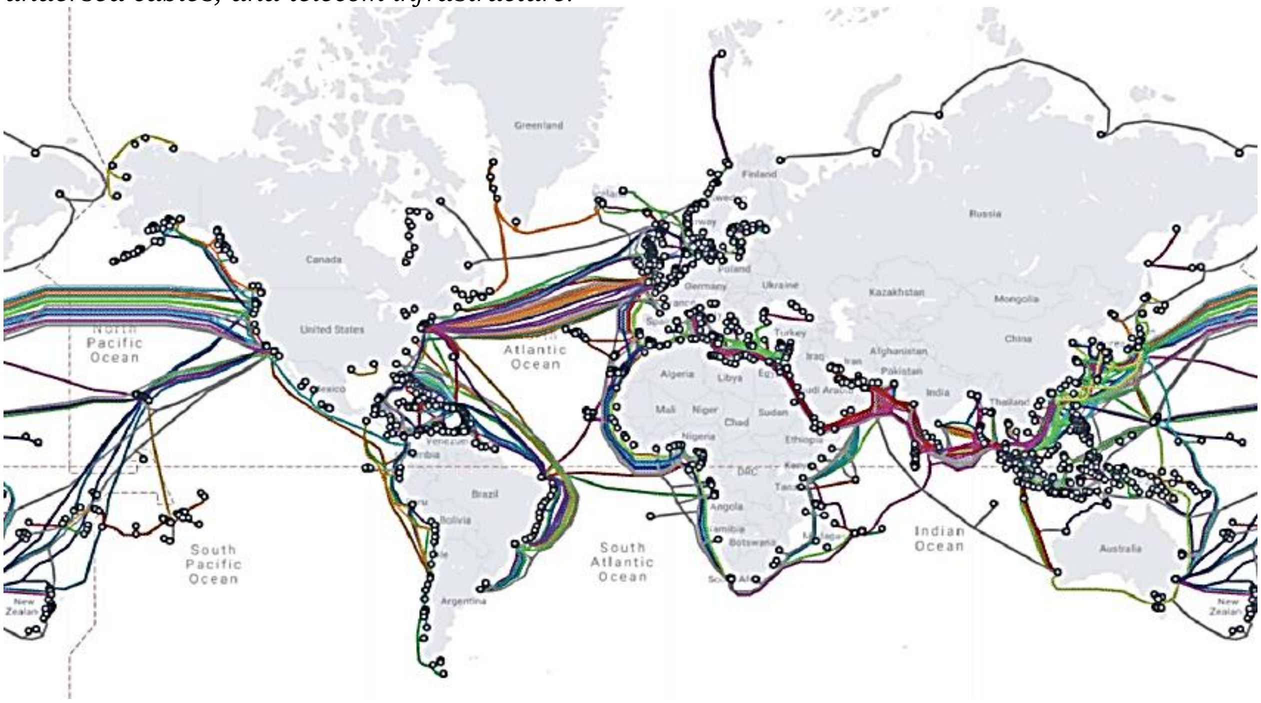


Fig: 4.4 Wide Area Network (WAN) .

4.1.2 Comparison table of PAN, LAN, MAN, and WAN

Feature	PAN (Personal Area Network)	LAN (Local Area Network)	MAN (Metropolitan Area Network)	WAN (Wide Area Network)
Full Form	Personal Area Network	Local Area Network	Metropolitan Area Network	Wide Area Network
Coverage Area	Very small (within a few meters)	Small (home, school, office)	Medium (city or town)	Very large (country or world)
Devices Connected	Phones, laptops, smartwatches	Computers, printers, servers	Multiple LANs	Multiple LANs and MANs
Example	Bluetooth headset with phone	School computer lab	City-wide cable TV network	The Internet
Speed	Low to Medium	High	Medium to High	Medium
Ownership	Individual user	Organization or individual	Internet service provider (ISP)	ISP or large companies
Cost	Very low	Low	Medium	High
Security Level	Low	High (with setup)	Medium	Depends on encryption and protocols

Table 4.1: Comparison table of PAN, LAN, MAN, and WAN

4.2 Wireless Network Security

Wireless network security refers to the measures taken to protect data and devices connected through wireless networks from unauthorized access, misuse, or damage. Unlike wired networks, wireless networks transmit data using radio waves, making them more vulnerable to various types of attacks. As wireless technology becomes more common in homes, schools, offices, and public places, securing wireless networks has become increasingly important.

When a device connects to a wireless network, it sends and receives signals through the air. This open-air communication can be intercepted by hackers if the network is not properly protected. Common threats include unauthorized access, eavesdropping, data theft, and denial-of-service attacks. To prevent such risks, wireless network security uses several tools, settings, and protocols.

4.2.1 Common Security Measures

1. **Encryption**: The most essential protection for wireless networks is encryption. It scrambles the data being sent, making it unreadable to anyone without the correct key. Common encryption standards include:
   - **WEP (Wired Equivalent Privacy)**: An older, weaker method that is no longer considered secure.
   - **WPA (Wi-Fi Protected Access)** and **WPA2**: More secure standards, with WPA2 being the most widely used.
   - **WPA3**: The newest and most secure standard, offering better encryption and protection from brute-force attacks.
2. **Passwords and Authentication**: A strong network password prevents unauthorized devices from connecting. Users should create passwords that are long, unique, and contain a mix of letters, numbers, and symbols. Advanced networks may also use **two-factor authentication** or digital certificates for added security.
3. **Hiding SSID (Network Name)**: Every wireless network has an SSID (Service Set Identifier) or network name. Hiding the SSID can make the network less visible to outsiders, though it is not a strong form of security by itself.

4. **MAC Address Filtering**: Each device has a unique MAC (Media Access Control) address. Networks can be set up to allow only specific MAC addresses to connect, adding an extra layer of control.
5. **Firewalls and Antivirus Software**: Firewalls help block harmful traffic, while antivirus software protects individual devices connected to the network from malware.
6. **Network Monitoring**: Regularly checking the network for unusual activity can help identify threats early. Tools and apps are available for this purpose.

Why It Matters

If wireless networks are not secured, attackers can:

- Steal private data like passwords and bank details.
- Use the network for illegal activities.
- Install malware on connected devices.
- Interrupt normal communication by overloading the network.

Schools, businesses, and even homes depend on wireless networks to stay connected. A security breach can lead to data loss, financial damage, and even legal problems. Therefore, it's important to regularly update routers, change passwords, and use the latest security standards.

Practical Activity 4.1

Objective:

To demonstrate different types of wireless networks using simulations or videos.

Tools & Platform Needed:

Projector/screen, internet-enabled computer, simulation tool (like Cisco Packet Tracer or NetSim), or educational videos (YouTube or offline).

Procedure:

Step 1. Begin with a teacher-led introduction to wireless network types:

- WLAN (Wireless Local Area Network)
- WPAN (Wireless Personal Area Network)
- WMAN (Wireless Metropolitan Area Network)
- WWAN (Wireless Wide Area Network)

Step 2. Play an animated simulation/video showing how each network works (e.g., laptop connecting to Wi-Fi = WLAN; Bluetooth headphones = WPAN).

Step 3. Discuss:

- Range of each network type
- Examples from daily life
- Speed and coverage differences

Step 4. Use a diagram or a classroom activity to simulate how devices connect wirelessly in each type.

Step 5. Students note key differences in a table:

Type	Range	Devices Used	Real-life Example

Step 6. Each student/group creates a slide or poster summarizing the types of wireless networks with visuals and examples.

Practical Activity 4.2

Objective:

To demonstrate wireless network security techniques using a simulation or video.

Tools & Platform Needed:

Computer with internet, video/simulation on Wi-Fi security (e.g., WPA2, passwords, MAC filtering), optional router for demo, projector/screen.

Procedure:

Step 1. The teacher shows a video/simulation of:

- Setting up Wi-Fi security (WPA2/WPA3)
- Changing default router credentials

- Using MAC address filtering
- Hiding SSID (network name)

Step 2. Discuss each security measure:

- What it protects against
- Real-world example (e.g., neighbor can't use Wi-Fi without password)
- Strong vs. weak passwords

Step 3. If a demo router is available, show how to:

- Log into router settings
- Change the password and SSID
- Enable WPA2 encryption

Step 4. Students note the techniques and their purpose:

Security Technique	**Purpose**	**Example**
WPA2 Encryption	Encrypts data	Safer home Wi-Fi
Strong Password	Stops unauthorized access	Mix of letters/numbers
MAC Filtering	Allows only known devices	Prevents strangers' access

Step 5. Groups submit a 1-page summary or short oral presentation:
"How can we make our Wi-Fi safer?"

Assessment

Multiple Choice Questions (MCQs)

1. What does PAN stand for?
   a) Public Area Network
   b) Personal Area Network
   c) Private Access Network
   d) Protected Access Node

2. Which type of network connects devices in a small area like a home or office?
   a) MAN
   b) WAN
   c) LAN
   d) PAN

3. What does Wi-Fi use to transmit data?
   a) Wires
   b) Radio waves
   c) Optical fiber
   d) Bluetooth

4. Which one is an example of a PAN device?
   a) Smartwatch
   b) City-wide CCTV network
   c) School computer lab
   d) Bank server

5. What is the full form of WPA2?
   a) Wireless Protected Access 2

b) Wide Protected Area
c) Wireless Password Access
d) Web Privacy Area

6. Which network covers large geographical areas?
a) LAN
b) PAN
c) WAN
d) HAN

7. What helps protect wireless networks from hackers?
a) Using open networks
b) Disabling encryption
c) Setting strong passwords
d) Connecting many users

8. Which of the following is used to encrypt data on Wi-Fi networks?
a) HTTP
b) VPN
c) WPA3
d) FTP

9. A MAN is most likely used in a:
a) School
b) Small office
c) Entire city
d) Bedroom

10. What should you avoid doing on an open public Wi-Fi?
a) Checking weather
b) Downloading safe apps
c) Banking or sharing passwords
d) Watching videos

Fill in the Blanks

1. _________ uses radio waves to connect devices without wires.
2. A _________ connects devices like phones and smartwatches within a few meters.
3. A _________ covers a larger area than LAN but smaller than WAN.
4. _________ is used to protect wireless networks by converting data into secret code.
5. The latest and most secure Wi-Fi protection method is _________.
6. Using a strong _________ helps prevent unauthorized access to your Wi-Fi.

True or False

1. Bluetooth is used to create a Personal Area Network.
2. A LAN covers a larger area than a WAN.
3. Wi-Fi is a type of wireless network.
4. Encryption helps secure wireless communication.
5. All wireless networks are automatically secure.

Short Answer Questions

1. What is a Personal Area Network (PAN)?
2. Name two types of wireless networks.
3. Why is wireless network security important?
4. What does LAN stand for?

5. How can you make a Wi-Fi network more secure?

Answer Key

Multiple Choice Questions
1. b, 2. c, 3. b, 4. a, 5. a, 6. c, 7. c, 8. c, 9. c, 10. c

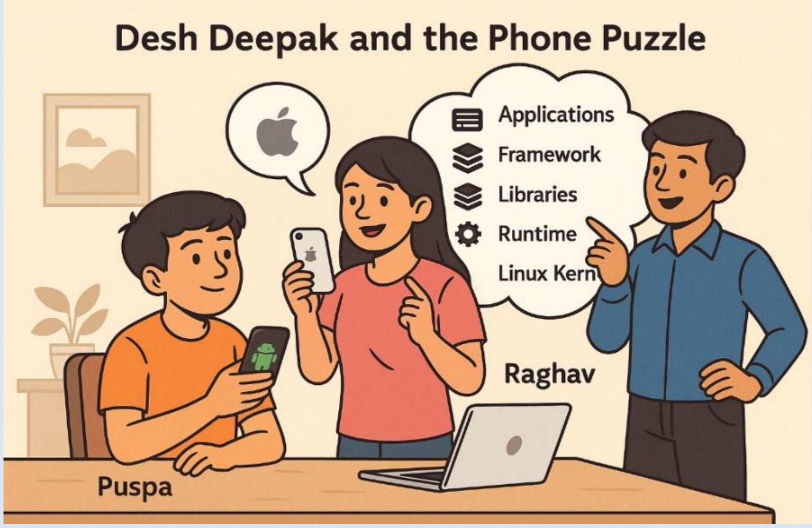
Fill-in-the-blanks
1. Wi-Fi, 2. PAN, 3. MAN, 4. Encryption, 5. WPA3, 6. password

True/False questions
1. True, 2. False, 3. True, 4. True, 5. False

Chapter-5

Introduction to Mobile Operating Systems – Android and iOS

Desh Deepak was thrilled when he received a Samsung smartphone for his birthday. He couldn’t wait to explore its features. But his excitement grew even more when he saw that his cousin Puspa had also gotten a new phone—an iPhone!



Curious, Desh Deepak asked, “Why does your phone look so different from mine?”
Puspa smiled and said, “I’m using iOS, and you’re using Android. Both are mobile operating systems, but they are different.”

Desh Deepak was confused. “What’s an operating system?”

Puspa explained, “An operating system is like the brain of the phone. It controls everything, from apps to the camera to the internet.”

Desh Deepak’s eyes widened. “So, what makes Android special?”

“Android is made by Google,” Puspa said. “It’s used in many phones, like Samsung, Xiaomi, and OnePlus. You can customize it—change wallpapers, add widgets, and download lots of apps from the Google Play Store.”

“That sounds fun!” Desh Deepak said. “What about iOS?”

Puspa grinned. “iOS is made by Apple and works only on iPhones. It’s very secure and smooth. Plus, I use Siri, my voice assistant, to set reminders or ask questions.”

Just then, Desh Deepak’s older brother, Raghav, walked in and offered to explain how Android works.

“Android has parts like Applications, Framework, Libraries, Runtime, and the Linux Kernel,” Raghav said. “These parts work together to run the phone smoothly.”

Desh Deepak was amazed. “Now I understand! Both systems are amazing in their way.”

From that day, Desh Deepak became curious about how smartphones worked and wanted to learn more about both Android and iOS. Let's also dive in and explore together.

5.1 Introduction of Android OS and iPhone iOS

Today, most people use smartphones for calling, chatting, watching videos, playing games, and doing schoolwork. But have you ever thought—what makes a smartphone work?

The answer is a mobile operating system (OS). It is the main software that controls everything on your phone.

Two of the most popular mobile operating systems are:

1. Android OS – Made by Google, used in many phones like Samsung, Vivo, Redmi, OnePlus, etc.
2. iPhone iOS – Made by Apple, used only in Apple phones like iPhone, iPad, and iPod.

These operating systems help you:

- Open and use apps
- Connect to the internet
- Take pictures
- Watch videos
- Play games
- and much more!

Android and iOS look different and work in different ways, but both are very powerful and easy to use.

5.2 Specialization and Features of Android OS

Android is a mobile operating system made by Google. It is used in many different brands of phones like Samsung, Redmi, Realme, Vivo, OnePlus, and more.

5.2.1 Specialization (What makes Android special)

- *Open to all:* Android is open-source, which means phone companies can change it and add new features.
- *Works on many phones:* You can find Android in all kinds of phones – expensive and budget-friendly.
- *Customizable:* You can change the wallpaper, ringtone, and even the look of the screen.
- *Millions of apps:* You can download games, study apps, tools, and more from the Google Play Store.

5.2.2 Features of Android

- Google Assistant helps you by voice, like asking questions or setting reminders.
- Widgets show important information on the home screen, like time, weather, or calendar.
- Easy notifications for calls, messages, and updates.
- Multitasking – you can run more than one app at the same time.
- Google apps like YouTube, Gmail, and Maps come built-in.

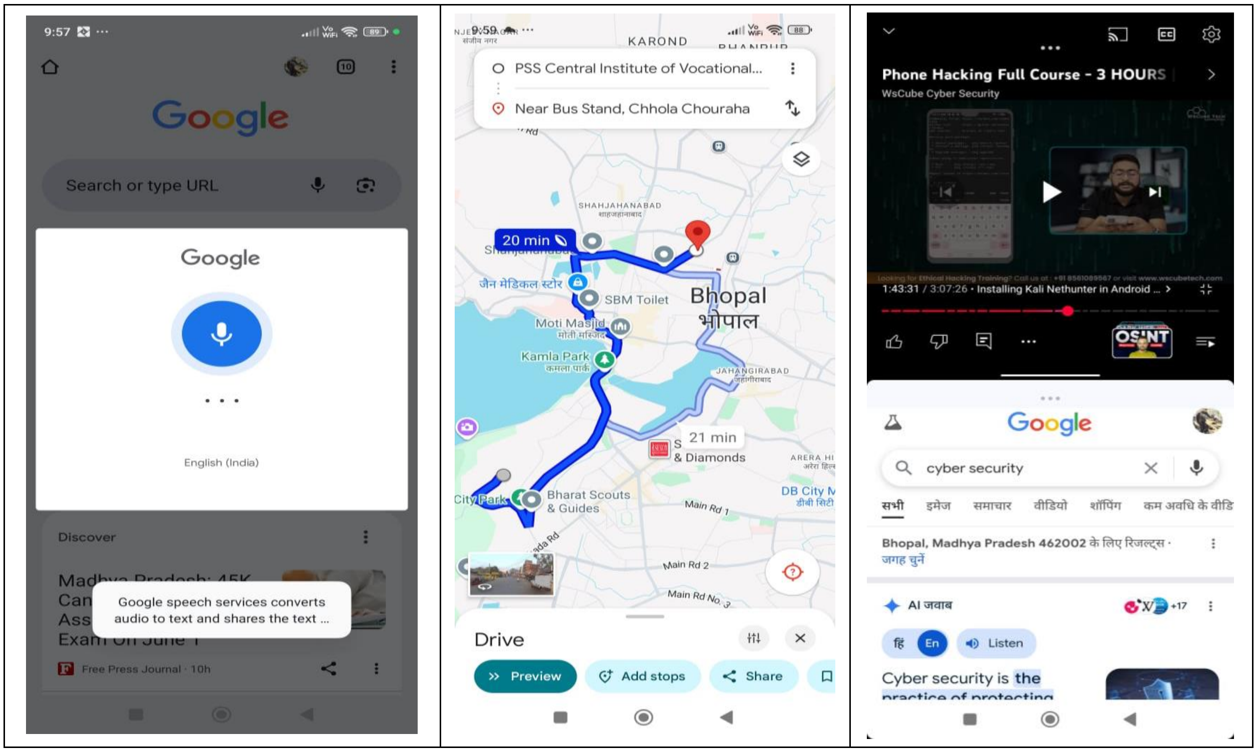

Google
Search or type URL
Google
English (India)
Discover
Google speech services converts audio to text and shares the text ...
Free Press Journal · 10h
PSS Central Institute of Vocational...
Near Bus Stand, Chhola Chouraha
20 min
21 min
Bhopal
भोपाल
Drive
Preview
Add stops
Share
Phone Hacking Full Course - 3 HOURS
WsCube Cyber Security
1:43:31 / 3:07:26 · Installing Kali Nethunter in Android
Google
cyber security
Bhopal, Madhya Pradesh 462002 के लिए रिजल्ट्स
AI जवाब
Listen
Cyber security is the practice of protecting

Fig: 5.1 Google Assistant and Google Map, and Split Screen in an Android phone

5.3 Specialization and Features of iPhone iOS (in Simple Words)

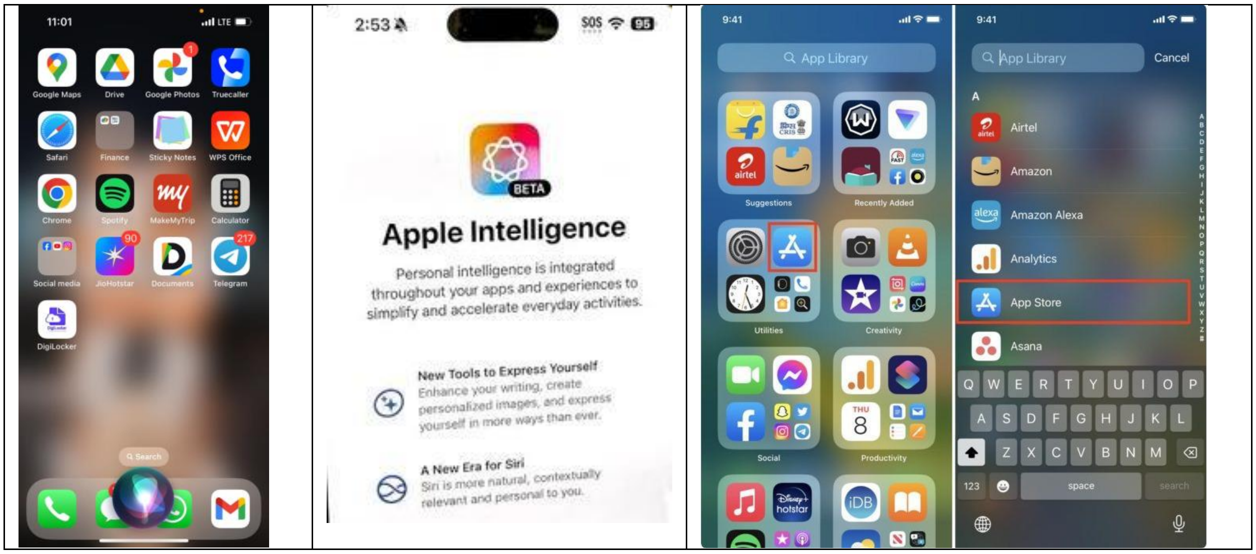
iOS is the mobile operating system made by Apple. It is used only in Apple devices like the iPhone, iPad, and iPod Touch.

5.3.1 Specialization (What makes iOS special)

- *Only for Apple:* iOS works only on Apple devices. It is not used in any other brand.
- *Very safe and secure:* Apple controls everything, so the system is more protected from viruses.
- *Very smooth and fast:* iPhones run very well because iOS is made specially for Apple hardware.
- *Regular updates:* Apple gives new updates to all iPhones at the same time.

5.3.2 Features of iOS

- Siri – Apple's voice assistant, like Google Assistant.
- App Store – A place to download high-quality apps and games.
- iCloud – Automatically backs up your photos, messages, and files online.
- Face ID or Touch ID – Unlock your phone using your face or fingerprint.
- Strong privacy – iOS asks your permission before any app uses your camera, mic, or location.



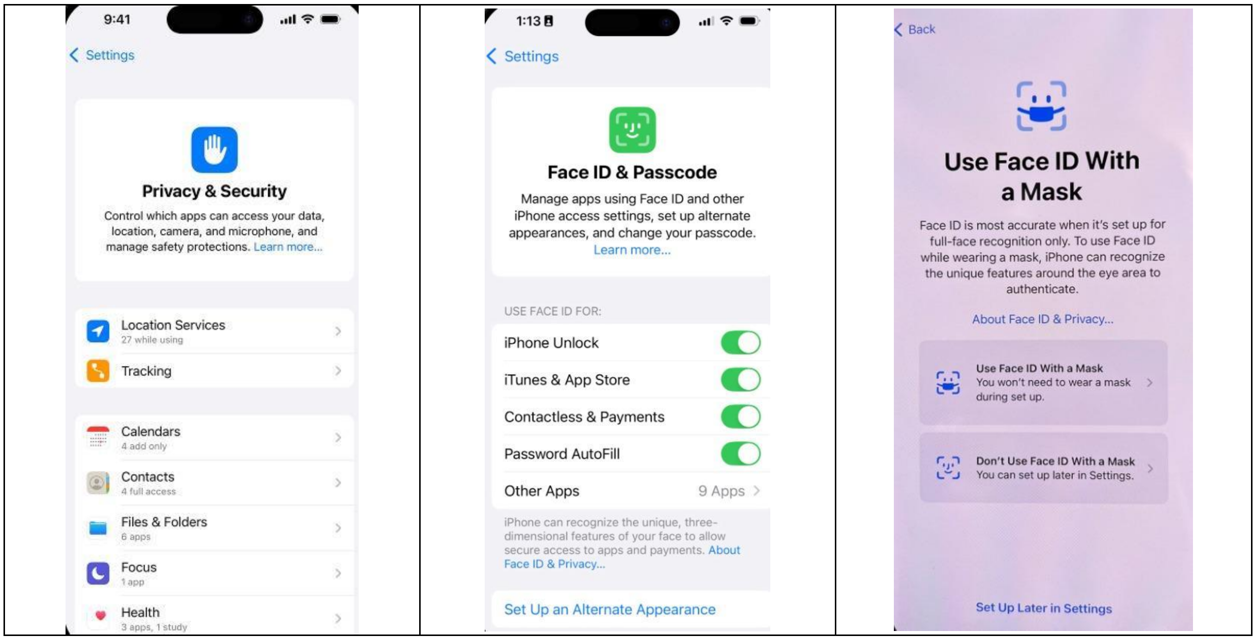
Apple Intelligence

Personal intelligence is integrated throughout your apps and experiences to simplify and accelerate everyday activities.

New Tools to Express Yourself
Enhance your writing, create personalized images, and express yourself in more ways than ever.

A New Era for Siri
Siri is more natural, contextually relevant and personal to you.

Fig: 5.2 Apple Siri and App Library



Privacy & Security

Control which apps can access your data, location, camera, and microphone, and manage safety protections. Learn more...

Location Services — 27 while using
Tracking
Calendars — 4 add only
Contacts — 4 full access
Files & Folders — 6 apps
Focus — 1 app
Health — 3 apps, 1 study

Face ID & Passcode

Manage apps using Face ID and other iPhone access settings, set up alternate appearances, and change your passcode. Learn more...

USE FACE ID FOR:
iPhone Unlock
iTunes & App Store
Contactless & Payments
Password AutoFill
Other Apps — 9 Apps

iPhone can recognize the unique, three-dimensional features of your face to allow secure access to apps and payments. About Face ID & Privacy...

Set Up an Alternate Appearance

Use Face ID With a Mask

Face ID is most accurate when it's set up for full-face recognition only. To use Face ID while wearing a mask, iPhone can recognize the unique features around the eye area to authenticate.

About Face ID & Privacy...

Use Face ID With a Mask
You won't need to wear a mask during set up.

Don't Use Face ID With a Mask
You can set up later in Settings.

Set Up Later in Settings

Fig: 5.3 Privacy Setting in Apple and Face ID & Passcode Setting

5.4 Basic Components of Android

Android is made up of different parts that work together to run your phone and its apps. Let's learn about them in a simple way:

1. Applications

These are the apps you use every day, like WhatsApp, YouTube, Camera, and Messages. Android lets you easily open, close, and switch between apps.

2. Application Framework

This is like the "manager" of the apps. It helps apps to work together and use phone features like the camera, contacts, and internet.

3. Libraries

Libraries are ready-made codes that help apps do things like play videos, show images, or connect to the internet. App developers use these to save time.

4. Android Runtime (ART)

This is the part where Android apps run. It makes sure the apps work smoothly and don't crash. Earlier, Android used something called Dalvik; now it uses ART.

5. Linux Kernel

This is the core or base of Android. It helps the phone talk to the hardware parts like the battery, screen, buttons, camera, and Wi-Fi.

Summary

- Android OS is made by Google and used in many phones like Samsung, Redmi, and Realme.
- iOS is made by Apple and used only in Apple devices like the iPhone and iPad.
- Android is open to all and easy to customize, while iOS is more secure and smooth.
- Android has millions of apps through the Google Play Store; iOS has its App Store.
- Android is built with different parts like Applications, Framework, Libraries, Runtime, and Linux Kernel. These parts help it run apps and talk to the phone's hardware.

Practical Activity 5.1

Objective:

To demonstrate the basic interface, settings, and key features of the Android OS or iOS.

Tools & Platform Needed:

Smartphone or tablet (Android or iPhone), internet access, projector or screen (optional for class demo).

Procedure:

Step 1. Divide students into two groups:

- Group A: Android users
- Group B: iOS users

Step 2. Each group will explore the following features on their respective devices:

Task	**Android**	**iOS**
Open settings and identify the OS version	Settings > About Phone	Settings > General > About
Explore system apps and permissions	App Manager	iPhone Storage / App Permissions
Connect to Wi-Fi and Bluetooth	Quick Settings or Settings > Network	Settings > Wi-Fi / Bluetooth
Explore the app store.	Google Play Store	Apple App Store
Use built-in security features.	PIN, Pattern, Face Unlock	Face ID, Passcode, Touch ID

Step 3. Students document:

- What OS version is installed
- What makes their OS unique (design, gestures, features)
- One feature they find most useful or interesting

Step 4. Groups create a short slide or poster comparing Android and iOS:

- Interface
- App store
- Customization
- Security options

Assessment

Multiple Choice Questions (MCQs)

1. What is the main job of a mobile operating system?
   a) Take photos
   b) Run games only
   c) Control how the phone works
   d) Make calls

2. Which company developed the Android OS?
   a) Apple
   b) Microsoft
   c) Samsung
   d) Google

3. iOS is the operating system used in which of the following devices?
   a) Samsung
   b) Nokia
   c) iPhone
   d) Xiaomi

4. Which app store is used to download apps on Android?
   a) Windows Store
   b) Google Play Store
   c) App Vault
   d) Apple Store

5. What is Siri in iOS?
   a) Camera app
   b) A game
   c) Voice assistant
   d) Antivirus

6. Which operating system allows more customization options?
   a) Android
   b) iOS
   c) Windows
   d) None

7. What is the base (core) of the Android OS called?
   a) BIOS
   b) Android Engine
   c) Linux Kernel
   d) OS Manager

8. Which OS is used only in Apple products?
   a) Android
   b) Symbian
   c) iOS
   d) Windows

9. What is the main feature of the iOS system?
   a) Free music
   b) High security and smooth performance
   c) Multiple SIM support

d) Access to all phones

10. Who explained the structure of the Android OS in the story?
    a) Desh Deepak
    b) Puspa
    c) Siri
    d) Raghav

Fill in the Blanks

1. The brain of the mobile phone is called the __________.
2. Android OS is developed by __________.
3. iOS is only used in __________ phones.
4. You can download Android apps from the __________.
5. Siri is a __________ assistant in iPhones.
6. Android allows users to change themes and use __________ for a personal look.
7. iOS is known for its high level of __________.
8. Android OS is based on the __________ Kernel.
9. Desh Deepak received a __________ phone on his birthday.
10. Puspa used an __________ device with iOS.

True or False

1. Android is used only in iPhones.
2. Google developed the Android OS.
3. iOS allows more customization than Android.
4. The Linux Kernel is a part of the Android OS.
5. Siri is found in Android phones.
6. Raghav is a software developer in the story.
7. Google Play Store is used to download iPhone apps.
8. Desh Deepak learned about operating systems from Puspa.
9. Android OS runs on Samsung and Xiaomi phones.
10. iOS works on all Android phones.

Short Answer Questions

1. What is the main difference between Android and iOS?
2. Why is the operating system important in a mobile phone?
3. Name two phones that commonly use the Android OS.
4. What features make iOS known for better security?
5. How did Desh Deepak learn about Android components?

Answer Key

Multiple Choice Questions

1. c, 2. d, 3. c, 4. b, 5. c, 6. a, 7. c, 8. c, 9. b, 10. a

Fill-in-the-blanks

1. processor, 2. Google, 3. Apple, 4. Google Play Store, 5. voice, 6. widgets, 7. security, 8. Linux, 9. mobile, 10. Apple

True/False questions

1. False, 2. True, 3. False, 4. True, 5. False, 6. True, 7. False, 8. True, 9. True, 10. False

Chapter-6

Web Application Protocols and Browser Security

Kabir owned a locksmith business and built his website to let customers book appointments online. Business was booming, and Kabir was thrilled. One day, Kabir received a panicked call from a customer. The customer claimed he received an email from Kabir's business asking for personal details, including personally identifiable information. Confused, Kabir contacted a web application security expert, he checked the website and realized it had been hacked. Hackers used the site to send phishing emails and steal sensitive customer information. Worse, Kabir hadn't updated the website or installed security protections, thinking a locksmith's site wouldn't be a target. The breach not only caused legal troubles but also tarnished Kabir's reputation. The irony wasn't lost—how could a locksmith, a master of physical security, neglect digital security?

With the help of a web application security expert, he rebuilt the website with robust protections:

- SSL encryption to secure customer data.
- Regular updates to software and plugins.
- Multi-factor authentication for admin access.

From then on, Kabir made it a mission to educate others: "If you lock your doors at night, you should lock your website too."

Introduction to Web Application Terminologies

In the digital age, web applications have become integral to our daily lives. These applications run on web servers and are accessed through web browsers. Web applications form the backbone of modern internet experiences, enabling users to interact with websites dynamically. Understanding basic terminologies is vital for grasping the functionality and security of web applications. Understanding the key terminologies associated with web applications is essential for anyone looking to delve into web development or cybersecurity.

6.1 Key Terminologies

- **Web Application**: A software application that runs on a web server and is accessed through a web browser.

  Examples: Gmail, Facebook, and Amazon.
- **Web Server**: A server that hosts web applications and serves web pages to clients. Examples are Apache, Nginx, and Microsoft- Internet Information Services (IIS)

- **Client and Web Client**:

  (a) Client: The end user's device that accesses the web application through a Web browser. **Examples**: Laptops, smartphones, tablets, etc.

  (b) Web Client: A web client is any application that allows users to browse the internet or interact with web services. Examples of web clients include:

  (i) Web browsers: Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, and Opera

  (ii) Mobile browsers: Chrome for Android, Safari for iOS, Samsung Internet, and Opera Mini

  (iii) File transfer clients: FileZilla, Cyberduck, WinSCP, and Transmit

  (iv) Social media apps: Facebook, Whatsapp, Twitter, Instagram, LinkedIn, and Pinterest

  (v) Video streaming client's apps: YouTube, Netflix, Amazon Prime Video, Disney+

  (vi) Cloud storage client's apps: Google Drive, Dropbox, Microsoft OneDrive, and iCloud

  (vii) Tools for remote meetings: Zoom, Google Meet, MS teams
- **Client-Server Architecture**: A model where a client with the help of a web client (e.g., a web browser) requests resources or services from a server (e.g., a web server). See Figure 6.1.
- **HTTP (Hyper Text Transfer Protocol)**: A protocol used for transmitting data between a client and a server. The protocol used for transmitting web pages over the internet.
- **Example**: When you visit a website, your browser uses HTTP to request and receive web pages.
- **HTTPS (Hyper Text Transfer Protocol Secure)**: An extension of HTTP that provides secure communication over the internet using SSL/TLS encryption.
- **Example**: Banking websites use HTTPS to secure user data.
- **HTML (Hyper Text Markup Language)**: HTML is a standard markup language for creating web pages. Web pages are built using HTML to structure content.
- **CSS (Cascading Style Sheets)**: A style sheet language used to describe the presentation of web pages. CSS controls the layout, colors, and fonts of a web page.

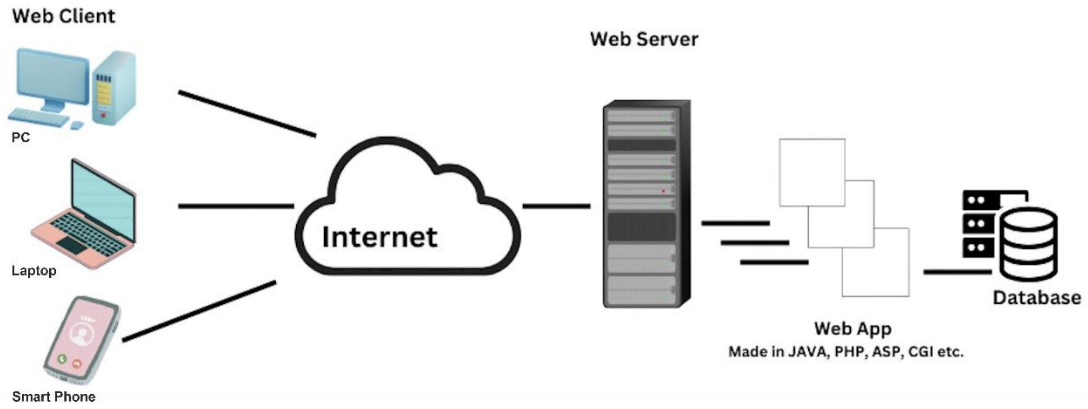


Fig: 6.1 Web Client Server Architecture

- **JavaScript**: A programming language used to create interactive effects within web browsers. **Example**: Form validations, dynamic content updates, and animations.
- **Session**: A period of interaction between a user and a web application, often maintained by cookies or tokens.
- **Cookies**: Small pieces of data stored on the client side to maintain the session state.

6.2 Basics of Web Application Protocols

Web application protocols are the rules and conventions used for communication between clients and servers. Web protocols define the rules for data exchange between web clients and servers. These protocols ensure that data is transmitted accurately and securely.

6.2.1 Common Web Application Protocols:

- **HTTP (Hyper Text Transfer Protocol):** HTTP is the standard protocol for transferring web pages. It is the foundation of data communication on the web. It defines how messages are formatted and transmitted, and how web servers and browsers respond to various commands.

  Example: When you type a URL into your browser, it sends an HTTP request to the web server, which responds with the requested web page.
- **HTTPS (Hyper Text Transfer Protocol Secure):** An extension of HTTP that includes encryption for secure communication. HTTPS adds a layer of encryption using SSL/TLS for secure communication and to encrypt data between the client and server.

  Example: Online banking transactions and login pages use HTTPS to protect sensitive information.
- **FTP (File Transfer Protocol):** A standard protocol for transferring files between a client and server over the internet.

  Example: Uploading files to a web server or downloading files from a server.
- **SMTP (Simple Mail Transfer Protocol):** A protocol for sending emails online.

  Example: Sending an email from your Gmail account to another email address.
- **WebSocket:** A protocol for full-duplex communication between clients and servers over a single, long-lived connection.

  Example: Real-time chat applications and live updates on web pages.
- **FTP (File Transfer Protocol):** Transfers files between a client and a server.
- **DNS (Domain Name System):** Resolves domain names (e.g., www.example.com) to IP addresses.
- **SMTP/IMAP/POP3:** Protocols for sending and receiving emails.

6.3 Exploring Web Application Protocols

To understand how web application protocols work, let's explore some examples in more detail:

- **DNS Resolution:**

  Example: Typing www.google.com triggers DNS resolution to find the IP address of Google's servers. See Fig: 6.2.
- **HTTP Request and Response**: When a user types a URL like http://google.com into a Web browser, the browser sends an HTTP GET request to the server. The server processes the request and responds HTTP response with an HTTP status code (e.g., 200 OK) and the requested HTML containing the requested web page.

Example: Request: GET /index.html HTTP/1.1, **Response**: HTTP/1.1 200 OK followed by the HTML content of the page. See Fig 6.2.

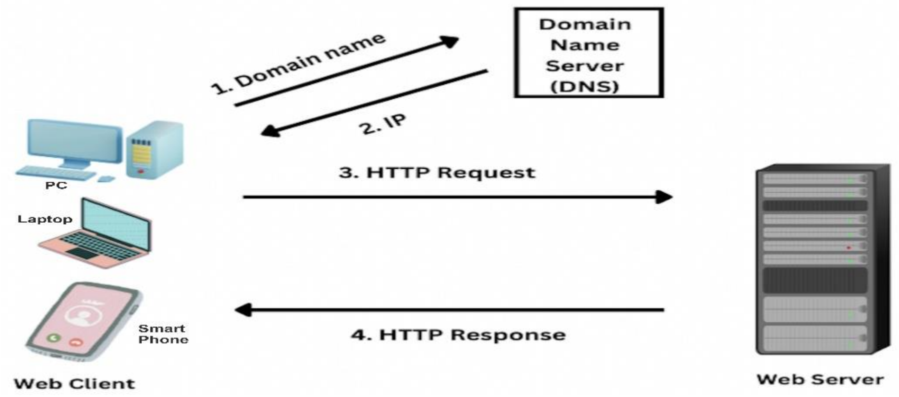


Fig 6.2: DNS, HTTP Request and HTTP Response

- **HTTPS Secure Communication**: When you visit https://example.com, your browser initiates and establishes a secure connection using SSL/TLS. This involves a handshake process where the client and server exchange encryption keys. All subsequent data transferred between the client and server is encrypted.

  Example: Online shopping websites use HTTPS to secure credit card information.
- **WebSocket Real-Time Communication**: A chat application uses WebSocket to establish a persistent connection between the client and server. This allows messages to be sent and received in real-time without the need for repeated HTTP requests.

  Example: A messaging app like WhatsApp Web uses WebSocket for instant message delivery.
- **FTP File Transfer**: To upload a file to a web server, you can use an FTP client. The client connects to the server using the FTP protocol, authenticates with a username and password, and transfers the file.

  Example: A web developer uses FTP to upload website files to a hosting server.

6.4 Connection Establishment Between Web Server and Web Client

A simplified example of establishing a connection:

Step 1: DNS Resolution-The client resolves the domain name of the server.

Step 2: TCP Handshake three-step handshake establishes a reliable connection.

- **SYN:** The client sends a synchronization request.
- **SYN-ACK:** Server acknowledges and synchronizes.
- **ACK:** The client confirms the handshake.

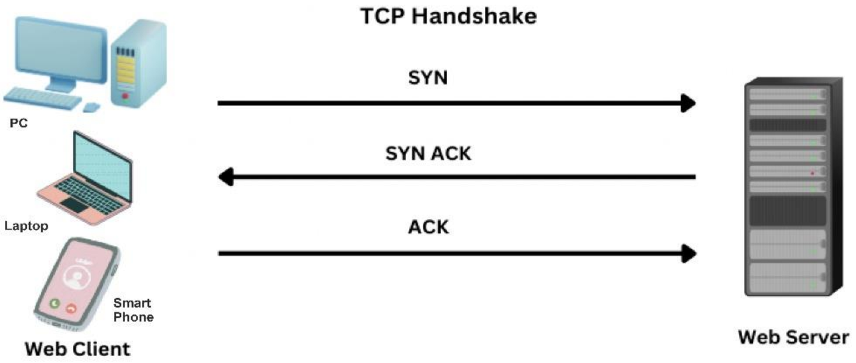


Fig: 6.3 TCP Handshake

Step 3: HTTP Request- The client sends an HTTP request to the server.

Step 4: Response- The server responds with the requested content.

Simulators like Wireshark can visualize this process

Points to remember:

- Web applications rely on client-server architecture and involve terms like HTTP, HTTPS, cookies, and sessions.
- Web application protocols, including HTTP/HTTPS, FTP, DNS, and email protocols, enable communication between web clients and servers.
- HTTP and HTTPS protocols facilitate data exchange, with HTTPS offering encryption for secure communication.
- The DNS protocol resolves domain names to IP addresses, enabling seamless access to web servers.
- A connection between a web client and server is established using DNS resolution, TCP handshake, and HTTP requests.

6.5 Browser Security

Browser security is crucial for protecting users from online threats such as malware, phishing, and data breaches. Modern browsers come with built-in security features to enhance user safety. It implements security measures to protect users.

6.5.1 Key Browser Security Features:

- **HTTPS Enforcement:** Browsers warn users when visiting non-HTTPS sites.
  Example: Google Chrome displays a "Not Secure" warning for non-HTTPS websites.
- **Warnings for Unsafe Sites:** Browsers display warnings for sites without SSL certificates.
- **Sandboxing:** Isolates web pages and plugins to prevent malicious code from affecting the entire system.
  Example: Firefox runs web content in separate processes to enhance security.
- **Secure Cookies:** Mark cookies as Secure and Http Only to protect against session hijacking.
- **Same-Origin Policy:** Prevents scripts on one site from interacting with another site's data.
  Example: JavaScript from siteA.com cannot access site B.com's cookies.
- **Phishing and Malware Protection:** Browsers block access to known phishing and malware sites.
  Example: Chrome and Firefox display warnings when users attempt to visit dangerous websites.
- **Content Security Policy (CSP):** It helps prevent cross-site scripting (XSS) and other code injection attacks by specifying which content is allowed to be loaded. Prevents cross-site scripting (XSS) by restricting the resources a page can load.
  Example: Websites can use CSP headers to restrict which scripts and resources are loaded. A CSP rule allows scripts only from trusted websites.
- **Privacy Controls:** Features like incognito mode and tracking protection help protect user privacy.
  Example: Chrome's incognito mode prevents browsing history and cookies from being stored.

6.5.2 Browser Security Settings Using Chrome and Mozilla Browser

To demonstrate browser security settings, we'll look at how to configure security and privacy settings in Google Chrome and Mozilla Firefox.

Security Setting Steps for Google Chrome

➔ **Open Security Settings:**

- ◆ Click on the three vertical dots in the top-right corner and select "Settings." (Fig: 6.4)
- ◆ Scroll down and click on "Privacy and security." (Fig: 6.5)

➔ **Configure HTTPS-Only Mode:**

- ◆ In "Security," enable "Always use secure connections" to ensure Chrome attempts to use HTTPS for all websites. (Fig: 6.6 & Fig: 6.7)

➔ **Enable Safe Browsing:**

- ◆ Under "Security," select "Enhanced protection" to enable Safe Browsing, which provides better protection against phishing and malware. (Fig: 6.8)

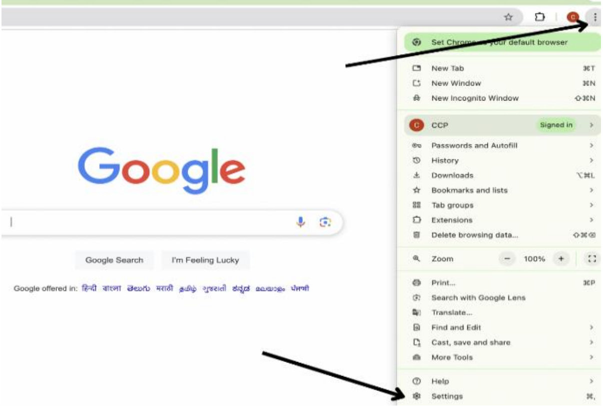


Fig: 6.4 Accessing Chrome Browser Settings

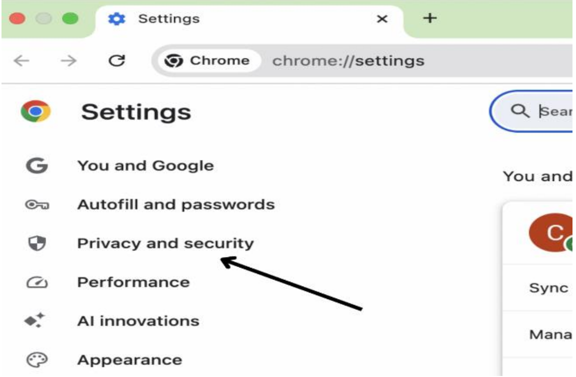
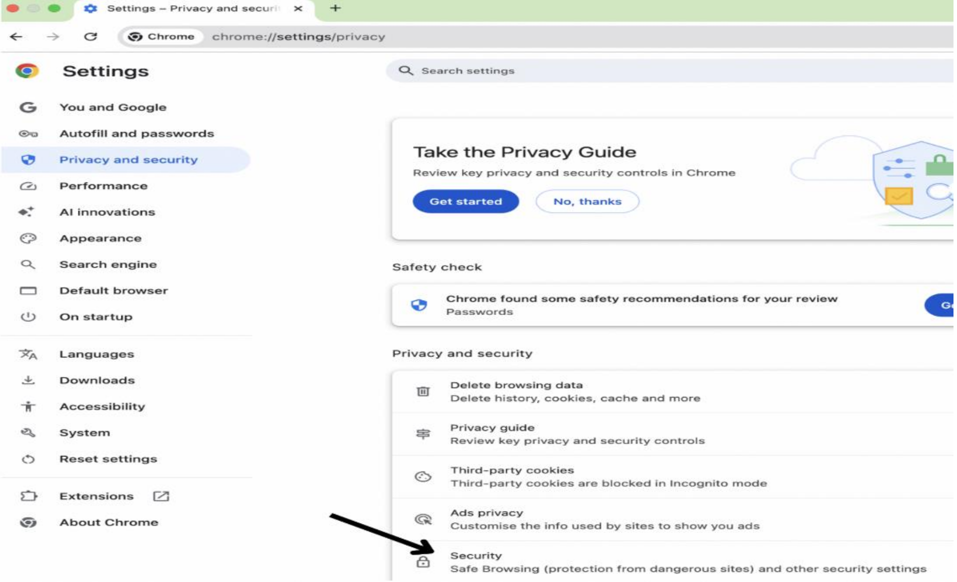


Fig: 6.5 Accessing Chrome Browser Privacy & Security



Take the Privacy Guide

Review key privacy and security controls in Chrome

Safety check

Chrome found some safety recommendations for your review
Passwords

Privacy and security

Delete browsing data
Delete history, cookies, cache and more

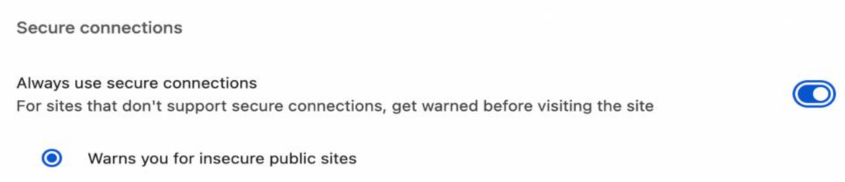
Privacy guide
Review key privacy and security controls

Third-party cookies
Third-party cookies are blocked in Incognito mode

Ads privacy
Customise the info used by sites to show you ads

Security
Safe Browsing (protection from dangerous sites) and other security settings

Fig: 6.6 Accessing Chrome Browser Security

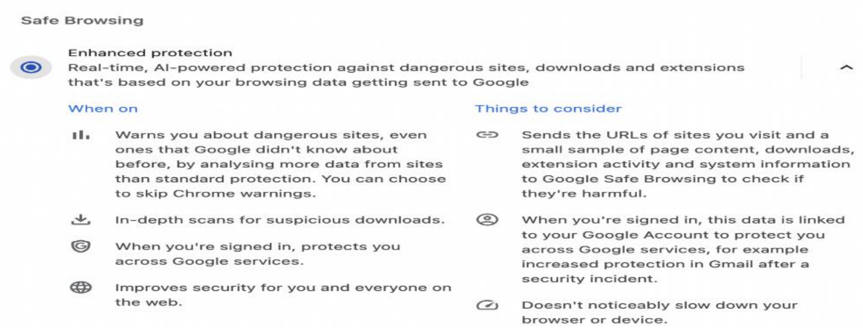


Secure connections

Always use secure connections
For sites that don't support secure connections, get warned before visiting the site

● Warns you for insecure public sites

Fig: 6.7 Enabling Secure Connections Option



Safe Browsing

● Enhanced protection
Real-time, AI-powered protection against dangerous sites, downloads and extensions that's based on your browsing data getting sent to Google

When on

- Warns you about dangerous sites, even ones that Google didn't know about before, by analysing more data from sites than standard protection. You can choose to skip Chrome warnings.
- In-depth scans for suspicious downloads.
- When you're signed in, protects you across Google services.
- Improves security for you and everyone on the web.

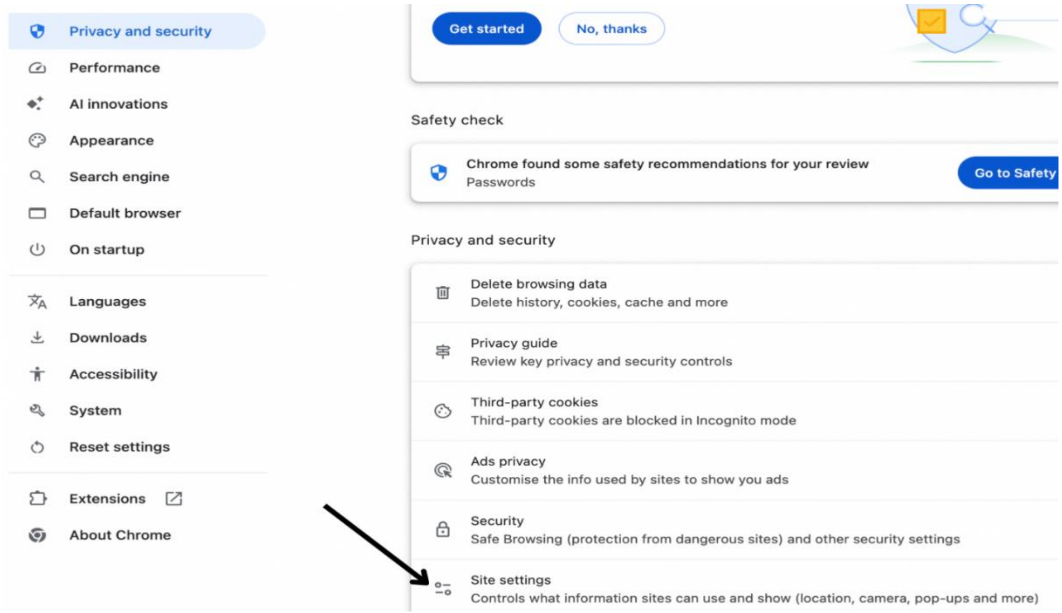
Things to consider

- Sends the URLs of sites you visit and a small sample of page content, downloads, extension activity and system information to Google Safe Browsing to check if they're harmful.
- When you're signed in, this data is linked to your Google Account to protect you across Google services, for example increased protection in Gmail after a security incident.
- Doesn't noticeably slow down your browser or device.

Fig: 6.8 Enabling Enhanced Protection Option

➔ **Manage Site Settings:**

- Click on "Site Settings" to configure permissions for location, camera, microphone, JavaScript, and more (Fig: *6.9).*



Safety check

Chrome found some safety recommendations for your review
Passwords

Privacy and security

Delete browsing data
Delete history, cookies, cache and more

Privacy guide
Review key privacy and security controls

Third-party cookies
Third-party cookies are blocked in Incognito mode

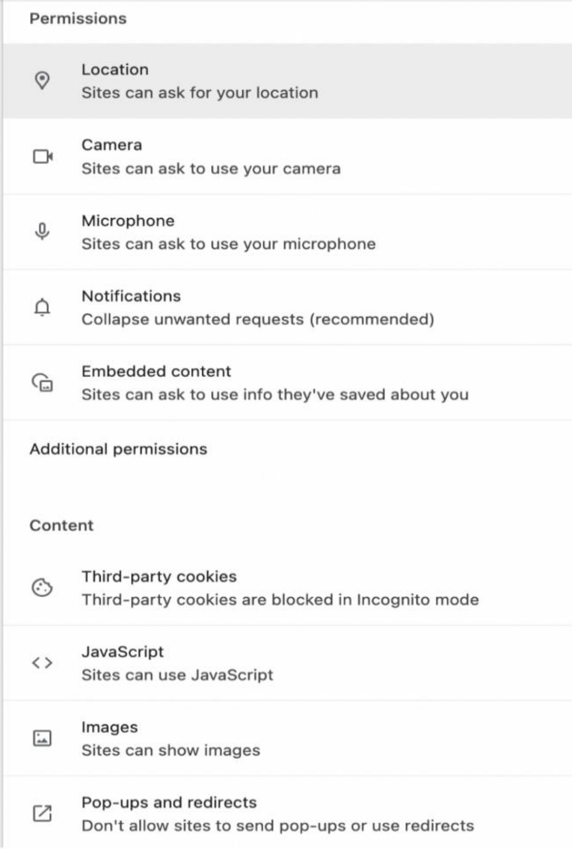
Ads privacy
Customise the info used by sites to show you ads

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site settings
Controls what information sites can use and show (location, camera, pop-ups and more)

Fig: 6.9 Accessing the Site settings option

- Adjust settings to control which sites can access these features (Fig: *6.10).*



Permissions

Location
Sites can ask for your location

Camera
Sites can ask to use your camera

Microphone
Sites can ask to use your microphone

Notifications
Collapse unwanted requests (recommended)

Embedded content
Sites can ask to use info they've saved about you

Additional permissions

Content

Third-party cookies
Third-party cookies are blocked in Incognito mode

JavaScript
Sites can use JavaScript

Images
Sites can show images

Pop-ups and redirects
Don't allow sites to send pop-ups or use redirects

Fig: 6.10 Configuring permissions for a site from Site settings

Example: To restrict JavaScript for unknown sites, one can navigate to Site Settings > JavaScript and block or allow JavaScript for specific sites.

Security Setting Steps for Mozilla Firefox:

➔ **Open Security Settings:**

- Click on the three horizontal lines in the top-right corner and select "Settings". (Fig: *6.11)*

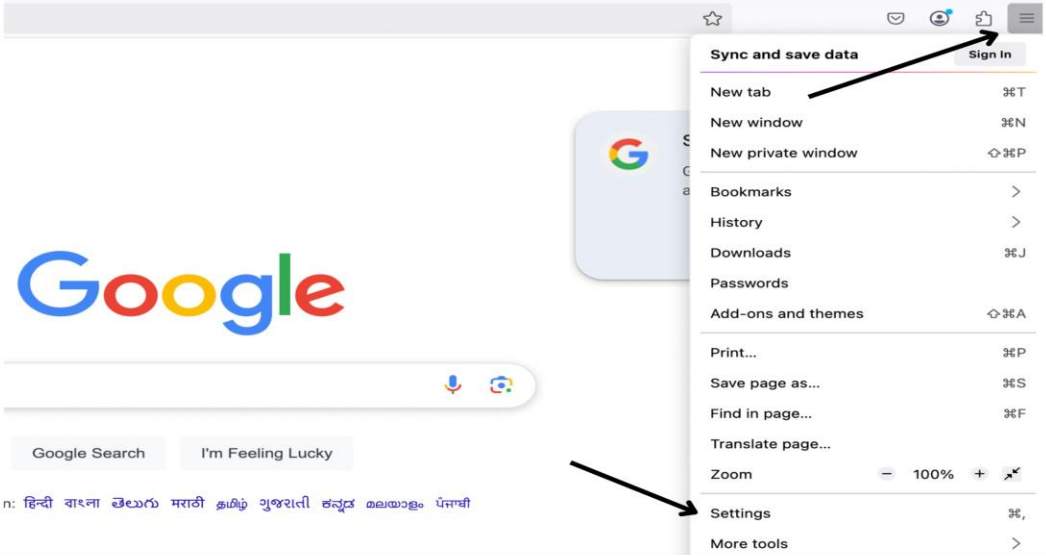
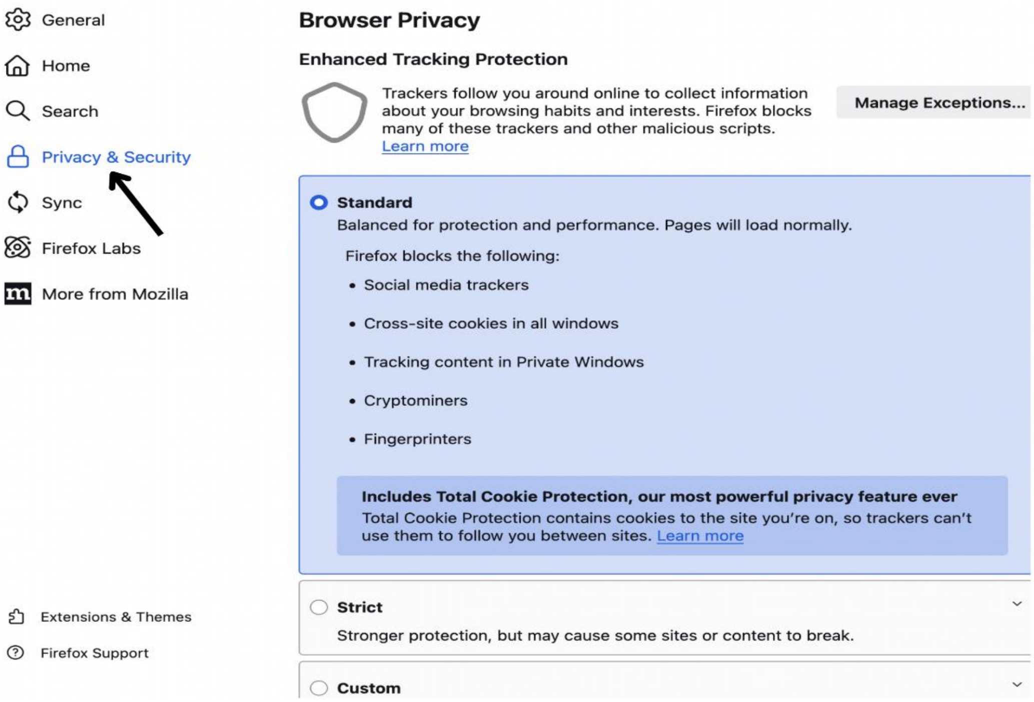


Fig: 6.11 Accessing Mozilla Firefox Web Browser Settings

- Navigate to the "Privacy & Security" tab (Fig: *6.12).*
  - Configure features like "Enhanced Tracking Protection."



Browser Privacy

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

● Standard

Balanced for protection and performance. Pages will load normally.

Firefox blocks the following:

- Social media trackers
- Cross-site cookies in all windows
- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

Includes Total Cookie Protection, our most powerful privacy feature ever

Total Cookie Protection contains cookies to the site you're on, so trackers can't use them to follow you between sites. Learn more

○ Strict

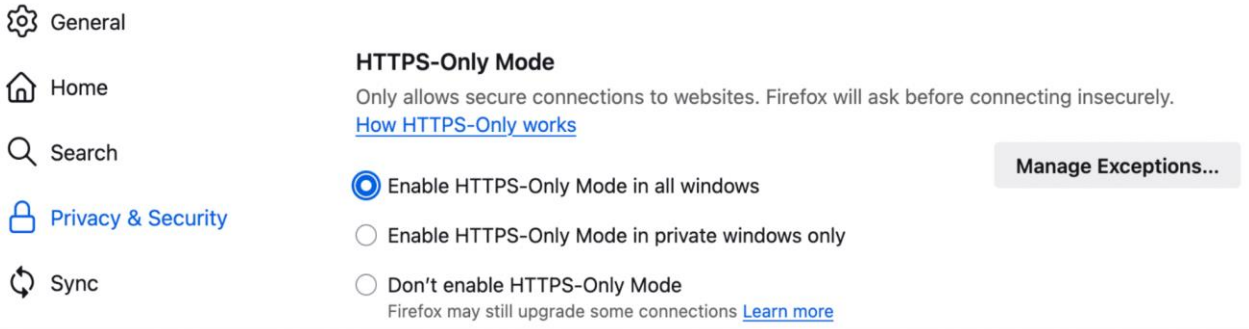
Stronger protection, but may cause some sites or content to break.

○ Custom

Fig: 6.12 Configuring Enhanced Tracking Protection in Mozilla Firefox

➔ **Enable HTTPS-Only Mode:**

◆ Scroll down to "HTTPS-Only Mode" and select "Enable HTTPS-Only Mode in all windows (Fig: *6.13).*



HTTPS-Only Mode

Only allows secure connections to websites. Firefox will ask before connecting insecurely.
How HTTPS-Only works

● Enable HTTPS-Only Mode in all windows

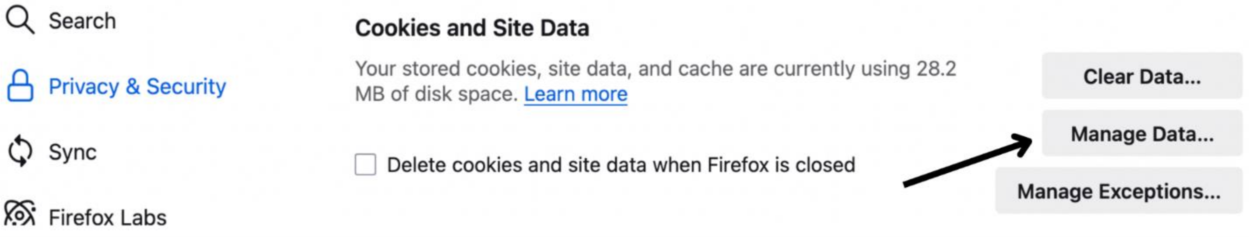
○ Enable HTTPS-Only Mode in private windows only

○ Don't enable HTTPS-Only Mode
Firefox may still upgrade some connections Learn more

Fig: 6.13 Enabling HTTPS-Only Mode in Mozilla Firefox

➔ **Managing cookie behavior:**

◆ Go to Cookies and Site Data and click on Manage Data (Fig: *6.14).*



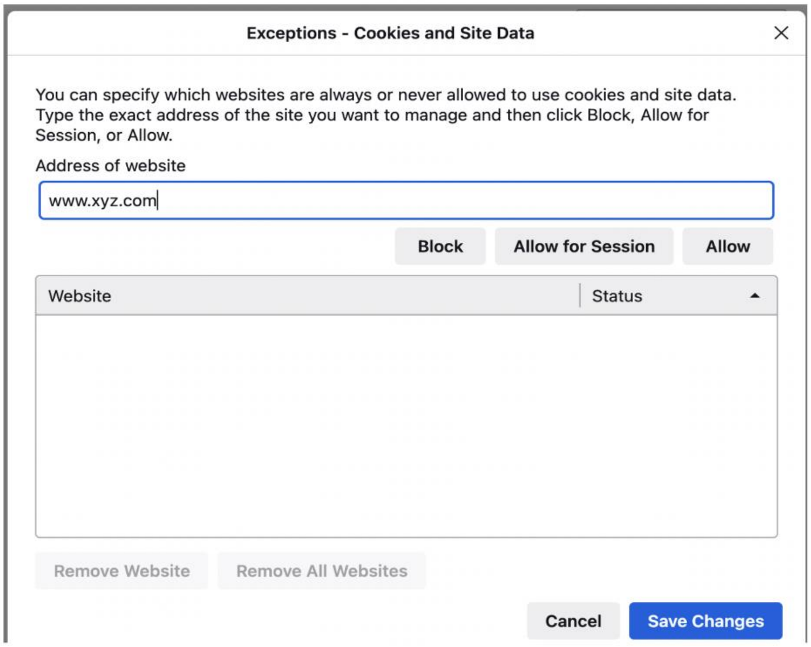
Cookies and Site Data

Your stored cookies, site data, and cache are currently using 28.2 MB of disk space. Learn more

□ Delete cookies and site data when Firefox is closed

Fig: 6.14 Accessing the Cookies & Site Data option in Mozilla Firefox

◆ Block third-party cookies for enhanced privacy (Fig: *6.15*)



Exceptions - Cookies and Site Data

You can specify which websites are always or never allowed to use cookies and site data. Type the exact address of the site you want to manage and then click Block, Allow for Session, or Allow.

Address of website

www.xyz.com

Website	Status

Fig: 6.15 Block and Allow Cookies and Site Data in Mozilla Firefox

Points to remember:

- **Browser security** features safeguard user data and privacy, such as Content Security Policy (CSP), secure cookies, same-origin policy, and site warnings.
- **Browser security** settings in Chrome and Firefox include enabling safe browsing, managing cookies, and controlling JavaScript behavior.

Practical Activity 6.1

Objective: Learners will understand how HTTPS secures communication between a client and server.

Tools & Platform Needed:

- Internet connection
- Laptop or desktop computer
- Web browser (Chrome, Firefox, etc.)

Procedure:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group available web browsers (Chrome, Firefox, etc.)

Step 3. Each group ‘ll open their preferred web browser.

Step 4. Visit a Secure Website: Enter the URL of a secure website, such as https://www.isro.gov.in.

Step 5. To inspect the HTTPS Connection, do the following:

(i) Click on the padlock icon in the browser's address bar.

(ii) Select "Connection is secure" or a similar option to view the details of the HTTPS connection.

Step 6. View the SSL/TLS Certificate:

(i) Click on "Certificate" or "View certificate" to examine the SSL/TLS certificate.

(ii) Note the certificate details, such as the issuing authority, validity period, and encryption algorithm used.

Step 7. Document Your Findings:

(i) Describe the steps taken to inspect the HTTPS connection.

(ii) Summarize the information obtained from the SSL/TLS certificate.

Each group will showcase their findings in the form of presentation slides in front of the class and discuss their importance & impact on cyber security.

List of other suggested practical activities:

- **Configuring Browser Security Settings in Google Chrome & Mozilla Firefox**: Assign each group to configure browser security settings by following the steps as discussed in the chapter.
- **Monitoring WebSocket Communication:**

(i) Open a Web Browser & visit a WebSocket Demo Site:

https://echo.websocket.org/.ws

(ii) Establish a WebSocket Connection, Send and Receive Messages

(iii) Inspect WebSocket Communication & Document the process

- **Simulating a TCP Handshake:** Visualize the TCP handshake process using a network monitoring tool-Wireshark (a network protocol analyzer).
  (i) Open Wireshark & start capturing packets.
  (ii) Open a browser and visit a website.
  (iii) Stop the packet capture in Wireshark.
  (iv) Use the filter tcp.port == 443 to focus on HTTPS traffic.
  (v) Locate a packet with SYN, and observe subsequent SYN-ACK and ACK packets.
  vi) Document the TCP handshake process with timestamps.

Summary

- Web applications rely on client-server architecture and involve terms like HTTP, HTTPS, cookies, and sessions.
- Web application protocols enable communication between web clients and servers, including HTTP/HTTPS, FTP, DNS, and email protocols.
- HTTP and HTTPS protocols facilitate data exchange, with HTTPS offering encryption for secure communication.
- The DNS protocol resolves domain names to IP addresses, enabling seamless access to web servers.
- A connection between a web client and server is established using DNS resolution, TCP handshake, and HTTP requests.
- Browser security features, such as CSP, secure cookies, same-origin policy, and site warnings, safeguard user data and privacy.
- Browser security settings in Chrome and Firefox include enabling safe browsing, managing cookies, and controlling JavaScript behavior.

ASSESSMENT

Multiple-choice questions (MCQs)

1. Which protocol is used to transfer web pages between a client and server?
   a) FTP
   b) HTTP
   c) SMTP
   d) DNS

2. What does HTTPS add to HTTP for secure communication?
   a) DNS resolution
   b) SSL/TLS encryption
   c) TCP handshake
   d) FTP transfer

3. A browser warning about an "insecure site" is most likely due to:
   a) No DNS resolution
   b) Missing SSL certificate
   c) A slow server response
   d) Invalid HTML content

4. What does the Same-Origin Policy in browsers prevent?
   a) Cross-site scripting
   b) Unauthorized cookies
   c) Access to third-party scripts
   d) Domain name resolution

5. The DNS protocol is responsible for:
    a) Encrypting web traffic
    b) Resolving domain names to IP addresses
    c) Establishing secure browser sessions
    d) Transferring files

6. Which part of the connection process involves SYN, SYN-ACK, and ACK?
    a) HTTP Request
    b) DNS Resolution
    c) TCP Handshake
    d) Content Delivery

7. Which tool is commonly used to inspect HTTP requests and responses?
    a) Chrome Developer Tools
    b) Notepad
    c) Word Processor
    d) File Explorer

8. What is the role of Content Security Policy (CSP)?
    a) Protect against DNS spoofing
    b) Restrict the loading of untrusted resources
    c) Enable cross-site scripting
    d) Enhance FTP performance

9. Which protocol is used for transferring files between client and server?
    a) HTTP
    b) FTP
    c) SMTP
    d) IMAP

10. Which browser security setting blocks cookies from unknown sources?
    a) DNS settings
    b) Privacy settings
    c) JavaScript settings
    d) Secure browsing settings

11. What is a web server?
    a) A software application that runs on a web browser.
    b) A server that hosts web applications and serves web pages.
    c) A protocol for transferring files.
    d) A programming language for web development.

12. What does HTTPS stand for?
    a) Hyper Text Transfer Protocol
    b) Secure Transfer Protocol
    c) Hyper Text Transfer Protocol Secure
    d) High Transfer Protocol Secure

13. Which feature helps prevent cross-site scripting attacks?
    a) HTTPS
    b) Sandboxing
    c) Content Security Policy (CSP)
    d) Incognito mode

14. What is a client in the context of web applications?
    a) A server that hosts applications
    b) A protocol for secure communication
    c) The end user's device accessing the web application
    d) A programming language for interactive effects

15. Which browser feature isolates web pages to prevent malicious code execution?
    a) HTTPS enforcement
    b) Sandboxing
    c) Phishing protection
    d) Privacy controls

Fill in the Blanks

1. The __________ protocol is used to encrypt web traffic, ensuring secure communication.
2. A browser session is typically maintained using __________.
3. __________ resolves domain names into IP addresses.
4. A __________ handshake establishes a connection between a client and server.
5. Secure cookies are marked as __________ and __________.
6. __________ protects against cross-site scripting attacks by restricting resources.
7. The three steps of a TCP handshake are __________, __________, and __________.
8. Chrome’s safe browsing feature can be found under the __________ menu.
9. Browsers warn users about unsafe sites when there is no __________ certificate.
10. A _______ is a software application that runs on a web server and is accessed through a web browser.
11. _______ is the protocol used for transmitting web pages over the Internet.
12. The secure version of HTTP is called _______.
13. _______ is the standard markup language used to create web pages.
14. Browsers use _______ to isolate web pages and prevent malicious code execution.
15. _______ is a style sheet language used to describe the presentation of web pages.

True/False Questions

1. HTTPS uses FTP to encrypt web traffic.
2. Cookies help maintain user sessions on web applications.
3. DNS resolves IP addresses into domain names.
4. Secure cookies can be accessed by JavaScript.
5. A TCP handshake consists of four steps.
6. CSP stands for Client Security Policy.
7. The same-origin policy restricts cross-site interactions.
8. Firefox has built-in features for blocking third-party cookies.
9. Browsers do not enforce security for scripts from untrusted domains.
10. FTP is used for real-time communication between the client and the server.
11. Sandboxing helps prevent malicious code from affecting the entire system.
12. SMTP is a protocol for transferring files.
13. JavaScript is used to create interactive effects within web browsers.
14. Safe Browsing blocks access to known phishing and malware sites.
15. CSS is used to structure content on web pages.

Short Answer Questions

1. Describe the purpose of HTTPS and how it differs from HTTP.
2. How does FTP facilitate file transfers between a client and server?
3. Explain the concept of sandboxing in browser security.
4. What is the role of JavaScript in web development?
5. What is the main purpose of the HTTPS protocol?
6. What role does the DNS protocol play in web applications?
7. What is a web server, and what role does it play in web applications?

8. Mention two features of browser security settings.
9. What is the significance of the Same-Origin Policy in web browsers?
10. Name one tool to inspect HTTP requests and responses.

Long Answer Questions

1. Explain the process of connection establishment between a web client and a server, detailing DNS resolution, TCP handshake, and HTTP request/response.
2. Discuss browser security measures like Content Security Policy (CSP), secure cookies, and the same-origin policy. Provide examples.
3. Explain the similarities and differences in features like enhanced tracking protection, safe browsing, and cookie management.
4. Discuss the various web application protocols (HTTP, HTTPS, FTP, SMTP, WebSocket) and their roles in web communication. Provide examples of each protocol in use.
5. Explain the importance of browser security features such as HTTPS enforcement, sandboxing, and phishing protection. How do these features protect users from online threats?

Answer Key

Multiple Choice Questions

1. b, 2. b, 3. b, 4. c, 5. b, 6. c, 7. a, 8. b, 9. b, 10. b, 11. b, 12. c, 13. c, 14. c, 15. b

Fill-in-the-blanks

1. HTTPS, 2. Cookies, 3. DNS, 4. TCP, 5. Secure, HttpOnly, 6. Content Security Policy (CSP), 7. SYN, SYN-ACK, ACK, 8. Settings, 9. SSL, 10. Web application, 11. HTTP, 12. HTTPS, 13. HTML, 14. Sandboxing, 15. CSS

True/False questions

1. False, 2. True, 3. False, 4. False, 5. False, 6. False, 7. True, 8. True, 9. False, 10. False, 11. True, 12. False, 13. True, 14. True, 15. False

Chapter-7

Social Media and Its Security

Riya, an ambitious high school student preparing for board exams, loved using social media to chat, post pictures, and even follow educational pages. One evening, she received a direct message with a link promising free premium study material. Excited, she clicked the link and logged in using her social media credentials. A message popped up: "Error: Try again later." Assuming it was a glitch, Riya moved on. The following day, her phone buzzed nonstop. Her account had been hacked, posting inappropriate content and messaging her teachers. Embarrassed and scared, Riya found her password had changed. Her father acted swiftly, contacting the cyber cell. The hackers had stolen her identity and attempted financial fraud using her linked accounts. Thankfully, the damage was controlled due to quick action.

This was an eye-opener for Riya and her family. Cyber officers advised:

- Enable Two-Factor Authentication for extra security.
- Avoid clicking suspicious links, even from trusted contacts.
- Use strong, unique passwords and update them regularly.
- Review and update privacy settings often.

Riya shared her experience in a school seminar, teaching classmates the importance of cyber safety. She learned that vigilance in the digital world is as crucial as in real life. In this chapter, we will explore the various types of social media, their advantages and disadvantages, security issues, and ways to enhance privacy and security.

7.1 Introduction to Social Media

Social media refers to digital platforms that enable users to create, share, and interact with content and connect with others worldwide. It has transformed the way we communicate, share information, access information, connect with others globally, and express ourselves (Figure 7.2). It encompasses various platforms, each serving distinct purposes and catering to diverse audiences. Here are some of the main types of social media:

Fig: 7.1 The world of social media

7.1.1 Types of Social Media

Social media platforms can be broadly classified into the following categories:

- **Social Networking Sites:** These are digital platforms where users can create profiles, connect with friends, family, and other contacts. We share updates and engage in conversations.

  Examples: Facebook from Meta

Fig: 7.2 Facebook Logo

- **Microblogging Platforms:** These platforms allow users to post and share short updates, news, and ideas in real-time, often limited by character count.

  Examples: X platform-previously known as Twitter, Tumblr

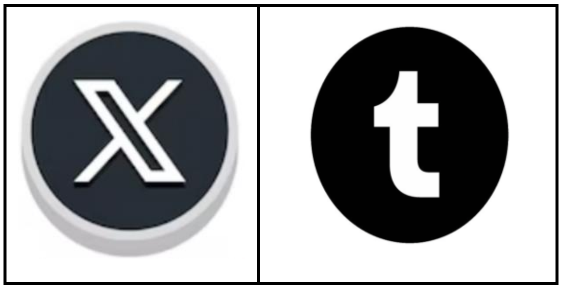


Fig: 7.3 Logo of X and Tumblr

- **Photo and Video Sharing Platforms:** These platforms are focused on discovering, creating, and sharing visual content like photos, videos, and live streams.

  Examples: Instagram, Snapchat, YouTube

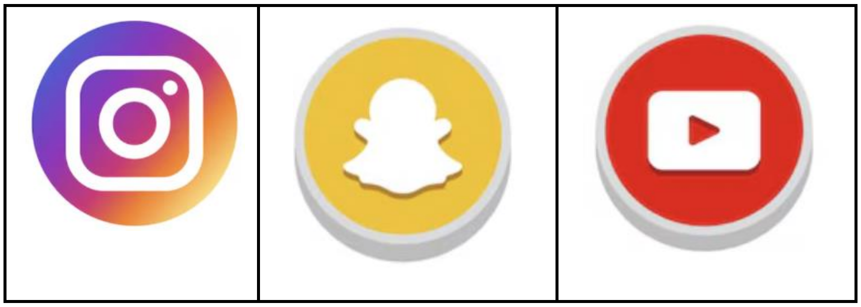


Fig: 7.4 Logo of Instagram, Snapchat, and Youtube

- **Discussion Forums:** These are online spaces and platforms where users can start and engage in asking questions, discussing topics, and sharing knowledge on various topics

  Examples: Reddit, Quora, Stackoverflow

Fig: 7.5 Logo of Reddit, Quora, and Stackoverflow

- **Content Curation Sites:** These platforms allow users to collect, organize, and share content from the web.

  Examples: Pinterest, Flipboard.

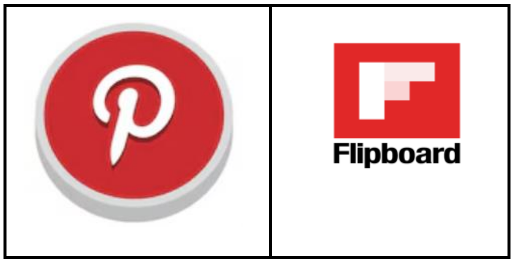


Fig: 7.6 Logo of Pinterest and Flipboard

- **Messaging and Communication Apps:** These platforms enable instant messaging, voice (audio), and video communication.

  Examples: WhatsApp, Telegram, Messenger.

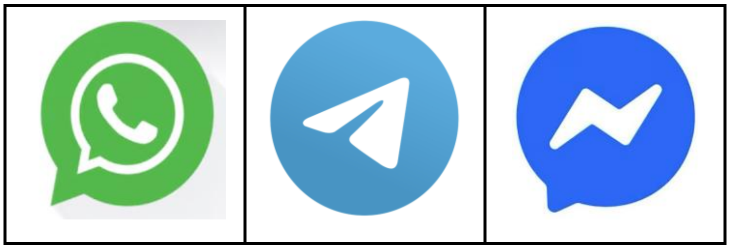


Fig: 7.7 Logo of WhatsApp, Telegram & Messenger

- **Professional Networking Sites:** These platforms are designed for professional interactions, showcasing skills, job searching, and business networking with professionals.

  Examples: LinkedIn, Xing

Fig: 7.8 Logo of LinkedIn and Xing

7.2 Advantages and Disadvantages of Social Media

7.2.1 Advantages of Social Media

- **Endless Connectivity**: It enables people to connect with friends and family, regardless of geographical barriers. It facilitates communication with people worldwide.
  - **For example,** Facebook allows users to stay in touch with distant relatives.
- **Rapid Information Sharing**: It facilitates the rapid spread of information and news. It provides quick access to news, trends, and educational content.
  - **Example:** X platform (previously known as Twitter) is often used to share breaking news and real-time updates.
- **Marketing and Business Growth using Branding**: It is an effective platform for businesses to promote their products and services. It provides businesses with a platform to reach and engage with their target audience.
  - **Example:** Instagram allows businesses to showcase their products and interact with customers.
- **Community and People Network Building**: It encourages collaboration, support, and help among like-minded individuals in forming communities and support networks.
  - **Example:** Reddit communities (subreddits) bring together people with common interests.
- **Variety of Entertainment**: These platforms offer engaging content and a variety of entertainment options, including videos, memes, live streams, and games.
  - **For example,** YouTube provides endless video content for entertainment and education.
- **Social Awareness Campaigns**: It helps in amplifying social causes and awareness initiatives and raises the voice of the common public.
  - **Example:** Social Media like X, YouTube, Facebook provide a platform for social campaigns for any noble cause. It can be started by anyone.

Fig: 7.9 Privacy concerns of all types of social media

7.2.2 Disadvantages of Social Media

- **Privacy Concerns:** There is a risk that an individual's personal information on social media can be exposed to unauthorized users or misused. It is happening day by day (Figure 7.10).
  - **Example:** Facebook data breaches have raised concerns about user privacy.
- **Getting misinformation:** There is a chance of spreading fake news, misleading content, false information, and rumors through social media.
  - **Example:** Fake news on social media platforms can mislead users and cause panic.
- **Victims of Cyberbullying:** Harassment or abuse in online spaces is common these days. Social media users may be subjected to harassment and bullying.
  - **Example:** X platform (previously known as Twitter) users sometimes face harassment through tweets and direct messages.

- **Highly Addictive:** Excessive use of social media can lead to addiction and negatively impact mental health. It can lead to dependency and reduced productivity.
  - ○ **Example:** Continuous scrolling on Instagram can lead to reduced productivity and anxiety.
- **Time Consumption:** The purposeless use of social media can significantly distract from important tasks. It consumes a significant amount of time that could be used for productive activities.
  - ○ **Example:** Spending hours on YouTube watching videos.
- **Mental Health Issues**: The experts say that exposure to harmful content on social media may cause anxiety, depression, or low self-esteem.

💡**Points to remember:**

- **Social media** refers to platforms for creating, sharing, and interacting with content and connecting globally.
- **Types of social media include:**
  - ○ Social networking sites (e.g., Facebook, LinkedIn).
  - ○ Microblogging platforms (e.g., Twitter, Tumblr).
  - ○ Photo and video sharing platforms (e.g., Instagram, Snapchat).
  - ○ Content sharing and curation platforms (e.g., YouTube, Pinterest).
  - ○ Discussion forums (e.g., Reddit, Quora).
  - ○ Messaging apps (e.g., WhatsApp, Telegram).
  - ○ Professional platforms (e.g., LinkedIn).
- **Advantages of social media:**
  - ○ Endless connectivity and rapid information sharing.
  - ○ Marketing and Business growth using branding
  - ○ Provides entertainment, community, and people network building
- **Disadvantages of social media:** Privacy Concerns, Risks include addiction, getting misinformation, victims of cyberbullying, wastage of time & mental health impacts.

7.3 Security Issues and Challenges While Using Social Media

Social media platforms face numerous security issues and challenges that users should be aware of:

- **Account Hacking:** Unauthorized access to user accounts and sensitive personal data. It can lead to identity theft and misuse of personal information.
  - ○ **Example:** Hackers sometimes gain access to Instagram and X accounts and post inappropriate content.
- **Phishing Attacks and Impersonation**: Phishing attacks are fraudulent attempts to obtain sensitive information by pretending to be trustworthy. Impersonation is the creation of fake profiles to deceive or scam others.
  - ○ **Example:** Social media users might receive Fake emails or messages that trick users into providing Fake login pages on Instagram and other social media platforms to steal login credentials and other personal details.
- **Malware and Viruses:** Malicious software that can infect devices and compromise data security. It can be spread by sharing malicious links or scams through messages.
  - ○ **Example:** Clicking on a malicious link shared on Twitter that downloads malware onto the device.
- **Data Breaches:** Sometimes, social media platforms fail to protect user data, allowing intruders or hackers to gain unauthorized access to large volumes of user information.

  - **Example:** Data breaches on LinkedIn exposing user email addresses and Passwords. Facebook's Cambridge Analytica scandal.
- **Invasion of Privacy of User by Social Media Itself:** Many social media platforms track user behavior for targeted advertising.
- **Inappropriate Content and Spreading Hatred:** Social media can be a medium of inappropriate content for children or the community. It might lead to exposure to harmful or explicit material. Sometimes it becomes impossible for security experts as well to trace the origin of such messages and break down the chain of spreading.

7.3.1 Tips for safe and secure use of Social Media

- **Use Strong Passwords:** Create strong passwords combined with letters, numbers, and special characters. Avoid using easily guessed information like birthdays, mobile numbers etc.
- **Enable Two-Factor Authentication (2FA):** Adds an extra layer of security by requiring a verification code on personal email and mobile.
- **Be Cautious about sharing on social media:** Twice think of its consequences before sharing anything online on social media, and Avoid oversharing details like your address, phone number, or location.
- **Review social media app permissions before use:** Ensure that security and privacy settings and app permission are enabled before using a particular social media platform. It restricts access to unnecessary data and features.

7.4 Platform-Specific Privacy and Security on Social Media

Users can take proactive steps to enhance their privacy and security on social media platforms like Facebook, Instagram, and X:

Facebook

On Facebook platform navigate to Settings & Privacy to enable, review, manage, and control the following options one by one:

➔ Enable Two-Factor Authentication (2FA):

  - Go to Settings & Privacy > Settings > Password and security.
  - Under Two-Factor Authentication, click "Edit" and follow the instructions to set it up *(Fig: 7.10).*

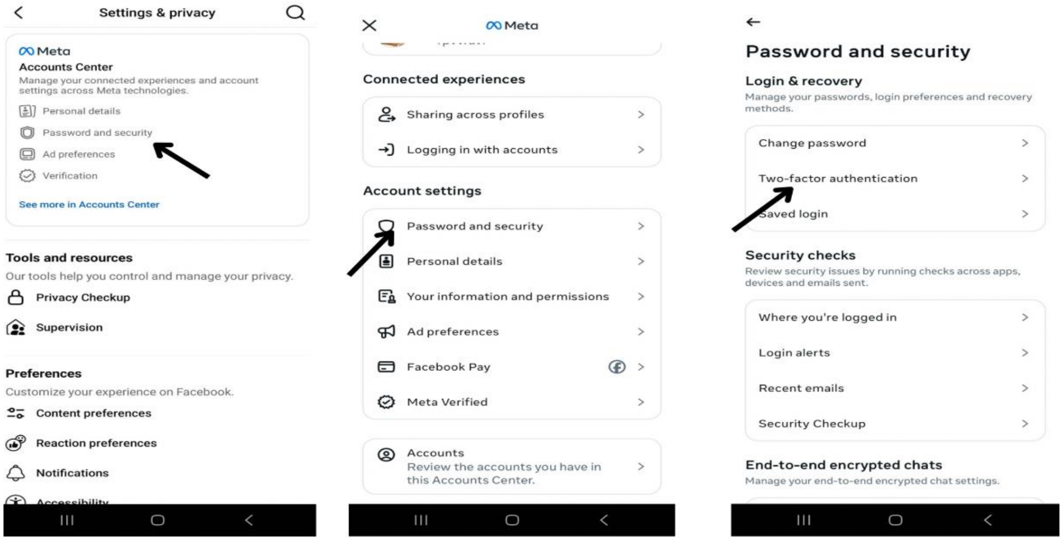
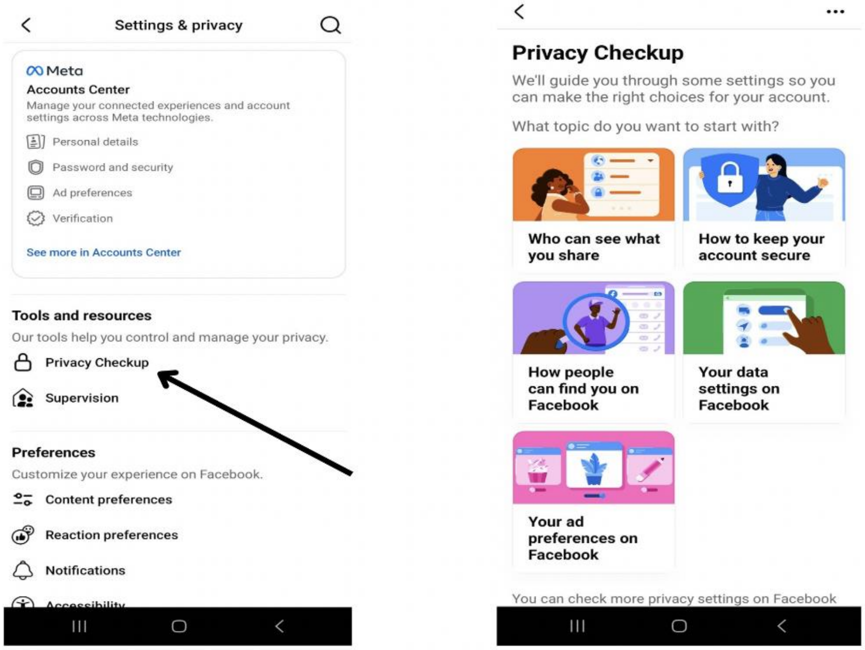


Fig:7.10 Enable Two-Factor Authentication in Facebook Apps

- ➔ Review Privacy Settings:
  - ◆ Go to Settings & Privacy > Privacy Checkup.
  - ◆ Review and control who can see your posts, profile information, and manage your block list *(Fig: 7.11)*.



Manage your connected experiences and account settings across Meta technologies.

Our tools help you control and manage your privacy.

Customize your experience on Facebook.

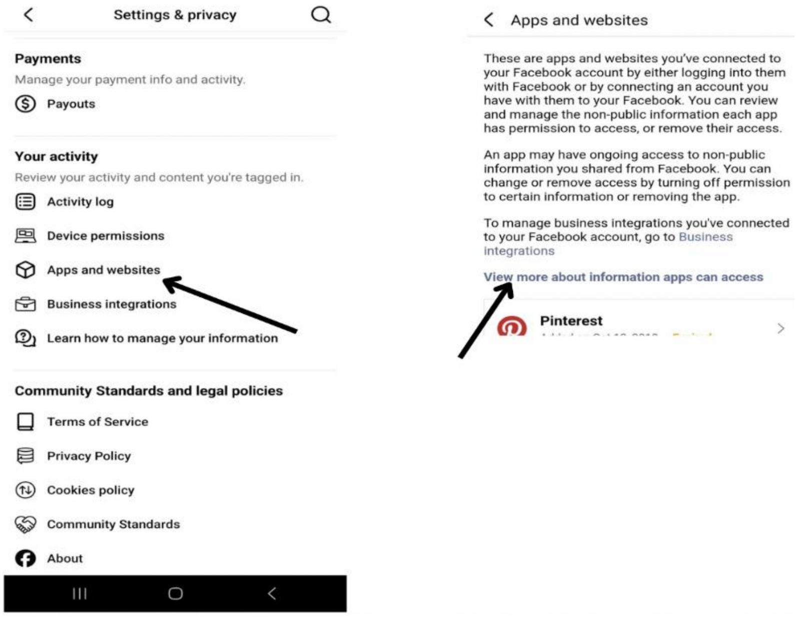
We'll guide you through some settings so you can make the right choices for your account.

What topic do you want to start with?

You can check more privacy settings on Facebook

Fig: 7.11 Privacy Checkup in Facebook App

- ➔ Manage App Permissions:
  - ◆ Go to Settings & Privacy > Settings > Apps and Websites.
  - ◆ Review and remove any apps or websites that have access to your Facebook account *(Fig: 7.12)*.



Manage your payment info and activity.

Review your activity and content you're tagged in.

These are apps and websites you've connected to your Facebook account by either logging into them with Facebook or by connecting an account you have with them to your Facebook. You can review and manage the non-public information each app has permission to access, or remove their access.

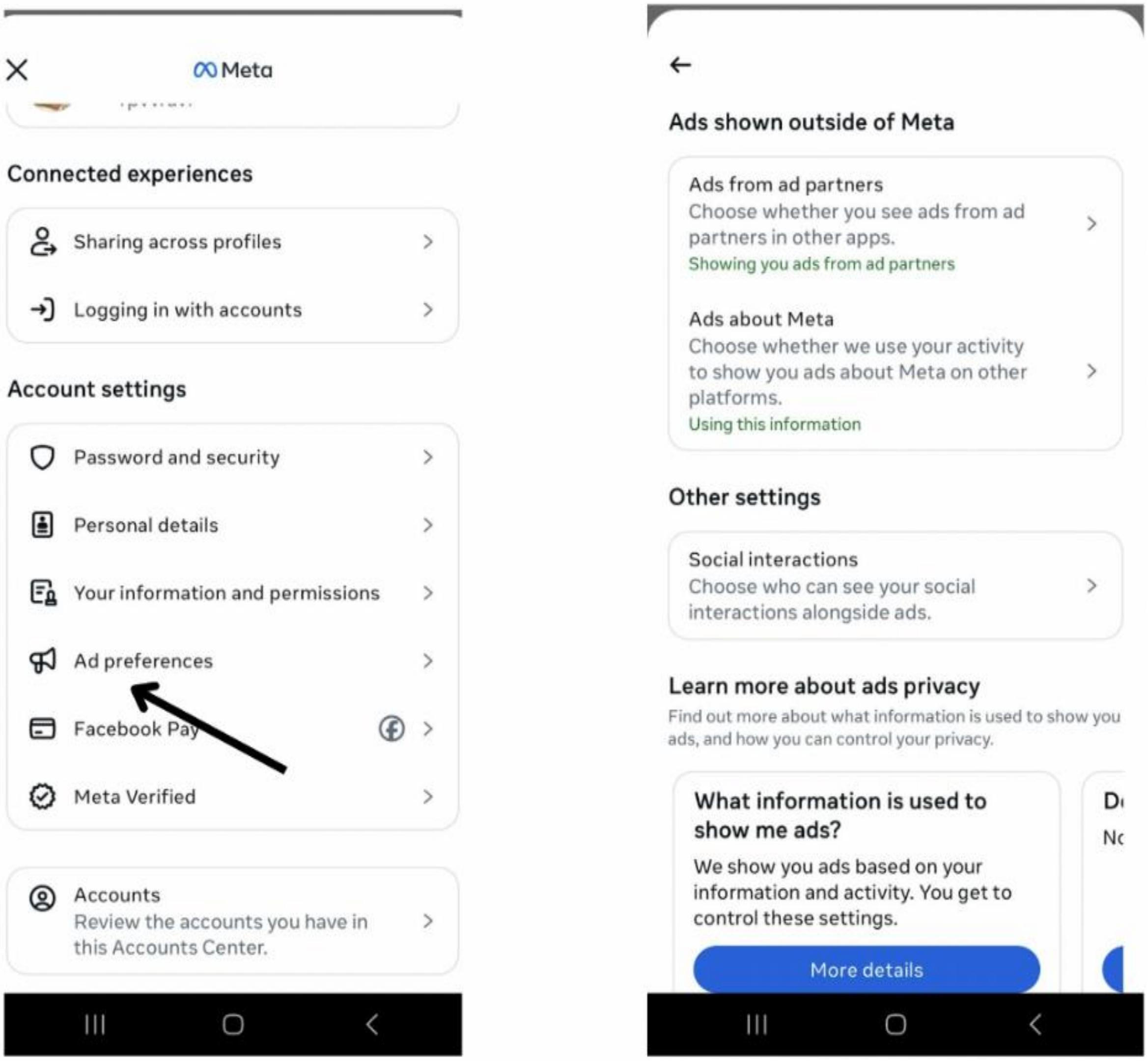
An app may have ongoing access to non-public information you shared from Facebook. You can change or remove access by turning off permission to certain information or removing the app.

To manage business integrations you've connected to your Facebook account, go to Business integrations

Fig: 7.12 Managing other apps permissions in Facebook App

➔ Control Ad Preferences:

- Go to Settings & Privacy > Settings > Ads.
- Adjust your ad preferences and limit how your data is used for advertising. (Fig: *7.13)*



Meta

Connected experiences

Sharing across profiles >

Logging in with accounts >

Account settings

Password and security >

Personal details >

Your information and permissions >

Ad preferences >

Facebook Pay >

Meta Verified >

Accounts
Review the accounts you have in this Accounts Center. >

Ads shown outside of Meta

Ads from ad partners
Choose whether you see ads from ad partners in other apps.
Showing you ads from ad partners >

Ads about Meta
Choose whether we use your activity to show you ads about Meta on other platforms.
Using this information >

Other settings

Social interactions
Choose who can see your social interactions alongside ads. >

Learn more about ads privacy
Find out more about what information is used to show you ads, and how you can control your privacy.

What information is used to show me ads?
We show you ads based on your information and activity. You get to control these settings.

More details

e

Fig: 7.13 Controlling Ads preferences in Facebook App

Instagram

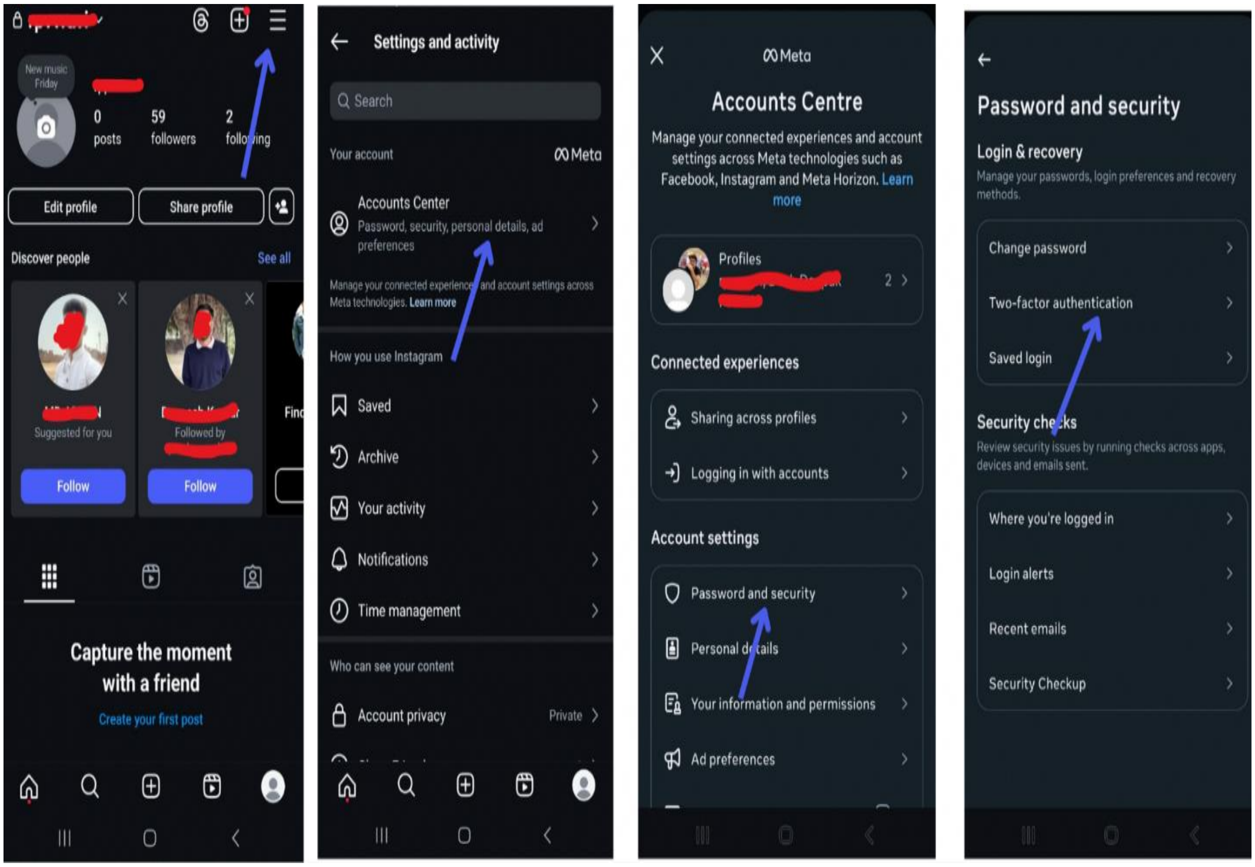
On Instagram platform navigate to Settings and enable, review, manage, and control the following options one by one:

➔ Enable Two-Factor Authentication (2FA):

- Go to Settings and Activity> Accounts Center > Password and Security> Two-Factor Authentication.
- Tap "Get Started" and follow the instructions to set it up. (Fig: *7.14)*

➔ Make Your Account Private:

- Go to Settings and Activity>Account Privacy.
- Toggle on "Private Account" to limit who can see your posts. (Fig: *7.15)*
- Use the Blocked Accounts feature to prevent unwanted interactions. (Fig: *7.15)*
- Limit app permissions and monitor third-party app access. (Fig: *7.16)*



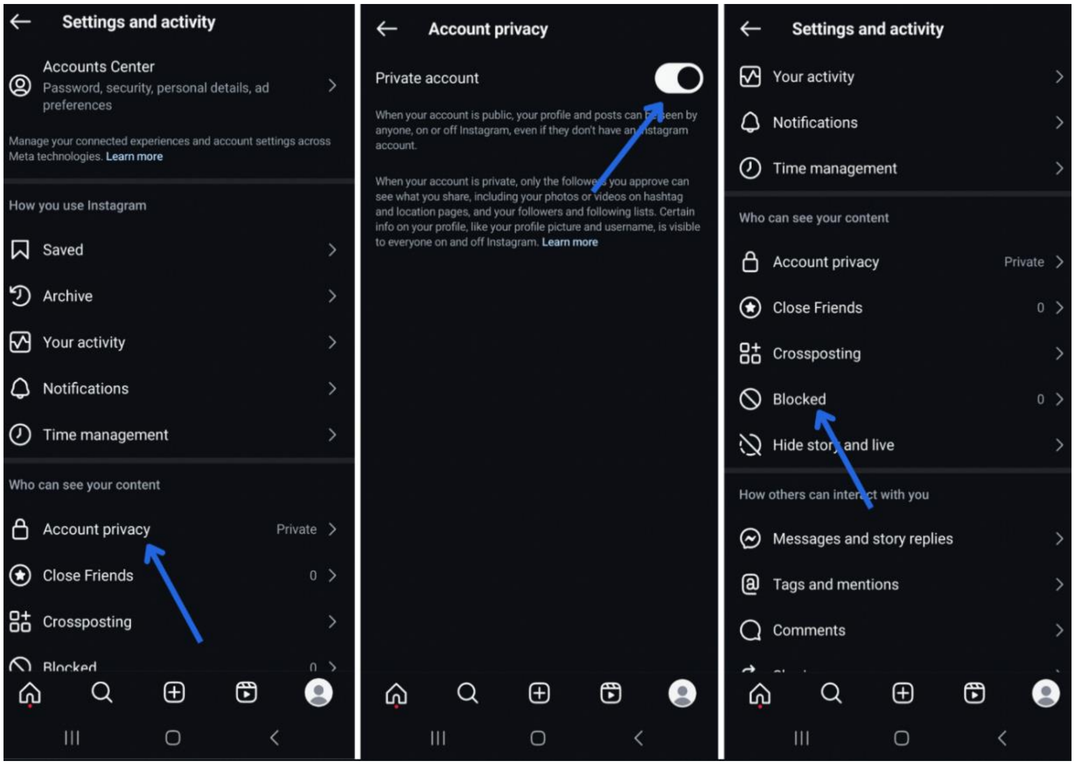
Manage your connected experiences and account settings across Meta technologies. Learn more

Manage your connected experiences and account settings across Meta technologies such as Facebook, Instagram and Meta Horizon. Learn more

Manage your passwords, login preferences and recovery methods.

Review security issues by running checks across apps, devices and emails sent.

Fig: 7.14 Enable Two-Factor Authentication in the Instagram App



Manage your connected experiences and account settings across Meta technologies. Learn more

When your account is public, your profile and posts can be seen by anyone, on or off Instagram, even if they don't have an Instagram account.

When your account is private, only the followers you approve can see what you share, including your photos or videos on hashtag and location pages, and your followers and following lists. Certain info on your profile, like your profile picture and username, is visible to everyone on and off Instagram. Learn more

Fig: 7.15 Making Instagram account private and accessing the Blocked feature

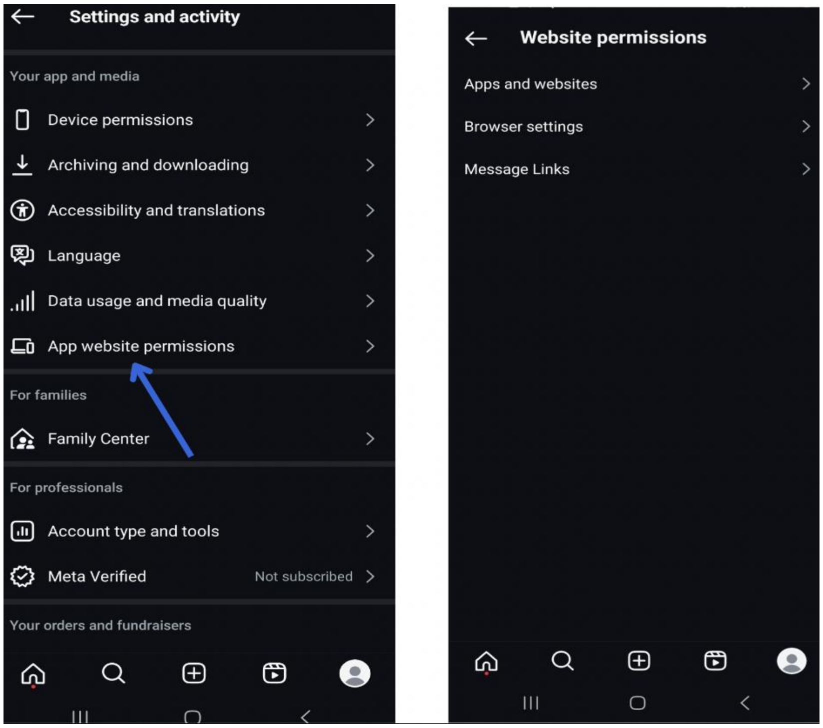
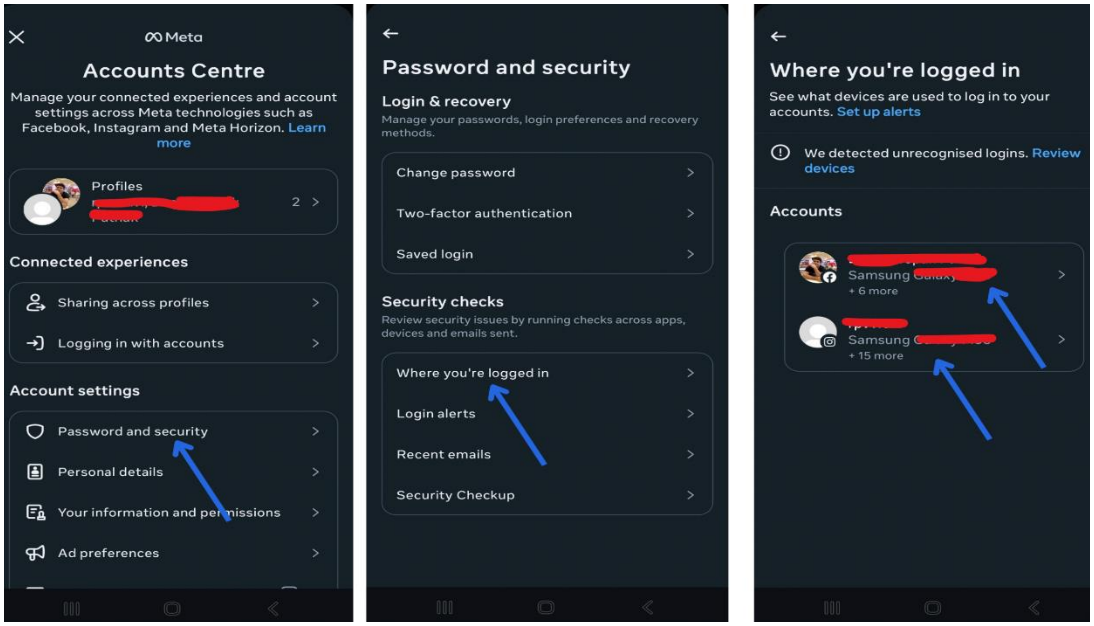


Fig: 7.16 App website permissions while using the Instagram app

➔ Review Account Activity:

- Go to Settings and Activity>



Manage your connected experiences and account settings across Meta technologies such as Facebook, Instagram and Meta Horizon. Learn more

Manage your passwords, login preferences and recovery methods.

Review security issues by running checks across apps, devices and emails sent.

See what devices are used to log in to your accounts. Set up alerts

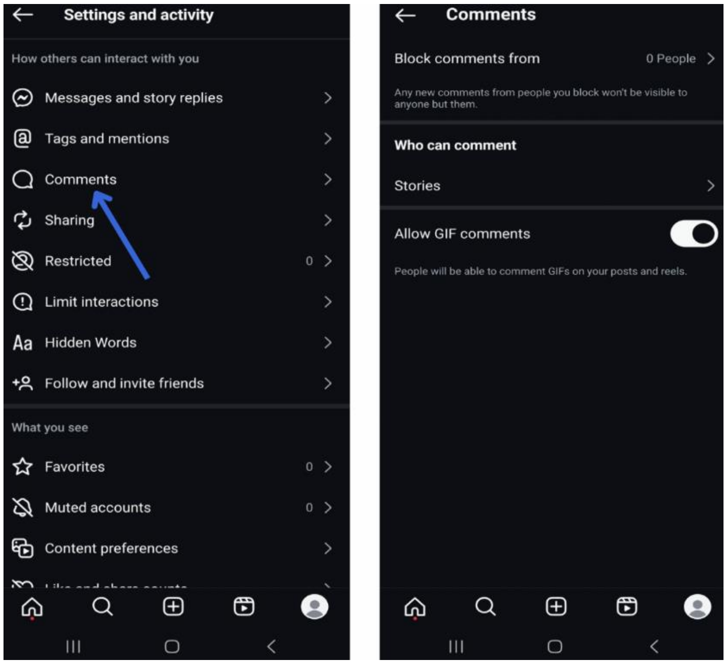
We detected unrecognised logins. Review devices

Fig: 7.17 Review account activity in the Instagram app

- Tap Accounts Center
- Tap Password and security
- Tap Where you're logged in
- Review and log out of any suspicious devices or locations. (*Figure 7.18*)

➔ Manage Comment Controls:

- Go to Settings and Activity>Comments.
- Filter out offensive comments and block specific users from commenting on your posts (Fig: *7.18).*



Comments

Block comments from 0 People

Any new comments from people you block won't be visible to anyone but them.

Who can comment

Stories

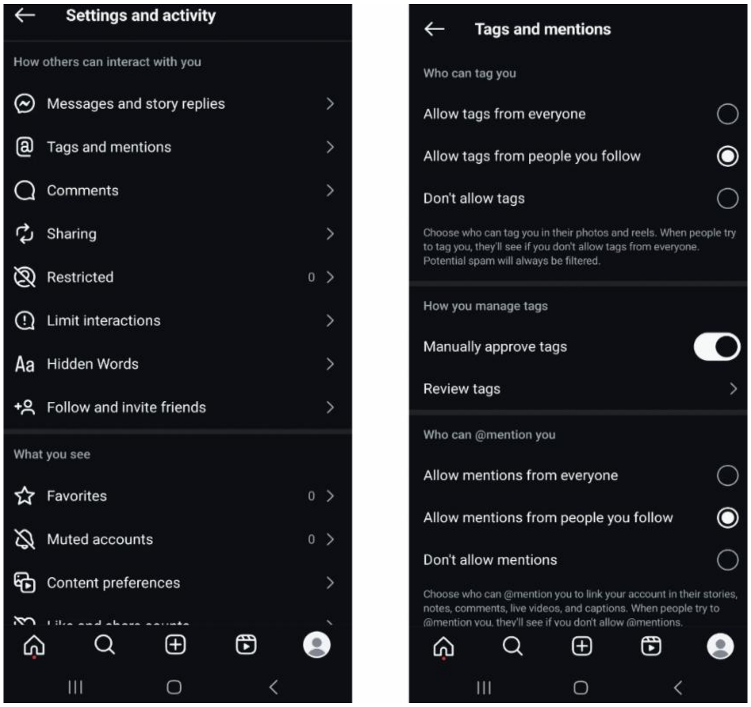
Allow GIF comments

People will be able to comment GIFs on your posts and reels.

Figure 7.18 Manage comment control in the Instagram app

➔ Manage Tags and mentions:

- Go to Settings and Activity>Tags and mentions.
- Allow and Don't allow tags and mentions (Fig: *7.19)*



Tags and mentions

Who can tag you

○ Allow tags from everyone

● Allow tags from people you follow

○ Don't allow tags

Choose who can tag you in their photos and reels. When people try to tag you, they'll see if you don't allow tags from everyone. Potential spam will always be filtered.

How you manage tags

Manually approve tags

Review tags

Who can @mention you

○ Allow mentions from everyone

● Allow mentions from people you follow

○ Don't allow mentions

Choose who can @mention you to link your account in their stories, notes, comments, live videos, and captions. When people try to @mention you, they'll see if you don't allow @mentions.

Fig: 7.19 Manage Tags and mentions in the Instagram app

WhatsApp

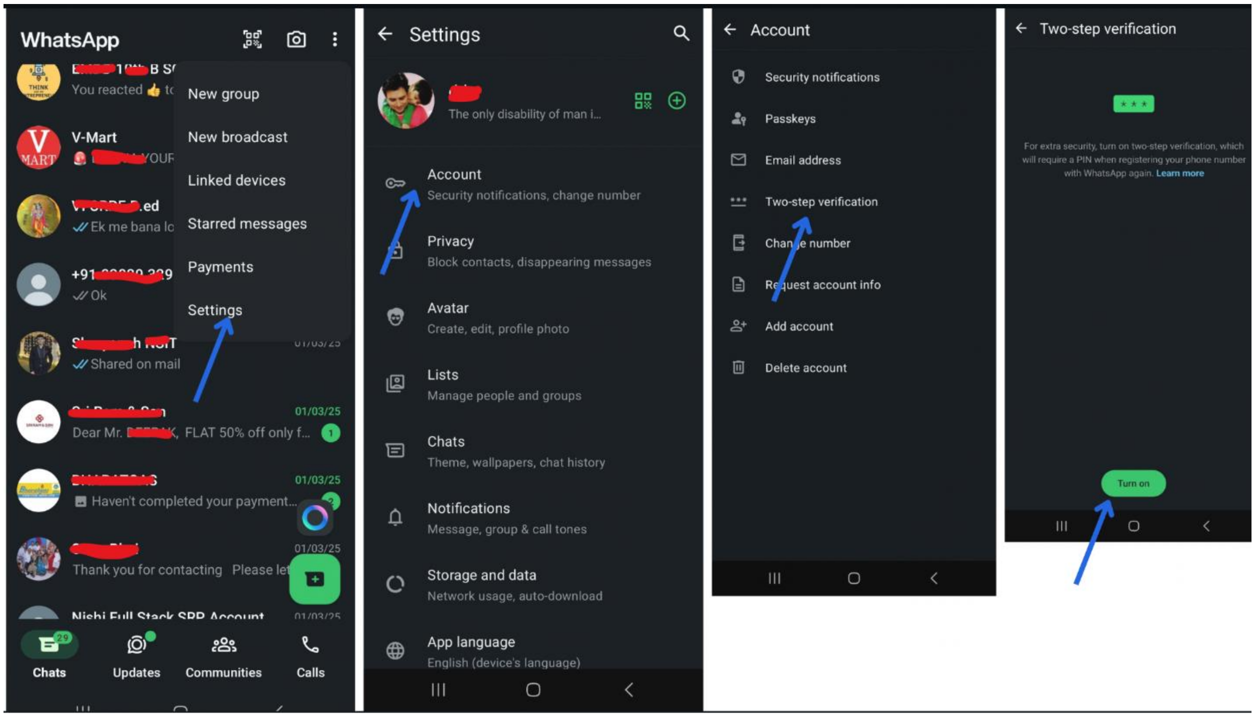
On WhatsApp navigate to Settings and Privacy and enable, set, protect, control, and review the following options one by one:

➔ Enable Two-Step Verification:

- Go to Settings > Account > Two-step verification.
- Tap "Enable" and follow the instructions to set up a PIN code to protect your account (Fig: *7.20).*

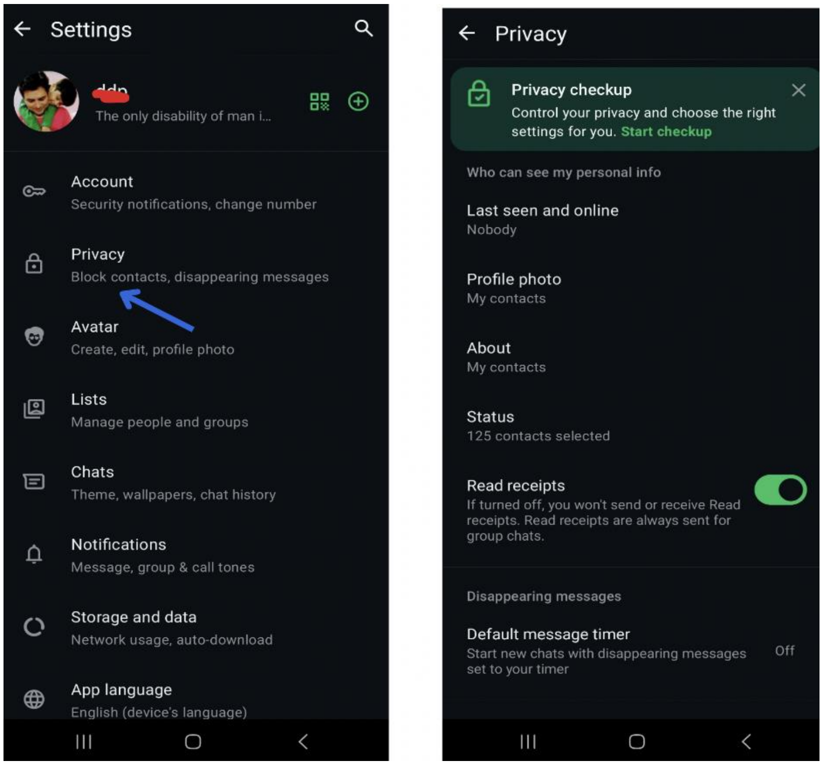
➔ Set Privacy Settings:

- Go to Settings > Privacy>.
- Adjust settings for Last Seen, Profile Photo, About, Status, and Read Receipts according to your preferences. As you can set your status can be seen to "My Contacts" or "Nobody" (Fig: *7.21).*
- One can enable Disappearing Messages for sensitive conversations.
- One can use Fingerprint Lock or similar features for additional security.



For extra security, turn on two-step verification, which will require a PIN when registering your phone number with WhatsApp again. Learn more

Fig: 7.20 Enable Two-Step Verification in WhatsApp



Settings

[redacted]
The only disability of man i...

Account
Security notifications, change number

Privacy
Block contacts, disappearing messages

Avatar
Create, edit, profile photo

Lists
Manage people and groups

Chats
Theme, wallpapers, chat history

Notifications
Message, group & call tones

Storage and data
Network usage, auto-download

App language
English (device's language)

Privacy

Privacy checkup
Control your privacy and choose the right settings for you. Start checkup

Who can see my personal info

Last seen and online
Nobody

Profile photo
My contacts

About
My contacts

Status
125 contacts selected

Read receipts
If turned off, you won't send or receive Read receipts. Read receipts are always sent for group chats.

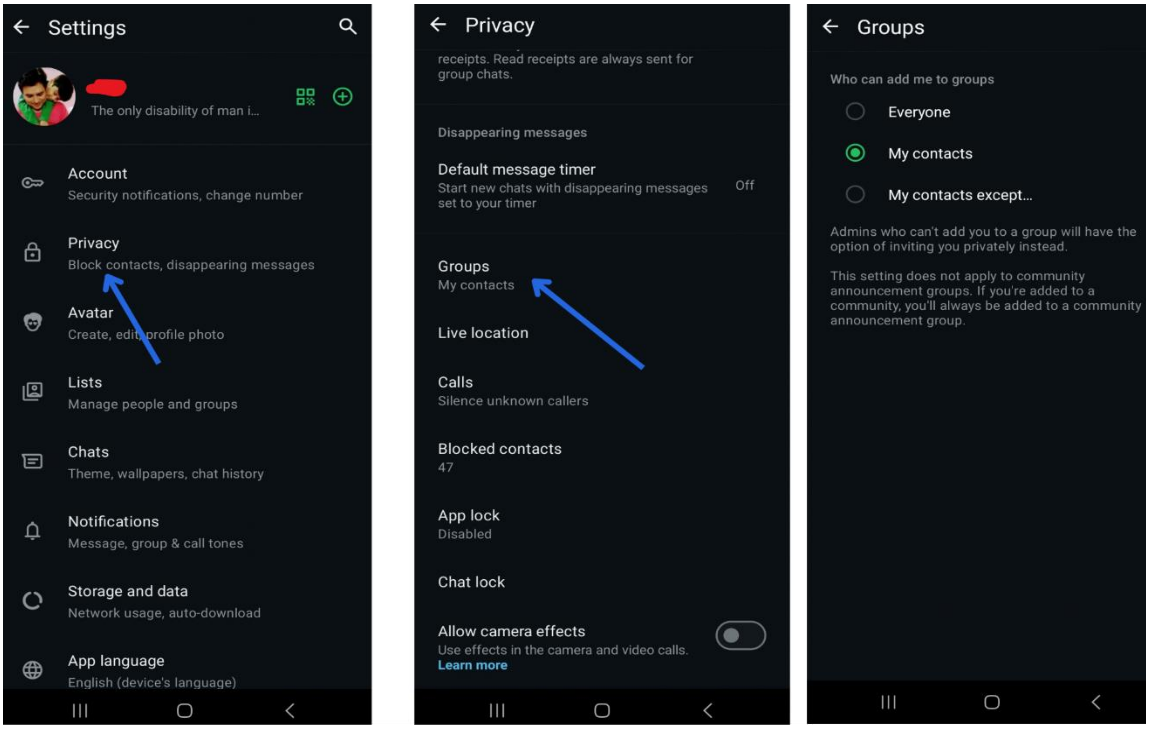
Disappearing messages

Default message timer
Start new chats with disappearing messages set to your timer
Off

Fig: 7.21 Setting privacy in WhatsApp

➔ Control Who Can Add You to Groups:

- ◆ Go to Settings > Privacy > Groups.
- ◆ Review and manage group settings to control who can add you to groups.
- ◆ Select "My Contacts" or "My Contacts Except..." to limit who can add you to groups.



Settings

[redacted]
The only disability of man i...

Account
Security notifications, change number

Privacy
Block contacts, disappearing messages

Avatar
Create, edit, profile photo

Lists
Manage people and groups

Chats
Theme, wallpapers, chat history

Notifications
Message, group & call tones

Storage and data
Network usage, auto-download

App language
English (device's language)

Privacy

receipts. Read receipts are always sent for group chats.

Disappearing messages

Default message timer
Start new chats with disappearing messages set to your timer
Off

Groups
My contacts

Live location

Calls
Silence unknown callers

Blocked contacts
47

App lock
Disabled

Chat lock

Allow camera effects
Use effects in the camera and video calls.
Learn more

Groups

Who can add me to groups

○ Everyone

● My contacts

○ My contacts except...

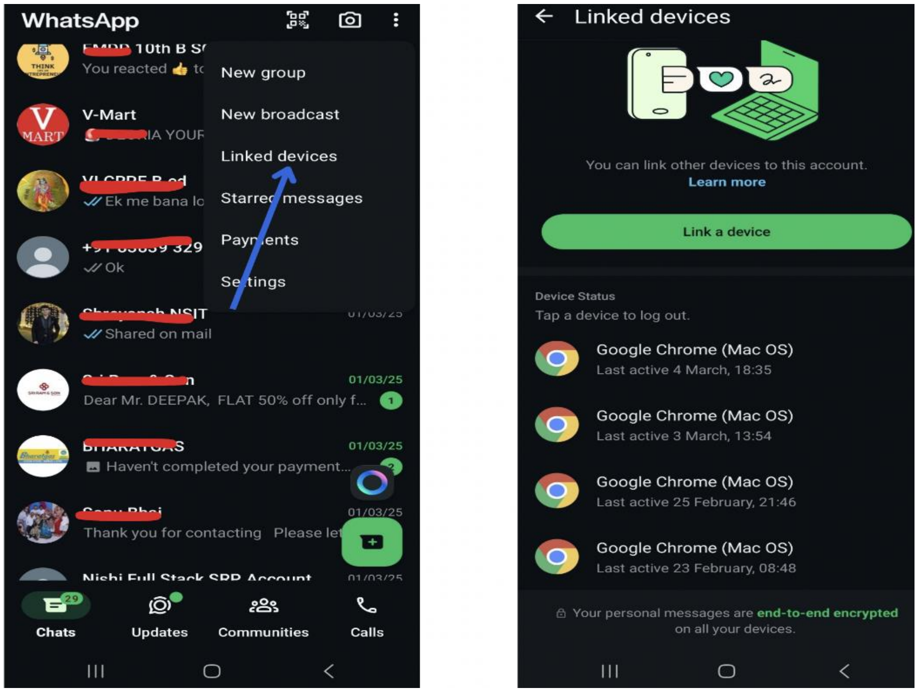
Admins who can't add you to a group will have the option of inviting you privately instead.

This setting does not apply to community announcement groups. If you're added to a community, you'll always be added to a community announcement group.

Fig: 7.22 Setting group's privacy in WhatsApp

➔ Review and Delete Linked Devices:

- Go to Settings > Linked Devices.
- Review devices linked to your WhatsApp account and log out from any that are not recognized (Fig: *7.23)*.



[redacted] 10th B S
You reacted 👍 to

V-Mart
[redacted]IA YOUR

[redacted]
Ek me bana lo

[redacted]
Ok

[redacted]
Shared on mail

[redacted] 01/03/25
Dear Mr. DEEPAK, FLAT 50% off only f... 1

[redacted] 01/03/25
Haven't completed your payment...

[redacted] 01/03/25
Thank you for contacting Please let

Nishi Full Stack SPP Account 01/03/25

You can link other devices to this account. Learn more

Device Status
Tap a device to log out.

Google Chrome (Mac OS)
Last active 4 March, 18:35

Google Chrome (Mac OS)
Last active 3 March, 13:54

Google Chrome (Mac OS)
Last active 25 February, 21:46

Google Chrome (Mac OS)
Last active 23 February, 08:48

Your personal messages are end-to-end encrypted on all your devices.

Fig: 7.23 Review and delete linked devices in WhatsApp

Points to remember:

- **Security issues:** Account hacking, phishing, impersonation, malware, data breaches, and scams.
- **Steps to enhance privacy and security:**
  - Use strong passwords and enable two-factor authentication.
  - Be Cautious about sharing on social media, think twice before share
  - Review social media app permissions before use
  - Customize platform-specific privacy and security options.

Practical Activity 7.1

Objective: Learners will configure Privacy and Security Settings on Instagram to protect personal information.

Tools & Platform Needed: Desktop/Laptop with the internet connection or Smartphone/tablet with the Instagram app

Group Formation and Task Assignment:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group a task to configure Privacy and Security Settings on Instagram.

Step 3. Activity 1 Make Your Account Private:

(i) Go to "Settings" > "Privacy" > "Account Privacy."

(ii) Toggle on "Private Account" to ensure that only approved followers can see your posts.

Step 4. Activity 2-Review Account Activity:

(i) Go to "Settings" > "Security" > "Login Activity."

(ii) Review the list of devices and locations where your account has been accessed.

(iii) Log out of any sessions that you do not recognize or no longer use.

Step 5: Activity 3-Manage Comment Controls:

(i) Go to "Settings" > "Privacy" > "Comments."

(ii) Filter out offensive comments and block specific users from commenting on your posts.

Document the process: Describe each step taken to enhance privacy and security on Instagram. Each group will showcase their findings in the form of presentation slides in front of the class and discuss the importance of Social media security

Practical Activity 7.2

Objective: Learners will configure Privacy and Security Settings in WhatsApp to protect personal information.

Tools & Platform Needed: Desktop/Laptop with internet connection or Smartphone/tablet with WhatsApp app

Procedure:

Group Formation and Task Assignment:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group a task to configure Privacy and Security Settings on WhatsApp.

Step 3. Activity 1-Set Privacy Settings:

(i) Go to Settings > Account > Privacy.

(ii) Adjust settings for Last Seen, Profile Photo, About, Status, and Read Receipts according to your preferences. You can set your status as seen by “My Contacts" or "Nobody."

(iii) One can enable Disappearing Messages for sensitive conversations.

(iv) One can use Fingerprint Lock or similar features for additional security.

Step 4. Activity 2-Control Who Can Add You to Groups:

(i) Go to Settings > Account > Privacy > Groups.

(ii) Review and manage group settings to control who can add you to groups.

(iii) Select "My Contacts" or "My Contacts Except..." to limit who can add you to groups.

Step 5: Activity 3-Review and Delete Linked Devices:

(i) Go to Settings > Linked Devices.

(ii) Review devices linked to your WhatsApp account and log out from any that are not recognized.

Document the process: Describe each step taken to enhance privacy and security on WhatsApp. Each group will showcase their findings in the form of presentation slides in front of the class and discuss the importance of Social media security

List of other suggested practical activities:

- **Facebook Account Protection:** Configure privacy and security settings in Facebook to protect personal information.

- **X Account Protection:** Configure privacy and security settings on X- platform user account to protect personal information.
- **Enabling Two-Factor Authentication (2FA):** To implement two-factor authentication for enhanced security on a social media platform.
- **Detecting and Reporting Phishing Attempts on Social Media:** Search online for examples of phishing emails or messages targeting social media users and to identify phishing attacks and learn how to report them.

Summary

- Social media refers to platforms for creating, sharing, and interacting with content and connecting globally.
- **Types of social media include:**
  - Social networking sites (e.g., Facebook, LinkedIn).
  - Microblogging platforms (e.g., Twitter, Tumblr).
  - Photo and video sharing platforms (e.g., Instagram, Snapchat).
  - Content sharing and curation platforms (e.g., YouTube, Pinterest).
  - Discussion forums (e.g., Reddit, Quora).
  - Messaging apps (e.g., WhatsApp, Telegram).
  - Professional platforms (e.g., LinkedIn).
- **Advantages of social media:**
  - Enhances connectivity and information sharing.
  - Aids marketing, branding, and awareness campaigns.
  - Provides entertainment and builds communities.
- **Disadvantages of social media:**
  - Risks include addiction, misinformation, privacy issues, cyberbullying, and mental health impacts.
- **Security issues:**
  - Challenges include hacking, phishing, impersonation, data breaches, and scams.
- **Steps to enhance privacy and security:**
  - Use strong passwords and enable two-factor authentication.
  - Review privacy settings and control shared information.
  - Customize platform-specific privacy and security options.

ASSESSMENT

Multiple Choice Questions (MCQs)

1. Which social media platform is primarily used for professional networking?
   a) Instagram
   b) LinkedIn
   c) Snapchat
   d) Pinterest

2. What security measures can help protect your Facebook account?
   a) Ignoring privacy settings
   b) Enabling Two-Factor Authentication (2FA)
   c) Using the same password for all accounts
   d) Sharing personal information publicly

3. What is a common security threat on social media?
   a) Safe browsing
   b) Phishing attacks
   c) Enhanced protection
   d) Secure browsing

4. What type of social media platform is X?
   a) Social Networking Site
   b) Microblogging Site
   c) Content Curation Site
   d) Professional Networking Site

5. Which security issue involves unauthorized access to user data on social media platforms?
   a) Data Breaches
   b) Connectivity
   c) Community Building
   d) Entertainment

6. What setting can limit who can see your tweets on X?
   a) Two-Factor Authentication
   b) Protecting Your Tweets
   c) Reviewing Connected Apps
   d) Adjusting Ad Preferences

7. What does enable two-factor authentication do?
   a) Makes your password more complex
   b) Adds an additional security layer
   c) Deletes unauthorized accounts
   d) Encrypts your messages

8. Which of the following is NOT an advantage of social media?
   a) Community building
   b) Misinformation
   c) Entertainment
   d) Marketing opportunities

9. The Cambridge Analytica scandal is an example of:
   a) Malware
   b) Impersonation
   c) Data breach
   d) Cyberbullying

10. Excessive use of social media can lead to:
   a) Cybersecurity risks
   b) Addiction
   c) Improved productivity
   d) More privacy

Fill in the Blanks

1. _______ is a social networking site that helps users connect with friends and family.
2. A major disadvantage of social media is _______ concerns.
3. _______ are online spaces where users can start and engage in discussions on various topics.
4. The spread of false information on social media is referred to as _______.
5. _______ is an example of a messaging app.
6. Enabling _______ can enhance the security of your Instagram account.
7. A common security threat on social media is _______ attacks.
8. To protect your Facebook account, you can review _______ settings.
9. _______ is the term for malicious software that can infect devices.
10. LinkedIn is primarily used for _______ networking.
11. Social media platforms are designed to help users _________, share, and interact with content.
12. Examples of microblogging platforms include _________ and Tumblr.
13. _________ is a key feature to protect accounts using an additional security layer.
14. Exposure to _________ content on social media can harm mental health.
15. Facebook is classified as a _________ site.
16. Data breaches often result from inadequate _________ measures.
17. Setting an account to private limits visibility to _________ followers only.
18. Fake profiles created to scam others is an example of _________.
19. _________ is an app commonly used for instant messaging.
20. Strong passwords should include letters, numbers, and _________.

True or False

1. Instagram is a professional networking site.
2. Privacy concerns are a major disadvantage of social media.
3. Enabling Two-Factor Authentication can help protect your social media accounts.
4. Reddit is a photo and video sharing site.
5. Cyberbullying is a common issue on social media platforms.
6. Data breaches involve unauthorized access to user data.
7. Misinformation is the spread of accurate information on social media.
8. Facebook allows users to control ad preferences.
9. Snapchat is an example of a content curation site.
10. Reviewing account activity can help identify suspicious access on Instagram.
11. LinkedIn is a messaging app.
12. Cyberbullying is a disadvantage of social media.
13. Twitter is an example of a photo-sharing platform.
14. Two-factor authentication reduces the risk of hacking.
15. Social media cannot be used for marketing purposes.
16. Instagram allows users to set their profiles to private.
17. A phishing attack aims to obtain sensitive user information fraudulently.
18. Excessive social media use can lead to addiction.
19. YouTube is primarily used for messaging.
20. Privacy settings are the same for all social media platforms.

Short Answer Questions

1. Describe a common security issue faced by social media users.
2. How can users enhance the security of their X accounts?
3. What are the benefits of enabling Two-Factor Authentication on social media platforms?
4. Explain the concept of misinformation on social media.
5. What are the main categories of social media platforms?
6. List two advantages and two disadvantages of social media.
7. What is phishing, and how does it affect social media users?
8. Mention two ways to ensure privacy on Instagram.

Long Answer Questions

1. Discuss the different types of social media platforms and their primary functions. Provide examples for each type.
2. Explain the advantages and disadvantages of social media. How can users balance the benefits while mitigating the drawbacks?
3. Discuss the advantages and disadvantages of social media, providing examples for each.
4. Explain the common security issues faced by social media users and how they can be addressed.
5. Describe the steps a user can take to enhance their privacy and security on platforms like Facebook, Instagram, and X.

Answer Key

Multiple Choice Questions

1. b, 2. b, 3. b, 4. b, 5. a, 6. b, 7. b, 8. b, 9. c, 10. b

Fill-in-the-blanks

1. Facebook, 2. Privacy, 3. Forums, 4. Misinformation, 5. WhatsApp, 6. Two-Factor Authentication, 7. Phishing, 8. Privacy, 9. Malware, 10. Professional, 11. connect, 12. X (Twitter), 13. Two-Factor, Authentication, 14. harmful, 15. social networking, 16. security
17. approved, 18. impersonation, 19. WhatsApp, 20. symbols

True/False questions

1. False, 2. True, 3. True, 4. False, 5. True, 6. True, 7. False, 8. True, 9. False, 10. True, 11. False, 12. True, 13. False, 14. True, 15. False, 16. True, 17. True, 18. True, 19. False, 20. False

Chapter-8

Digital Payments and its Security

In a small town, Atharv, a tech enthusiast, relied heavily on digital payments for their convenience. One day, he discovered his account had been hacked, with large unauthorized transactions. Despite being cautious, he realized digital systems were vulnerable to scams like phishing and malware. Atharv learned about two-factor authentication and complex passwords to enhance security. Determined to help, he teamed up with his cybersecurity friend, Neer, to raise awareness. They conducted workshops teaching safe online practices and spotting potential threats. Local businesses were educated on secure payment systems and protecting customer data. Gradually, the town adopted safer digital payment habits, and banks improved security measures. Atharv and Neer's efforts safeguarded their community from digital payment risks. Their story emphasizes the importance of staying informed and vigilant in a digital world.

8.1 Introduction to Digital Payment Systems

Digital payments refer to the transfer of money or digital currency through electronic means. These systems enable seamless, fast, and secure financial transactions, eliminating the need for physical cash or checks. Digital payment systems have revolutionized the way we conduct financial transactions. These systems rely on digital platforms, bypassing traditional methods like cash or checks. With the proliferation of smartphones and the internet, digital payments have seen exponential growth both in India and globally.

In both Indian and international contexts, digital payments have become an integral part of daily life, facilitating everything from online shopping to bill payments and peer-to-peer transfers. In India, initiatives like the Digital India program have significantly boosted digital payment adoption. The Unified Payments Interface (UPI) has emerged as a game-changer, facilitating peer-to-peer and merchant payments. Internationally, systems such as PayPal, Apple Pay, and Alipay have gained popularity, offering a range of services from mobile wallets to cross-border transactions (Fig: 8.2*)*.

Fig: 8.1 Unified Payment System (UPI)

8.1.1 How do Digital Payment Systems Work

Digital payments work through the integration of mobile devices, payment gateways, banks, and merchant systems. A user initiates a payment through a digital platform, which is authenticated, processed, and settled in a secure and efficient manner. Throughout the process, sensitive data is encrypted to ensure security. Digital payment systems operate through the following steps:

- **User Account Registration:** Users create an account on the digital payment platform and link it to their bank account or credit/debit card.
- **Initiating a Transaction by User:** A user initiates a payment via a digital platform (e.g., mobile app or website). The user selects the recipient and enters the transaction amount.
- **Authentication:** The platform authenticates and verifies the user’s identity through various methods such as passwords, PINs, biometric verification, or OTPs (one-time passwords).
- **Payment Gateway:** The digital platform forwards the transaction details to a payment gateway, which acts as a bridge between the user and the financial institution.
- **Transaction Processing:** The payment gateway sends the request to the user’s bank for approval by communicating with the user's bank or card issuer to verify and transfer funds.
- **Settlement:** Upon approval, the funds are transferred to the recipient’s account, and both parties are notified of the transaction status.
- **Confirmation and Notification:** The user and recipient receive a confirmation of the transaction, often through notifications or email receipts.

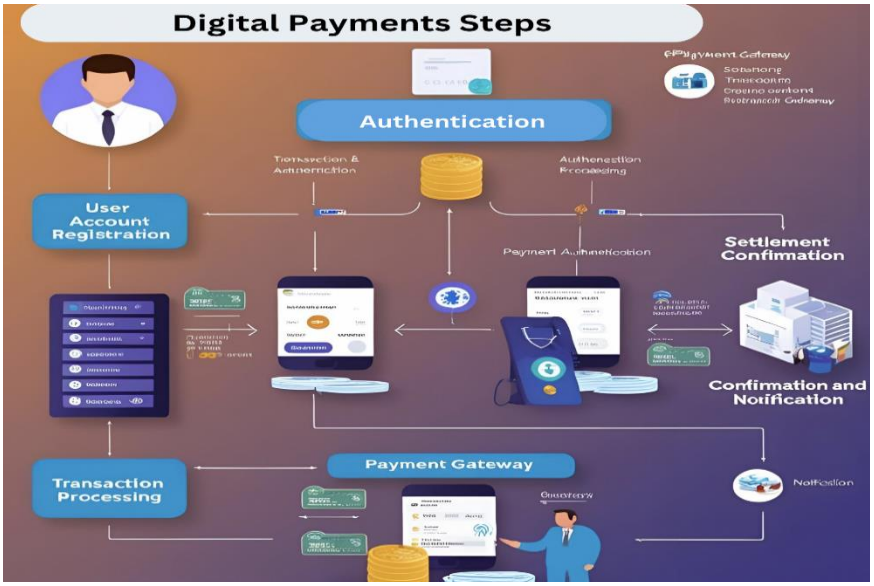


Fig: 8.2 How does the Digital Payment System Work?

Points to remember:

- **Digital Payment Systems:**
  - Revolutionized financial transactions, eliminating physical cash.
  - Integral part of daily life in both Indian and international contexts.
  - Digital payment systems enable cashless, seamless transactions.
  - Examples: UPI (India), PayPal (global).
  - Components include devices, payment gateways, banks, and merchants.
- **How Digital Payment Systems Work:**
  - User Account Registration
  - Initiating a Transaction by User
  - Authentication
  - Payment Gateway
  - Transaction Processing
  - Settlement
  - Confirmation and Notification

8.2 Types of Digital Payment Systems and Their Applications

1. **Mobile Wallets:** These are digital wallets stored on mobile devices that allow users to make payments. It helps in peer-to-peer transfers, merchant payments, online shopping. There are several mobile apps in India that allow users to transact without linking a bank account, primarily by using mobile wallet systems. Apps like Paytm, PhonePe, and Amazon pay dominate the Indian market, allowing users to store money and make transactions for utilities, shopping, and transportation. Services such as Apple Pay, Samsung Pay are widely used internationally for retail purchases, online shopping, and contactless payments. A list of Indian mobile wallets that do not require UPI for transactions. These mobile wallets primarily function through prepaid balance, wallet-to-wallet transfers, or direct linking with credit/debit cards:

- **Google Pay** is a digital wallet and payment app that lets you pay online, in stores, and in apps. You can also use it to send and receive money, recharge your phone, and pay bills.
- **PhonePe Wallet:** While PhonePe is UPI-based, it also provides a wallet option for transactions.
- **MobiKwik:** It is a versatile wallet for payments, recharge, and money transfers without requiring UPI (Fig: 8.3).

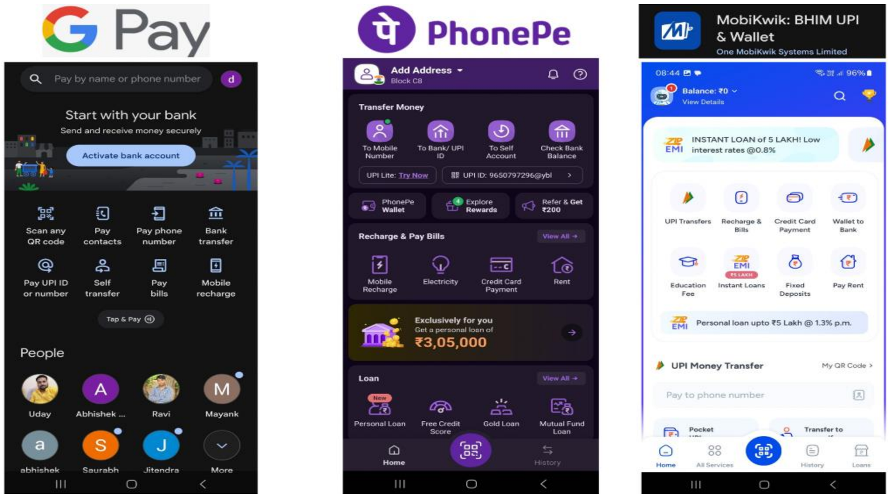


Fig: 8.3 G Pay, Phonepe and MobiKwik apps

- **Amazon Pay:** In this wallet users can load money into the wallet and use it for purchases or bill payments without UPI.
- **Paytm Wallet:** It offers wallet-to-wallet transfers, bill payments, and shopping. UPI is optional. wallet functionality operates independently. (Fig: 8.4*)*

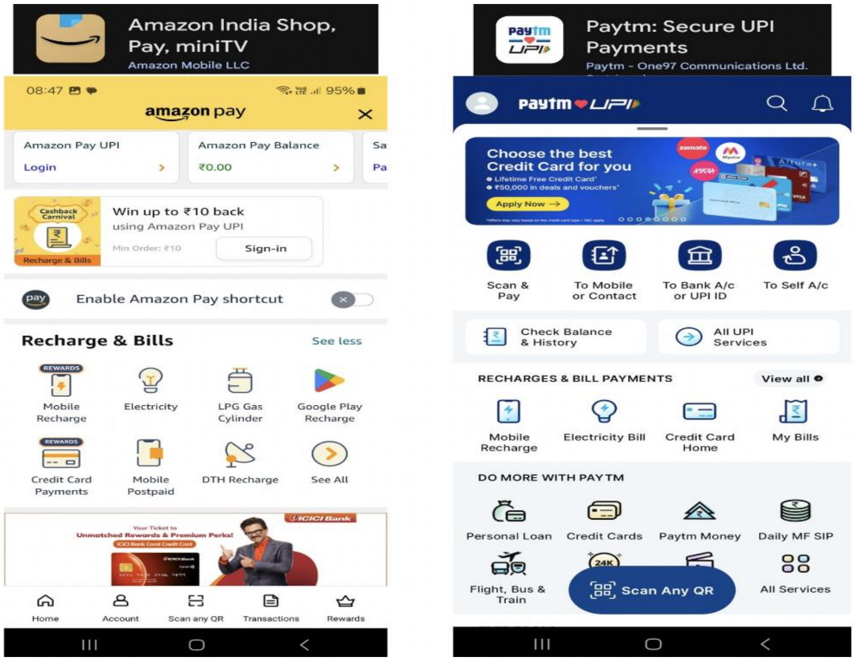


Fig: 8.4 Amazon Pay and Paytm apps

- **Freecharge:** It allows wallet-based transactions for utility bill payments, mobile recharges, and online shopping.
- **JioMoney:** It is a wallet service by Reliance for mobile recharges, utility payments, and shopping (Fig: 8.5*)*.

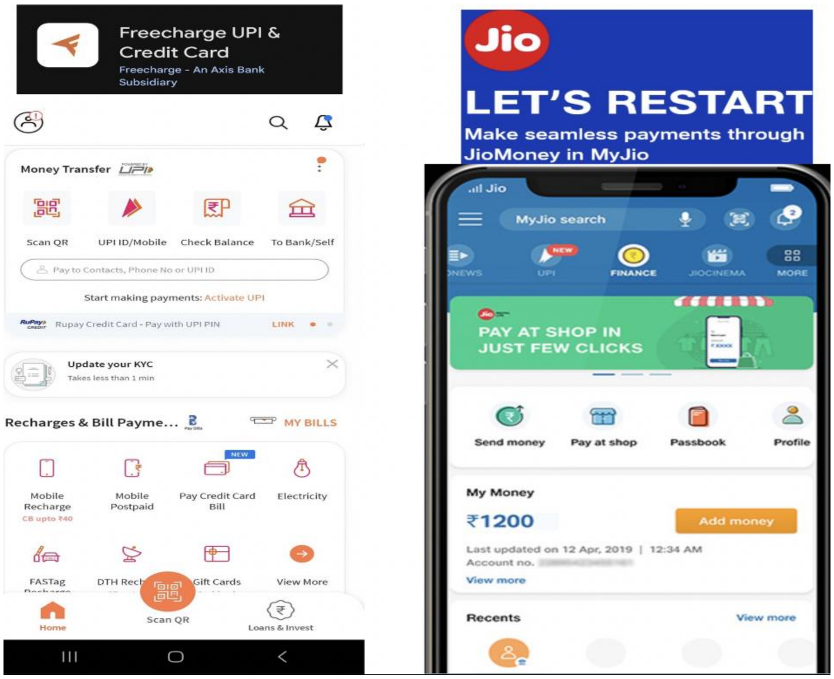


Fig: 8.5 Freecharge and Jio Money apps

- **Airtel Thanks App:** It allows you to make instant online payments for Mobile recharges utility bill payments. One can use it to send money to friends and family.
- **Payzapp by HDFC:** It functions as a wallet and offers direct payments without UPI (Fig: *8.6).*

Fig: 8.6 Airtel Thanks and Payzapp

2. **Credit/Debit Card Payments:** Debit and credit cards issued by Visa, MasterCard, and RuPay are commonly used for point-of-sale (POS) and online shopping, in-store purchases, bill payments. Card networks like Visa and MasterCard are globally accepted, facilitating transactions both online and offline (Fig: 8.7*).*

Fig: 8.7 Debit/Credit Cards issued by RuPay, VISA and MasterCard

3. **Bank Transfers:** In this type of digital payment direct transfer of funds between bank accounts is done for bill payments, peer-to-peer transfers. NEFT (National Electronic Funds Transfer), RTGS (Real-Time Gross Settlement), IMPS (Immediate Payment Service) enable instant money transfers with minimal fees in India. SWIFT and SEPA systems are commonly used internationally for cross-border bank transfers.
4. **Unified Payments Interface (UPI):** It is a real-time payment system that facilitates inter-bank transactions through a single mobile application. It performs Peer-to-peer transfers, merchant payments, bill payments. Examples include BHIM (Bharat Interface for Money), PhonePe, Google Pay.
5. **QR Code Payments:** QR code is quick response code. Bharat QR and individual wallet QR codes are extensively used for payments in local shops and street vendors. Both mobile wallets and UPI based apps use this feature for payment. WeChat Pay and Alipay in China leverage QR codes for everyday payments (Fig: 8.8*).*

Fig: 8.8 QR Code Payment

6. **Cryptocurrency Payments:** Digital currencies that use cryptography for secure transactions. These are used for Online purchases, investments, remittances. Although under regulatory scrutiny, platforms like CoinDCX and WazirX enable cryptocurrency transactions in India. Bitcoin, Ethereum, and other cryptocurrencies are gaining traction for online purchases and investments globally.
7. **Contactless Payments:** NFC-enabled debit and credit cards and devices are gradually gaining popularity. Digital payments are made using NFC (Near Field Communication) technology or QR codes. It is used for in-store purchases, public transportation. Tap-and-pay systems using NFC technology are prevalent in many developed countries. Examples include Apple Pay, Samsung Pay, Bharat QR.

Points to remember:

- **Types of Digital Payment Systems:**
  - Credit/Debit Card Payments: e.g., Visa, Mastercard, Rupay.
  - Mobile Wallets: e.g., Paytm, Apple Pay.
  - Bank Transfers: e.g., NEFT, RTGS, SWIFT.
  - Unified Payments Interface (UPI): Real-tie.g., BHIM, PhonePe).
  - Cryptocurrencies: e.g., Bitcoin, Ethereum).
  - Contactless Payments: e.g., NFC-enabled devices, Apple Pay, Bharat QR).

8.3 Security Issues and Threats in Digital Payments

While digital payment systems offer numerous benefits, they also come with security challenges and threats:

- **Phishing Attacks:** It is a fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity. Fraudulent emails or messages trick users into revealing sensitive information.

  Example: Fake emails or messages that trick users into providing login credentials or payment details.
- **Malware, Viruses & Ransomware:** Malicious software compromises devices to steal credentials and financial data. Ransomware is software that can infect devices and compromise data security.

  Example: Malware that captures keystrokes to steal passwords or ransomware that locks users out of their devices until a ransom is paid.
- **Man-in-the-Middle (MitM) Attacks:** This attack does interception of communication between the user and the payment platform. Interception of data during transmission can lead to unauthorized access.

  Example: Attackers intercepting and altering transaction data during transmission.
- **Data Breaches:** Data breaches are done by unauthorized access to large volumes of user data stored by payment platforms. Payment systems and databases are targets for hackers aiming to steal financial information. Weak authentication mechanisms increase the risk of unauthorized transactions.

  Example: Hackers gaining access to credit card information and personal details from a payment gateway.
- **Social Engineering:** It is a manipulation technique that exploits human psychology to trick people into revealing confidential information, granting access, or performing actions that compromise security. Unlike traditional hacking, social engineering relies on human error rather than technical vulnerabilities.

  Example: An attacker calls an employee pretending to be from IT support, asking for their password to "fix" a company-wide issue.

8.3.1 Techniques to Address and Resolve Digital Payment Security Issues

1. **Implementation of Strong Authentication Protocols:** There is a need for a strong authentication protocol which can be achieved by implementing multiple layers of authentication to verify user identity. Use of two-factor(2FA) or multi-factor authentication (MFA) and biometric verification are preferable.

   Example: Combining passwords with biometric verification or OTPs.
2. **Secure Payment Gateways with encryption:** The payment gateway must be secured with ensuring end-to-end encryption during transactions. Use encryption to protect data during transmission and storage. Also, replace sensitive data with encrypted tokens during transactions.

   Example: SSL/TLS encryption for securing online transactions.
3. **Regular Security Audits:** Conduct regular security audits to identify and address vulnerabilities in payment systems.

   Example: Payment platforms hiring cybersecurity firms to perform penetration testing.
4. **User Education & Public Awareness Campaigns:** Educate users about recognizing and avoiding fraud attempts. Launch public awareness campaigns about common security threats and safe practices.

   Example: Banks and payment platforms providing resources on how to recognize phishing attempts.
5. **Regulatory Frameworks:** Establish and adopt robust legal structures like the General Data Protection Regulation (GDPR) in Europe or India's IT Act to protect user data.
6. **Fraud Detection Systems:** Leverage AI and machine learning to identify and block suspicious activities in real-time. Implement systems that monitor transactions for suspicious activity.

   Example: AI-based fraud detection algorithms that flag unusual spending patterns.
7. **Data Minimization:** Collect and store only the necessary user information.

   Example: Payment platforms should limit the amount of personal data they store to reduce the impact of data breaches.

Points to remember:

- **Digital Payment Security Issues and Threats:**
  - Phishing Attacks
  - Malware and Ransomware
  - Data Breaches
  - Man-in-the-Middle (MitM) Attacks
  - Identity Theft
- **Addressing and Resolving Digital Payment Security Issues:**
  - Implementation of Strong Authentication Protocols
  - Multi-Factor Authentication (MFA)
  - Secure payment gateways with Encryption
  - Regular Security Audits
  - User Education Public awareness
  - Fraud Detection Systems
  - Data Minimization

Practical Activity 8.1

Objective: Learners will understand the process of setting up and Setting up and Conducting a secure UPI Transaction

Tools & Platform Needed: Android/iphone smartphone or tablet/ipad with internet access, UPI-enabled mobile app (e.g., BHIM, PhonePe, Google Pay etc.), Bank account linked to UPI

Procedure:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group a particular UPI mobile app discussed in chapter.

Step 3. Download the selected app on your smartphone/tablet.

Step 4. Check and set app permissions as discussed in chapter 6.

Step 5. Open UPI app and register using your mobile number linked to your bank account.

Step 6. Verify your phone number through OTP.

Step 7. Create a UPI ID (e.g., yourname@upi) and set a UPI PIN.

Step 8. Link Bank Account:

a) In the app, navigate to the settings or account section.
b) Select the option to link a bank account.
c) Choose your bank from the list and follow the prompts to link your account.

Step 9. Initiate a UPI Payment:

a) Go to the payment section of the app.
b) Select the recipient by entering their UPI ID or scanning their QR code.
c) Enter the transaction amount.
d) Confirm the payment by entering your UPI PIN or biometric authentication (fingerprint or facial recognition).

Step 10. Document the above steps and findings: Each group will showcase their findings in the form of presentation slides with screenshots in front of class and note any challenges encountered and how they were resolved and their impact on personal information security.

Practical Activity 8.2

Objective: Learners will explore and learn how to enable Digital Payment Security Features

Tools & Platform Needed: Laptop/Android/iphone smartphone or tablet/iPad with internet access, Digital Payment app (e.g., BHIM, Paytm,PhonePe, Google Pay etc.), Bank account linked to payment platform

Procedure:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group a particular digital payment platform discussed in chapter.

Step 3. Download the selected app on your smartphone/tablet.

Step 4. Check and set app permissions as discussed in chapter 6.

Step 5. Enable Multi-Factor Authentication (MFA):

a) Log in to your digital payment account on the platform.
b) Navigate to the security settings.
c) Identify common security features (e.g., two-factor authentication, encryption) in a payment app. Enable multi-factor authentication (MFA) by adding an additional layer of security, such as OTP or biometric verification.

Step 6. Set Up Transaction Alerts:

a) Go to the settings or notification section.
b) Enable transaction alerts to receive notifications for every transaction made using your account.

Step 7. Enable Encryption and Secure Browsing:

a) Ensure that the platform uses SSL/TLS encryption by checking for "https" in the URL when accessing the platform on a web browser.

b) Enable any available settings for secure browsing and data encryption in the app.

Step 8. Review and Update Passwords:

a) Go to the account settings.

b) Review and update your password to a strong, unique password that includes a mix of letters, numbers, and special characters.

c) Enable regular password updates and avoid using the same password across multiple platforms

Step 9. Test the app by logging in with and without enabling security features like biometric authentication.

Step 10. Simulate a phishing attempt (educational purpose only) to understand vulnerabilities.

Step 10. Document the above steps and security features: Each group will showcase their findings in the form of presentation slides with screenshots in front of class and note Describe each security feature enabled and its importance. Analyze how the app protects against potential threats and suggest improvements. Note any challenges encountered and how they were resolved. Provide screenshots of key steps if possible.

List of other suggested practical activities:

- **Setting Up and Using a Mobile Wallet:** Learn how to set up a mobile wallet, link it to a bank account, and make a payment.
- **QR Code Payment System:** To explore the use of QR codes in digital payments.
- **Enabling Two-Factor Authentication (2FA):** To implement two-factor authentication for enhanced security while using payment apps.
- **Conducting a Secure Online Purchase:** Learn how to perform a secure online purchase using a digital payment method and understand the security measures in place.

Summary

➔ **Introduction to Digital Payment Systems:**

- Revolutionized financial transactions, eliminating physical cash.
- Integral part of daily life in both Indian and international contexts.
- Digital payment systems enable cashless, seamless transactions.
- Examples: UPI (India), PayPal (global).
- Components include devices, payment gateways, banks, and merchants.

➔ **How Digital Payment Systems Work:**

- User Registration: Creating an account and linking it to a bank account or card.
- Initiating a Transaction: Selecting recipient & entering the transaction amount. User initiates payment via a digital platform.
- Authentication: Authentication methods (PIN, biometrics, OTPs) verify the user.
- Transaction Processing: Payment gateway processes transactions, banks authorize it. Communicating with the bank or card issuer to verify and transfer funds. Funds are transferred securely, using encryption.
- Confirmation and Notification: Sending transaction confirmation to both user and recipient.

➔ **Types of Digital Payment Systems and Their Applications:**

- Credit/Debit Card Payments: e.g., Visa, Mastercard, Rupay.
- Mobile Wallets: e.g., Paytm, Apple Pay.

- Bank Transfers: e.g., NEFT, RTGS, SWIFT.
- Unified Payments Interface (UPI): : e.g., BHIM, PhonePe.
- Cryptocurrencies: e.g., Bitcoin, Ethereum).
- Contactless Payments: e.g., NFC-enabled devices, Apple Pay, Bharat QR).

➔ **Digital Payment Security Issues and Threats:**

- Phishing Attacks: Fraudulent attempts to obtain sensitive information.
- Malware and Ransomware: Malicious software compromising data security.
- Data Breaches: Unauthorized access to user data.
- Man-in-the-Middle (MitM) Attacks: Interception of communication between user and platform.
- Identity Theft: Unauthorized use of personal information for fraud.

➔ **Addressing and Resolving Digital Payment Security Issues:**

- Multi-Factor Authentication (MFA): Verifying user identity through multiple layers.
- Encryption: Protecting data during transmission and storage.
- Regular Security Audits: Identifying and addressing vulnerabilities.
- User Education: Educating users about common security threats.
- Fraud Detection Systems: Monitoring transactions for suspicious activity.
- Data Minimization: Collecting and storing only necessary information.

➔ Security Issues: Threats include phishing, malware, MitM attacks, data breaches, unauthorized access, and social engineering.

➔ Addressing Security: Solutions include two-factor authentication, encryption, fraud detection, public awareness, and regulatory frameworks.

ASSESSMENT

Multiple Choice Questions (MCQs)

1. What is a digital payment system?
   a) A system for transferring physical cash
   b) A system for transferring money electronically
   c) A method for printing currency
   d) A manual bookkeeping method

2. Which of the following is an example of a mobile wallet?
   a) Visa
   b) Paytm
   c) NEFT
   d) Mastercard

3. What technology is used in contactless payments?
   a) Bluetooth
   b) QR codes and NFC
   c) Infrared
   d) Wi-Fi

4. What is a common security threat in digital payments?
   a) High transaction speed
   b) Phishing attacks

c) Low transaction cost
d) Multiple payment options

5. What is the role of multi-factor authentication (MFA) in digital payment security?
a) Simplifying login processes
b) Verifying user identity through multiple layers of authentication
c) Reducing transaction fees
d) Increasing transaction speed

6. Which protocol is commonly used to secure online transactions?
a) HTTP
b) FTP
c) SSL/TLS
d) SMTP

7. What can users do to recognize and avoid phishing attempts?
a) Ignore email notifications
b) Share their passwords widely
c) Educate themselves about common security threats
d) Use the same password for all accounts

8. What is the purpose of regular security audits for digital payment platforms?
a) To increase transaction volume
b) To identify and address vulnerabilities
c) To promote new payment methods
d) To simplify user interfaces

9. What does UPI stand for in the context of digital payments in India?
a) Unified Payments Interface
b) Universal Payment Initiative
c) Unified Payment Integration
d) Universal Payments Interaction

10. Which of the following components is NOT involved in digital payments?
a) Payment gateway
b) Authentication
c) Manual ledger entry
d) Bank authorization

11. What secures data transmission in digital payments?
a) Malware
b) Encryption
c) Phishing
d) Social engineering

12. UPI is an example of:
a) Cryptocurrency

b) Mobile Wallet
c) Bank Transfer
d) Encryption

13. Which technology underpins contactless payments?
a) Blockchain
b) QR Codes
c) NFC
d) OTP

14. A MitM attack targets which phase of digital payments?
a) Data storage
b) Data transmission
c) User authentication
d) Fund settlement

15. What is the primary benefit of tokenization in digital payments?
a) Enhances speed
b) Replaces sensitive data
c) Reduces costs
d) Avoids authentication

16. What is used for biometric authentication in digital payments?
a) Password
b) Fingerprint
c) OTP
d) QR code

17. Which international payment platform is widely used for cross-border transactions?
a) Paytm
b) SWIFT
c) Bharat QR
d) PhonePe

18. What Indian initiative promoted digital payment adoption?
a) Digital Bharat
b) Bharat QR Program
c) Digital India
d) IT Act

Fill in the Blanks

1. _______ refers to the transfer of money through electronic means.
2. Digital wallets stored on mobile devices that allow users to make payments are known as _______.
3. _______ is a digital currency that uses cryptography for secure transactions.
4. _______ attacks involve fraudulent attempts to obtain sensitive information by pretending to be trustworthy entities.
5. SSL/TLS encryption is used to secure _______ transactions.

6. Malware and _______ can infect devices and compromise data security.
7. The Unified Payments Interface (UPI) facilitates inter-bank transactions through a single _______.
8. Implementing multiple layers of authentication to verify user identity is known as _______.
9. AI-based fraud detection algorithms can flag unusual _______ patterns.
10. Data in digital payments is secured using ______.
11. NFC is used in ______ payments.
12. The process of replacing sensitive data with tokens is called ______.
13. SWIFT is primarily used for ______ bank transfers.
14. Phishing attacks often use ______ to trick users.
15. Biometric authentication methods include ______ and facial recognition.

True or False

1. Digital payment systems require physical cash to operate.
2. Mobile wallets are used for peer-to-peer transfers and online shopping.
3. Phishing attacks are a significant security threat in digital payments.
4. Encryption is used to protect data during transmission and storage.
5. Identity theft involves unauthorized use of someone's personal information to commit fraud.
6. Regular security audits help increase transaction volume.
7. UPI is a real-time payment system in India.
8. Malware does not affect digital payment security.
9. Multi-factor authentication simplifies login processes.
10. Educating users about common security threats can help prevent phishing attempts.
11. Digital payments eliminate the need for encryption.
12. PayPal is an Indian digital payment system.
13. Biometric authentication is a secure form of user verification.
14. QR codes are used only for contactless payments.
15. A payment gateway is essential for processing transactions.
16. Tokenization replaces sensitive data with encrypted keys.
17. UPI is limited to peer-to-peer transfers.
18. Malware can compromise financial data in digital payments.
19. Two-factor authentication improves payment security.
20. SWIFT is not used for domestic transactions.

Short Answer Questions

1. What are the key components of a digital payment system?
2. Explain the role of a payment gateway in digital payments.
3. Name three security threats in digital payment systems.
4. What is tokenization, and why is it important?
5. How do QR code payments work in India?
6. How does multi-factor authentication enhance the security of digital payments?
7. What is the role of encryption in digital payment security?
8. Explain the concept of Unified Payments Interface (UPI) and its applications.

Long Answer Questions

1. Discuss the different types of digital payment systems and their applications, providing examples for each type.
2. Describe the various security issues and threats associated with digital payment systems. How can these issues be addressed and resolved?
3. Explain how digital payment systems work, including the steps of user registration, transaction initiation, authentication, processing, and confirmation. How do these steps ensure secure and efficient transactions?

Answer Key

Multiple Choice Questions

1. b, 2. b, 3. b, 4. b, 5. b, 6. c, 7. c, 8. b, 9. a, 10. c, 11. b, 12. c, 13. c, 14. b, 15. b, 16. b, 17. b, 18. c

Fill-in-the-blanks

1. digital payment, 2. mobile wallets, 3. cryptocurrency, 4. phishing, 5. online, 6. spyware, 7. platform, 8. multi-factor authentication, 9. transaction, 10. encryption, 11. contactless, 12. tokenization, 13. international, 14. fake emails, 15. fingerprint

True/False questions

1. False, 2. True, 3. True, 4. True, 5. True, 6. False, 7. True, 8. False, 9. False, 10. True, 11. False, 12. False, 13. True, 14. False, 15. True, 16. True, 17. False, 18. True, 19. True, 20. True

Chapter-9

Introduction to Online Frauds in Banking

Amina, a fraud analyst at a major bank, sat in front of her screen, reviewing flagged transactions. One stood out: an amount of ₹ 10,00000 transferred from a high-profile client, Mr. Rajesh Kapoor, to an overseas account. The transfer seemed legitimate at first, with two-factor authentication and a matching IP address. But something felt off. Rajesh never made such large transfers at odd hours. Amina called Rajesh. "Mr. Kapoor, did you authorize a ₹ 10,00000 transfer last night?". "No, I didn't," he responded, panic rising in his voice. "I've been asleep!". Amina's heart sank. This wasn't a simple error — the funds had been sent to a shell company in a tax haven. Rajesh Kapoor had fallen victim to a phishing attack. The hacker had obtained his credentials through a fake email and transferred the money.

As Amina investigated further, she discovered multiple similar fraudulent transfers, pointing to an organized criminal group using *banking Trojans* to steal login information and *account takeover fraud* to bypass security. These criminals had even infiltrated bank employees' accounts, rerouting funds through sophisticated laundering schemes. Amina quickly froze the affected accounts and alerted law enforcement. But it was clear that the battle against cybercrime was just the beginning of a larger war. The fraudsters would always be one step ahead, finding new ways to exploit vulnerabilities.

Digital and online banking frauds involve unauthorized actions or schemes carried out using the internet or digital platforms to steal funds, access confidential information, or compromise banking systems. With the rapid growth of online banking and digital transactions, fraudsters have adopted increasingly sophisticated techniques, posing significant challenges to banks and their customers worldwide. Both Indian and international banking sectors have witnessed a rise in such frauds, driven by technological advancements and increased digital adoption. Digital and online banking frauds have become increasingly prevalent with the rise of internet banking and digital financial transactions. These frauds involve unauthorized access to and manipulation of banking systems to steal funds or sensitive information. Both in India and internationally, these frauds pose significant risks to individuals, businesses, and financial institutions.

9.1 Types of Digital and Online Banking Frauds and Their Causes

1. Phishing and Smishing: Fraudsters create fake websites or send emails/messages that appear to be from legitimate banks to steal sensitive information such as login credentials, credit card numbers, and personal identification details. Fraudulent emails (phishing) or SMS messages (smishing) trick recipients into sharing sensitive information like passwords or bank account details.

Causes: Poor email filtering, and deceptive links or messages that mimic legitimate entities. Lack of awareness among users, sophisticated email spoofing techniques, and the increasing use of online communication for banking.

2.Vishing (Voice Phishing): Fraudsters use phone calls to impersonate bank representatives and trick individuals into divulging personal information. Scammers make phone calls pretending to be bank officials or customer service representatives to trick individuals into providing their personal and financial information.

Causes: Social engineering tactics, insufficient customer education, Lack of awareness about fraud techniques, use of persuasive tactics by fraudsters, and inadequate verification processes.

3. Malware and Ransomware Attacks: Malicious software infects devices to capture banking credentials or lock systems until a ransom is paid. Malicious software is installed on users' devices to steal login credentials and other sensitive information or to encrypt data and demand a ransom for its release.

Causes: Clicking on malicious links, downloading infected files and unverified applications, and lack of updated antivirus software, weak cybersecurity practices.

4. SIM Swap Fraud: Fraudsters trick mobile carriers into transferring a victim's phone number to a new SIM card, thereby gaining access to OTPs (one-time passwords) and other sensitive information sent to the victim's phone. Fraudsters duplicate a victim's SIM card to gain access to OTPs (One-Time Passwords) and other banking information.

Causes: Lack of stringent verification by mobile carriers, social engineering tactics, and inadequate security measures by users. Social engineering, weak telecom security protocols.

5. Account Takeover Fraud: Cybercriminals and Fraudsters gain unauthorized access to a victim's online banking account to conduct fraudulent transactions using stolen credentials.

Causes: Data breaches, weak passwords, and reuse of passwords across multiple platforms. Weak passwords, credential leaks from data breaches, or phishing attacks.

6. E-wallet and UPI Frauds: Unauthorized transactions are carried out via digital wallets or Unified Payments Interface (UPI) apps.

Causes: Sharing of OTPs, fraudulent app downloads, and lack of two-factor authentication.

7. Card Skimming and Cloning: Devices are used to steal card information during transactions, which is then used to create cloned cards. Fraudsters install devices on ATMs or point-of-sale (POS) terminals to capture card information and PINs during transactions.

Causes: Poor physical security measures at ATMs and POS terminals, outdated technology, and unawareness among users about checking for skimming devices. Use of compromised ATMs or POS terminals and lack of EMV chip-enabled cards.

8. Fake Banking Apps: Fraudulent apps mimic legitimate banking apps to steal user credentials.

Causes: Downloading apps from unverified sources and lack of app verification processes.

9. Man-in-the-Middle (MITM) Attacks: Cybercriminals and attackers intercept and manipulate communication between users and banking site servers or apps to steal sensitive information or divert funds.

Causes: Insecure public Wi-Fi usage, Insecure Wi-Fi connections and lack of encryption, outdated security protocols.

10. Identity Theft: Attacker does it using stolen personal information to access accounts or obtain services fraudulently. It is done by Phishing, hacking, or physical theft of documents.

11. Cheque Fraud: It mainly happens offline altering or forging cheques to withdraw unauthorized funds. The main tactics are Signature forgery, tampering with cheque details, or issuing fake Cheques.

12. Loan Fraud: It also happens both online and offline by doing misrepresentation of documents or collusion to obtain loans fraudulently.

Examples: Fake property documents, identity theft for loans, or falsified income statements.

13. Money Laundering: Concealing the origins of illicitly obtained money by passing it through a legitimate banking channel is called money laundering. It is the very first step of bigger bank scams.

14. Insider Fraud: Fraud committed by employees of the bank, such as misappropriating funds or unauthorized account access.

9.1.1 Key Causes of Digital and Online Banking Fraud

1. **Increased Reliance on Online Transactions:** The shift towards digital transactions has created more opportunities for fraud.
2. **Sophistication of Cyber Criminals:** Fraudsters are using more advanced techniques to exploit vulnerabilities.
3. **Weak Passwords and Authentication:** Inadequate security measures make it easier for fraudsters to gain access.
4. **Inadequate Customer Education:** Many users are unaware of the risks and how to protect themselves.
5. **Data Breaches:** Leaks of personal information provide fraudsters with the data they need to commit fraud.
6. **Mobile Banking Vulnerabilities:** Mobile devices are often less secure than desktops, making them easier targets.
7. **Third-party Services:** Services that integrate with banking systems can be exploited by fraudsters.
8. **Regulatory Challenges:** Inconsistent regulations can create gaps that fraudsters exploit.

9.2 Tools, Techniques and Security Measures to Mitigate and Overcome Online Banking Frauds

As online banking frauds grow in sophistication, banks and individuals must employ advanced tools and techniques to safeguard financial transactions and data. Below are key approaches to mitigating digital and online banking fraud:

For Banks

- **Strengthen with Advanced Cybersecurity Frameworks:** Use advanced and latest firewalls, intrusion detection systems, and encryption technologies for Bank's Servers and banking infrastructures.
  - **Firewall and Intrusion Detection Systems (IDS):** Protect against unauthorized access and malicious activities.
  - **Encryption:** Encrypt sensitive data during storage and transmission to prevent unauthorized access.
  - **Secure Socket Layer (SSL) Certificates:** Ensure secure communication between users and banking websites.

- **Two-Factor and multi-factor Authentication (2FA):** Implement OTPs, biometrics (fingerprint and facial recognition), or app-based authenticators for all transactions in banking mobile apps and its web applications.

- **Secure Payment Channels**: Encourage the use of tokenization and secure payment gateways for online transactions. Use sandbox environments for testing new applications or features without exposing live systems.
- **Regular Security Audits:** Conduct vulnerability assessments and penetration testing to identify and mitigate risks with security experts. Conduct frequent vulnerability assessments to identify system weaknesses. Ensure compliance with regulatory standards like GDPR, PCI DSS, or local cybersecurity norms.
- **Transaction Monitoring with Fraud Detection Systems:** Fraud detection systems analyze transaction patterns and identify anomalies in real-time. Implement systems that monitor high-value or unusual transactions, flagging them for manual review. Use AI and machine learning to monitor and flag suspicious banking transactions in real time.
- **Customer Awareness Campaigns:** Educate customers on recognizing phishing attempts, securing devices, and avoiding public Wi-Fi for transactions. Provide tips on avoiding suspicious links, emails, or calls.
- **Robust Internal Controls of Database:** Implementing strong internal controls helps detect and prevent fraud by ensuring that all transactions are properly authorized and recorded.
- **Collaborative Strategies:** Engaging in consortium-based collaboration and sharing intelligence with other financial institutions can help detect and prevent fraud more effectively.
- **Proactive Risk Assessment:** Conducting proactive risk assessments to identify potential threats and vulnerabilities and implementing tailored controls to mitigate them.

For Customers

1. **Use Strong Passwords:** Create complex passwords with a mix of letters, numbers, and special characters, and change them regularly. Avoid sharing passwords or storing them in unsecured locations.

   Example: Avoid using easily guessable and predictable passwords like "password123" and opt for stronger passwords like "A1b2C3d4!".
2. **Enable Two-Factor Authentication (2FA):** Add an extra layer of security by requiring a second form of verification, such as an OTP or biometric authentication.

   Example: Enable 2FA on banking apps to ensure that transactions require verification through a secondary device or biometric scan.
3. **Verify Apps and Links:** Only download official apps from trusted sources and avoid clicking on suspicious links.
4. **Regularly Monitor Account Activity:** Regularly check bank statements and transaction alerts and its history for unauthorized activity.

   Example: Set up transaction alerts to receive notifications for every transaction made using your account.
5. **Avoid Sharing Sensitive Information:** Never share PINs, passwords, or OTPs with anyone, even if they claim to be from the bank.
6. **Install Security Software and secure devices:** Use antivirus and anti-malware programs and run regular scans to detect and remove malware to protect devices. Update operating systems, and enable device-level encryption.
7. **Avoid Public Wi-Fi for Transactions:** Use secure, private networks for online banking to prevent interception of sensitive information. Avoid conducting banking transactions over public Wi-Fi at cafes or airports. Use a Virtual Private Network (VPN) for secure connections.
8. **Report Suspicious Activity:** Immediately report any suspicious activity to your bank and relevant authorities. Inform the bank or relevant authorities at the earliest sign of suspicious activity. Block cards or accounts if unauthorized transactions are detected.

   Example: If you notice unauthorized transactions, contact your bank's fraud department and file a report and FIR to the nearest cyber cell.

9. **Be cautious and alert to Unsolicited Calls and Emails:** Do not share personal information unless you can verify the identity of the caller or sender. Be cautious of emails or calls asking for your banking credentials or personal information, and contact your bank directly to verify any suspicious requests.
10. **Educate Yourself and Others:** Stay informed about the latest fraud techniques and share this knowledge with family and friends. Stay informed about the latest fraud techniques and share this knowledge with family and friends.

    Example: Attend webinars or read articles on online banking security to stay updated on new threats and prevention measures.

By staying vigilant and adopting these security measures, you can significantly reduce the risk of falling victim to online banking frauds.

9.2.1 Emerging Trends & Technologies to Combat Fraud

- **Blockchain Technology:** It ensures transparency and immutability in transactions, reducing the risk of tampering or fraud.
- **Biometric Authentication:** Biometric authentication techniques like Fingerprint, voice, or iris recognition provides an additional layer of security, reducing reliance on passwords.
- **Real-Time Threat Intelligence:** Share threat data across financial institutions to identify and counteract evolving fraud techniques.
- **Tokenization:** Replace sensitive card details with tokens, reducing the risk of data breaches during transactions.
- **Behavioral Biometrics:** Monitor keystroke patterns, mouse movements, or navigation habits to detect anomalies.

9.3 Case Studies Related to Banking Frauds

Indian Banking Fraud

- **Cosmos Bank Cyber Attack (2018):** Hackers infiltrated the bank’s ATM server and conducted unauthorized transactions globally. Cosmos Bank was the victim of a cyber-attack on August 11 and 13, 2018, where hackers stole over ₹94 crore. Hackers used malware to steal information about customers' VISA and Rupay cards. Hackers attacked the bank's SWIFT system. Hackers attacked the bank's ATM switch server and withdrew ₹78 crore from ATMs in 28 countries. Hackers used the proxy SWIFT system to transfer ₹13.92 crore to a Hong Kong-based bank.
    - **Modus Operandi:** Malware attack allowed fraudsters to steal customer card details.
    - **Impact:** Loss of INR 94 crore; highlighted vulnerabilities in server-level security.
    - In April 2023, a Pune court convicted 11 people in connection with the cyber fraud case. The accused were charged under the Indian Penal Code and Information Technology Act.
- **PNB Nirav Modi Scam (2018):** Nirav Modi and Mehul Choksi orchestrated a fraud involving over ₹14,000 crore (approx. $2 billion) through fraudulent Letters of Undertaking (LoUs) issued by Punjab National Bank employees.

  Impact: Massive financial losses and regulatory scrutiny on internal controls in Indian banks. Significant financial loss to the bank, loss of investor confidence, and stricter regulatory measures introduced.
- **Yes Bank Fraud (2020):** Yes Bank reported a fraud of ₹1,000 crore (approx. $135 million) involving Dewan Housing Finance Corporation Limited (DHFL) and Yes Bank, where funds were diverted for personal gain.

  Impact: Losses for investors, increased scrutiny on banking practices, and regulatory reforms.
- **Vijay Mallya Fraud Case:** Vijay Mallya, a former chairman of United Spirits and United Breweries Group, is accused of bank fraud and money laundering. Vijay Mallya defrauded

banks of over ₹9,000 crore through Kingfisher Airlines. He and his companies have been involved in financial scandals since 2012. Here are some of the allegations against Mallya:

Loan fraud-Mallya is accused of routing loans from 17 Indian banks to gain a stake in companies around the world. The Central Bureau of Investigation (CBI) is investigating a ₹900 crore loan fraud case involving Mallya and Kingfisher Airlines. The CBI alleges that Mallya conspired with a senior IDBI Bank official to sanction a ₹150 crore loan to Kingfisher Airlines in 2009.

Money laundering-The Enforcement Directorate (ED) filed a money laundering case against Mallya in 2016 for allegedly sending ₹9 billion abroad from loans given to his airline. Mallya left India in 2016 to move to Britain, but the Westminster Magistrates Court ordered his extradition to India. The UK High Court confirmed the order, and Mallya has been denied permission to appeal in the UK Supreme Court. Mallya was declared a fugitive under the Fugitive Economic Offenders Act in 2019. Non-bailable warrant. A Mumbai Special Court issued a non-bailable warrant against Mallya for a ₹180 crore loan default.

- **Paytm KYC Scam (2020):** Fraudsters posed as Paytm executives to collect KYC details from users.

  Modus Operandi: Phishing and social engineering.

  Impact: Financial losses for several users and increased scrutiny on e-wallet security.

  - **VMC Systems Limited Fraud (2021):** VMC Systems Limited defrauded Punjab National Bank of over ₹1,000 crore.
  - **Satyam Scam (2009):** A corporate fraud where fake bank statements were used to inflate revenues and profits. Highlighted the lack of stringent auditing practices in India.

International Banking Fraud

- **Bangladesh Bank Heist (2016):** Hackers used SWIFT credentials to transfer USD 81 million from Bangladesh Bank's account at the Federal Reserve Bank of New York.

  Modus Operandi: Exploited weak security in the bank's SWIFT system.

  Impact: Highlighted the need for robust international banking security protocols.
- **Capital One Data Breach (2019):** Personal and financial data of over 100 million customers were exposed.

  Modus Operandi: A former employee exploited a misconfigured web application firewall.

  Impact: Affected customer trust and led to stricter data protection regulations.
- **Wirecard Scandal (2020):** A German payment processing company falsely inflated its balance sheets by EUR 1.9 billion, involving banking and audit irregularities.

  Impact: Collapse of Wirecard AG and increased focus on auditing and financial transparency globally.
- **Wells Fargo Fake Accounts Scandal (2016):** Bank employees created millions of fake accounts to meet sales targets. It impacted the significant penalties and a decline in customer trust.
- **Equifax Data Breach (USA, 2017):** A massive data breach at Equifax exposed personal information of 147 million people, including Social Security numbers, birth dates, and addresses. It impacted the increased incidents of identity theft, significant financial and reputational damage to Equifax, and heightened awareness of data security.
- **WannaCry Ransomware Attack (Global, 2017):** A ransomware attack that infected over 200,000 computers across 150 countries, encrypting data and demanding ransom payments in Bitcoin. It impacted the disruption of businesses and healthcare services, financial losses, and increased focus on cybersecurity measures.

Summary

Digital and online banking frauds are increasing due to technological advancements and widespread digital adoption.

➔ **Introduction to Different Types of Digital and Online Banking Frauds:**

- Phishing, Vishing (Voice Phishing), Skimming, SIM Swap Fraud, Malware, MitM Attacks, Account Takeover, Ransomware.

➔ **Types of Digital and Online Banking Frauds and Their Causes:**

- Phishing: Fake websites, emails or SMS messages to steal sensitive information.
- Vishing: Voice-based scams, Fraudulent calls posing as bank officials.
- Skimming: Devices on ATMs/POS terminals to capture card details.
- SIM Swap: Tricking carriers into transferring a victim's phone number.
- E-wallet/UPI Fraud: Unauthorized digital wallet transactions.
- Fake Apps: Fraudulent apps mimicking legitimate banking apps.
- Malware Attacks: Malicious software to steal data.
- MitM Attacks: Intercepting communication between user and bank.
- Account Takeover: Unauthorized access to bank accounts.
- Ransomware: Encrypting data and demanding ransom.

➔ **Tools and Security Measures to Mitigate and Overcome Online Banking Frauds:**

- For banks: Strengthened cybersecurity, 2FA, fraud detection systems, customer education.
- For customers: Strong and complex passwords with regular changes, verified apps, secure devices, avoiding public Wi-Fi.
- Complex passwords with regular changes.
- Enable Two-Factor Authentication (2FA): Additional layer of security.
- Regularly Monitor Accounts: Frequent checks for unauthorized activity.
- Avoid Public Wi-Fi for Transactions: Use secure networks.
- Install Security Software: Antivirus and anti-malware programs.
- Be Wary of Unsolicited Calls and Emails: Verify identities before sharing information.
- Educate Yourself and Others: Stay informed about fraud techniques.
- Report Suspicious Activity: Inform banks and authorities immediately.

➔ **Case Studies Related to Digital and Online Banking Frauds:**

- PNB Scam (India, 2018): Fraud involving ₹14,000 crore through fraudulent LoUs.
- Yes Bank Fraud (India, 2020): Fraud of ₹1,000 crore involving DHFL.
- Cosmos Bank attack, Paytm KYC scam.
- Bangladesh Bank heist, Capital One breach.
- Equifax Data Breach (USA, 2017): Exposure of 147 million personal records.
- WannaCry Ransomware Attack (Global, 2017): Infection of 200,000 computers across 150 countries.

Practical Activity 9.1

Objective: Learners will learn how fraudulent calls claiming Know Your Customer (KYC) verification can lead to bank account compromise.

Tools & Platform Needed: Laptop/Desktop/Smartphone with internet access

Procedure:

Step 1: Divide students into teams.

Step 2: Simulate a phone call where the scammer demands banking details under the guise of KYC updating.

Step 3: Develop and enact a role-play scenario.

Step 4: Include call transcripts and screenshots for complaint filing.

Step 5: Record complaint number and follow up.

Step 6: Create a slide-based presentation with step-by-step documentation.

Practical Activity 9.2

Objective: Learners will recognize how digital payment breaches can lead to unauthorized card transactions.

Tools & Platform Needed: Laptop/Desktop/Smartphone with internet access

Procedure:

Step 1: Form teams of 3-4 learners.

Step 2: Simulate a situation where a student's card data is stolen through an insecure website.

Step 3: Role-play the unauthorized purchase scenario.

Step 4: Include payment logs and mock screenshots.

Step 5: Record complaint reference and track progress.

Step 6: Present group insights with supporting visuals and learnings.

List of other suggested practical activities:

- **SIM Swap Scam:** It is a Cyber Crime related to Mobile number porting fraud used to access banking OTPs.
  Simulated Scenario: Scammers impersonate the victim to request a new SIM and gain access to transaction OTPs for fraudulent banking transfers.
  Additional Notes: Create scripts/dialogue for telecom interaction.
- **Fake Loan Approval Portal:** Identity theft via fake loan portal
  Simulated Scenario: Group explores a fraudulent website that offers instant loan approvals but harvests PAN/Aadhar details.
  Additional Notes: Use screenshots/mock forms for the portal.
- **Unauthorized Card Transactions:** Card cloning/data breach resulting in fraudulent purchases
  Simulated Scenario: Victim's card info is stolen after using it on a compromised merchant site and used for multiple online purchases.

Additional Notes: Showcase how digital payment safety could prevent this.

ASSESSMENT

Multiple Choice Questions (MCQs)

1. What is phishing?
   a) A technique to enhance online security.
   b) A fraudulent attempt to obtain sensitive information.
   c) A method of sending encrypted emails.
   d) A type of antivirus software.

2. What does vishing involve?
   a) Sending fake emails.
   b) Using malicious software.
   c) Making fraudulent phone calls.
   d) Capturing card details at ATMs.

3. How do fraudsters conduct skimming?
   a) By intercepting emails.
   b) By installing devices on ATMs or POS terminals.
   c) By hacking into bank accounts.
   d) By sending fake SMS messages.

4. What is SIM Swap fraud?
   a) Changing a phone number without user consent.
   b) Transferring a phone number to a new SIM card.
   c) Sending malicious emails.
   d) Encrypting data on a device.

5. What is Man-in-the-Middle (MitM) attack?
   a) Attacks that target mobile applications.
   b) Intercepting and manipulating communication between two parties.
   c) Sending malware to bank servers.
   d) Monitoring user activities on social media.

6. What is account takeover fraud?
   a) Opening new accounts with stolen identities.
   b) Unauthorized access to existing bank accounts.
   c) Installing skimming devices on ATMs.
   d) Sending phishing emails to users.

7. What is a key measure to secure online banking transactions?
   a) Using short, simple passwords.
   b) Enabling Two-Factor Authentication (2FA).
   c) Disabling security software.
   d) Using public Wi-Fi networks.

8. What should users do if they notice suspicious activity in their accounts?
   a) Ignore it.
   b) Report it to the bank and relevant authorities.
   c) Share their account details on social media.
   d) Change their passwords immediately.

9. Which attack involves intercepting communication between a user and the bank?
   a) Phishing
   b) MITM
   c) Vishing
   d) SIM swapping

10. Phishing attempts typically occur via:
    a) Phone calls
    b) SMS
    c) Emails
    d) All of the above

11. Which tool can detect unauthorized access in real-time?
    a) Machine learning-based fraud detection systems
    b) Basic firewalls
    c) Regular password updates
    d) Manual transaction monitoring

12. OTPs are commonly intercepted during:
    a) SIM swapping attacks
    b) Card cloning
    c) Phishing scams
    d) Malware attacks

Fill in the Blanks

1. _______ involves creating fake websites or emails to steal sensitive information.
2. Fraudsters make fraudulent phone calls in _______ attacks.
3. Devices installed on ATMs to capture card details are known as _______ devices.
4. _______ attacks involve intercepting communication between users and banks.
5. Malicious software used to steal data is referred to as _______.
6. _______ fraud involves tricking mobile carriers into transferring a phone number.
7. The WannaCry attack was a type of _______ attack.
8. Regularly monitoring accounts helps in detecting _______ activity.
9. ______ involves fraudulent emails to steal sensitive data.
10. Two-factor authentication adds a layer of security by requiring ______.
11. Fraudulent apps mimicking legitimate apps are called ______.
12. Malware attacks often result from clicking on ______ links.
13. Fraudsters use ______ to duplicate SIM cards.
14. Card skimming typically occurs at ______ terminals.
15. ______ detection systems can help banks identify unusual activity.

True/False

1. Phishing attacks use voice calls to trick victims.
2. Two-factor authentication eliminates all risks of fraud.
3. Malware attacks can compromise banking credentials.
4. SIM swapping relies on technical hacking alone.
5. Fraud detection systems use AI to flag suspicious transactions.
6. Card skimming is only possible with physical access to the card.
7. Avoiding public Wi-Fi reduces the risk of MITM attacks.
8. Fake apps are always identified by antivirus software.
9. Skimming devices are installed on ATMs to capture card details.
10. Man-in-the-Middle (MitM) attacks involve encrypting data on devices.
11. SIM Swap fraud involves transferring a phone number to a new SIM card.
12. Malware can infect devices and steal sensitive information.
13. Using public Wi-Fi networks for online banking enhances security.
14. Enabling Two-Factor Authentication (2FA) provides an extra layer of security.
15. Reporting suspicious activity is unnecessary if no funds are lost.

Short Answer Questions

1. Describe how vishing is conducted and its impact on victims.
2. What is the significance of Two-Factor Authentication (2FA) in online banking security?
3. How does malware pose a threat to digital and online banking?
4. Explain the concept of account takeover fraud and its consequences.
5. What is phishing, and how does it affect online banking security?
6. Describe the modus operandi of SIM swapping fraud.

7. Why is customer education essential in preventing online banking frauds?
8. List three critical measures banks should adopt to combat digital frauds.

Long Answer Questions

1. Discuss the different types of digital and online banking frauds, their causes, and how they impact individuals and financial institutions. Provide examples for each type.
2. Analyze case studies related to digital and online banking frauds, such as the PNB scam, Yes Bank fraud, and Equifax data breach. Discuss the implications and lessons learned from these cases.
3. Describe the various security measures that can be implemented to mitigate and overcome online banking frauds. How can individuals and organizations stay vigilant and protect themselves from such threats?
4. Discuss the role of customer awareness and technological advancements in mitigating online banking frauds.

Answer Key

Multiple Choice Questions

1. b, 2. c, 3. b, 4. b, 5. b, 6. b, 7. b, 8. b, 9. b, 10. d, 11. a, 12. a

Fill-in-the-blanks

1. phishing, 2. vishing, 3. skimming, 4. Man-in-the-Middle, 5. malware,
6. SIM swap, 7. ransomware, 8. suspicious, 9. phishing, 10. two factors, 11. spoofed apps, 12. malicious, 13. SIM cloning, 14. POS, 15. fraud

True/False questions

1. False, 2. False, 3. True, 4. False, 5. True, 6. True, 7. True, 8. False, 9. True, 10. False, 11. True, 12. True, 13. False, 14. True, 15. False

Chapter-10

Introduction to Cyber Crime and Cyber Law

In the Silicon Valley of India -Bengaluru, a 35-year-old software engineer named Rajesh found himself tangled in a web of deceit that would lead to a loss of ₹11.8 crore. The incident began on an ordinary day, November 11th, when Rajesh received a call from an individual claiming to be an officer from the Telecom Regulatory Authority of India (TRAI). The so-called officer informed Rajesh that his SIM card, linked to his Aadhaar card, was allegedly being misused for illegal advertisements and harassing messages. The tone of the caller was authoritative, and the accusations were grave. Rajesh was then told that a case had been registered in connection with this in Mumbai's Colaba Cyber Police Station.

As days passed, Rajesh received another alarming call, this time from someone claiming to be a police officer. The caller alleged that Rajesh's Aadhaar details were being used to open multiple bank accounts for money laundering. The situation seemed to escalate quickly, with the caller warning Rajesh to keep the matter confidential and threatening physical arrest if he did not cooperate with the ongoing "virtual investigation."

In a state of panic, Rajesh received instructions to download the Microsoft Skype app. Soon after, a man dressed in a Mumbai police uniform video-called him, asserting that a businessman had used Rajesh's Aadhaar card to conduct transactions worth ₹6 crore. The fear of legal repercussions gripped Rajesh as another call came in on November 25th. This time, the alleged police officer claimed that Rajesh's case was being heard in the top court and threatened to arrest his family if he did not comply.

The fraudsters cited fake Reserve Bank of India (RBI) guidelines and demanded Rajesh to transfer funds to certain accounts for "verification purposes" to avoid further legal consequences. Driven by fear and confusion, Rajesh transferred a total of ₹11.8 crore in multiple transactions to various bank accounts over a period of time.

However, when the demands for money persisted, Rajesh began to suspect that he had fallen into a digital trap. Realizing the gravity of the situation, he lodged a complaint with the police. The authorities registered a case under the IT Act and relevant sections of the Bharatiya Nyaya Sanhita (BNS) for cheating and impersonation. The investigation is ongoing as the cyber-crime cell works diligently to bring the perpetrators to justice.

Rajesh's story serves as a stark reminder of the perils of digital arrest and the importance of vigilance in the face of cyber threats. The cyber-crime cell's swift response and the ongoing investigation underscore the critical role of law enforcement in combating such sophisticated digital arrest scams.

10.1 Introduction to Cyber Crime

Cyber-crime refers to illegal and criminal activities conducted through digital platforms, computers, the internet or other digital technologies. It includes hacking, identity theft, phishing, cyberstalking, online harassment, and financial fraud. With the rapid adoption and expansion of digital technologies, cyber-crimes have become a national and global issue, refer Figure 10.2 National Crime Records Bureau (NCRB) Report 2022, how cyber-crimes are growing year by year. These crimes can target individuals, businesses, and governments, resulting in financial loss, data breaches, and reputational damage. Cybercrime can have serious consequences, including financial loss, reputational damage, and emotional distress. There is a requirement of robust legal frameworks and security measures to combat it.

Key Characteristics of Cyber Crime:

- Involves digital devices like computers, smartphones, and networks.
- Can be committed from remote locations.
- Leaves digital footprints that can be traced.
- Affects confidentiality, integrity, and availability of data.

10.1.1 Types of Cyber Crime & Cyber Fraud

Cyber Crime Against Individuals:

- **Phishing:** Fraudsters send fake emails or messages that appear legitimate to steal sensitive information like passwords, credit card numbers, and personal details. using fake emails or websites to trick people into revealing sensitive information
- **Cyber Stalking:** Using the internet to harass or stalk individuals, often causing emotional distress. It is unauthorized tracking, surveillance and intimidation using digital technologies to stalk or harass others.
- **Identity Theft:** Stealing personal information such as names, addresses, and credit card numbers to commit fraud or other crimes. Making fake profiles on social media.
- **Online Harassment:** Online Bullying or harassing individuals intimidate, or threaten others through social media, forums, or other online platforms, digital technologies.

Cyber Crime Against Property:

- **Financial Cyber Crime:** Credit Card and other banking fraud to make unauthorized purchases, payments, transfer of money and digital transactions.
- **Intellectual Property Theft:** Stealing or using someone else's intellectual property without permission. Piracy, counterfeit software.
- **Internet Time Theft:** Using someone's internet services without their knowledge, often by hacking into their network.
- **Ransomware Attacks:** Infecting computers with malware that encrypts data and demanding a ransom to decrypt it. using malware to encrypt files and demand payment in exchange for the decryption key

Cyber Crime Against Organizations:

- **Hacking and Data Breaches:** Gaining unauthorized access to computer systems or networks to steal information or cause damage.
- **Denial of Service (DoS) Attacks:** Overloading a system with traffic to make it unavailable to users.

Cyber Crime Against Society:

- **Cyber Terrorism:** Using digital technologies to conduct terrorist activities, such as disrupting critical infrastructure. Attacks on critical infrastructure and spreading extremist propaganda.
- **Web Jacking:** Taking control of a website for malicious purposes.
- **Cyber Espionage:** Unauthorized access to sensitive government or corporate data

- **Cyber Fraud:** Using digital technologies to commit fraudulent activities, such as online scams and auction fraud
- **Content-related Crime:** Spreading Misinformation, distributing false information to deceive the public, spreading fake news, morphed videos, images, hate speech.

💡**Points to remember:**

- **Cybercrime** refers to any illegal and criminal activities conducted through digital platforms, computers, the internet or other digital technologies. Targets individuals, businesses, and governments.
- **Types of Cyber Crime & Cyber Fraud:**
  - **Against Individuals:** Phishing, cyber stalking, identity theft, online harassment.
  - **Against Property:** Credit card fraud, all financial fraud digitally, intellectual property theft, internet time theft, ransomware attacks.
  - **Against Organizations:** Hacking, denial of service (DoS) attacks, data breaches.
  - **Against Society:** Cyber terrorism, web jacking, spreading misinformation, cyber espionage

10.2 Cyber Law

Cyber law, also known as Internet Law, governs the use of digital technologies and the internet. It encompasses a wide range of legal issues, including intellectual property, data protection, privacy, online contracts, cyber-crime and e-commerce frauds. Cyber laws aim to protect individuals and organizations from cyber-crimes and provide legal remedies for victims. It is a branch of law that deals with the regulation of digital technologies and the internet. It regulates digital activities and safeguard users from cyber-crimes.

10.2.1 Advantages of Cyber Law

- **Responsible digital behavior:** It promotes responsible digital behavior. It prepares a model code of conduct for the user of internet and digital technologies.
- **A framework for regulating digital technologies:** Cyber law provides a framework for regulating digital technologies and the internet. It enhances cybersecurity measures.
- **Legal Framework:** It provides a legal structure to address and prosecute cyber-crimes. Cyber law provides protections for individuals and businesses from cybercrime. It protects individuals and organizations from cyber fraud.
- **Promotes e-commerce and digital economy:** Cyber law promotes e-commerce and the digital economy by providing a secure and trusted environment for online transactions. It ensures legal recognition of electronic transactions.
- **Protection of Rights:** It safeguards individuals' and organizations' rights in the digital space.
- **Avoidance of cyber-crime:** It acts as a deterrent to potential cyber criminals by imposing penalties. It enables legal actions against cyber criminals.
- **Promotes Confidence:** It encourages the use of digital technologies by ensuring legal protections.

💡**Points to remember:**

- **Cyber law**, also known as Internet Law, governs the use of digital technologies and the internet.
- **Cyber law** provides a legal framework for regulating digital technologies, protects individuals and businesses from cybercrime, and promotes e-commerce and the digital economy.
- **Cyber law** covers intellectual property, data protection, privacy, e-commerce and many more similar aspects.

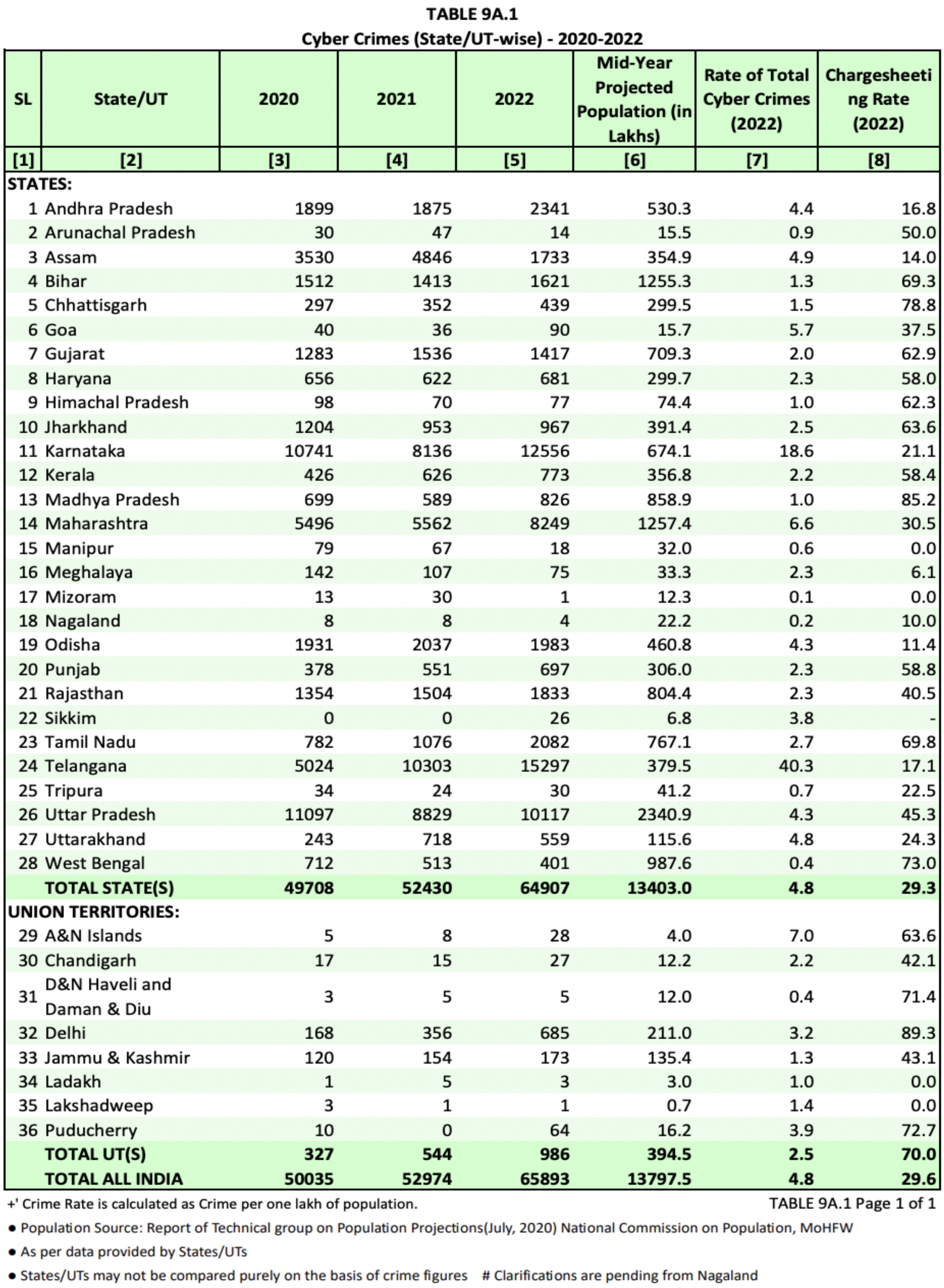


TABLE 9A.1

Cyber Crimes (State/UT-wise) - 2020-2022

SL	State/UT	2020	2021	2022	Mid-Year Projected Population (in Lakhs)	Rate of Total Cyber Crimes (2022)	Chargesheeting Rate (2022)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
STATES:							
1	Andhra Pradesh	1899	1875	2341	530.3	4.4	16.8
2	Arunachal Pradesh	30	47	14	15.5	0.9	50.0
3	Assam	3530	4846	1733	354.9	4.9	14.0
4	Bihar	1512	1413	1621	1255.3	1.3	69.3
5	Chhattisgarh	297	352	439	299.5	1.5	78.8
6	Goa	40	36	90	15.7	5.7	37.5
7	Gujarat	1283	1536	1417	709.3	2.0	62.9
8	Haryana	656	622	681	299.7	2.3	58.0
9	Himachal Pradesh	98	70	77	74.4	1.0	62.3
10	Jharkhand	1204	953	967	391.4	2.5	63.6
11	Karnataka	10741	8136	12556	674.1	18.6	21.1
12	Kerala	426	626	773	356.8	2.2	58.4
13	Madhya Pradesh	699	589	826	858.9	1.0	85.2
14	Maharashtra	5496	5562	8249	1257.4	6.6	30.5
15	Manipur	79	67	18	32.0	0.6	0.0
16	Meghalaya	142	107	75	33.3	2.3	6.1
17	Mizoram	13	30	1	12.3	0.1	0.0
18	Nagaland	8	8	4	22.2	0.2	10.0
19	Odisha	1931	2037	1983	460.8	4.3	11.4
20	Punjab	378	551	697	306.0	2.3	58.8
21	Rajasthan	1354	1504	1833	804.4	2.3	40.5
22	Sikkim	0	0	26	6.8	3.8	-
23	Tamil Nadu	782	1076	2082	767.1	2.7	69.8
24	Telangana	5024	10303	15297	379.5	40.3	17.1
25	Tripura	34	24	30	41.2	0.7	22.5
26	Uttar Pradesh	11097	8829	10117	2340.9	4.3	45.3
27	Uttarakhand	243	718	559	115.6	4.8	24.3
28	West Bengal	712	513	401	987.6	0.4	73.0
	TOTAL STATE(S)	**49708**	**52430**	**64907**	**13403.0**	**4.8**	**29.3**
UNION TERRITORIES:							
29	A&N Islands	5	8	28	4.0	7.0	63.6
30	Chandigarh	17	15	27	12.2	2.2	42.1
31	D&N Haveli and Daman & Diu	3	5	5	12.0	0.4	71.4
32	Delhi	168	356	685	211.0	3.2	89.3
33	Jammu & Kashmir	120	154	173	135.4	1.3	43.1
34	Ladakh	1	5	3	3.0	1.0	0.0
35	Lakshadweep	3	1	1	0.7	1.4	0.0
36	Puducherry	10	0	64	16.2	3.9	72.7
	TOTAL UT(S)	**327**	**544**	**986**	**394.5**	**2.5**	**70.0**
	TOTAL ALL INDIA	**50035**	**52974**	**65893**	**13797.5**	**4.8**	**29.6**

+' Crime Rate is calculated as Crime per one lakh of population. TABLE 9A.1 Page 1 of 1

- Population Source: Report of Technical group on Population Projections(July, 2020) National Commission on Population, MoHFW
- As per data provided by States/UTs
- States/UTs may not be compared purely on the basis of crime figures # Clarifications are pending from Nagaland

Fig: 10.1 National Crime Records Bureau (NCRB) Report 2022 Volume 2 Page No. 785

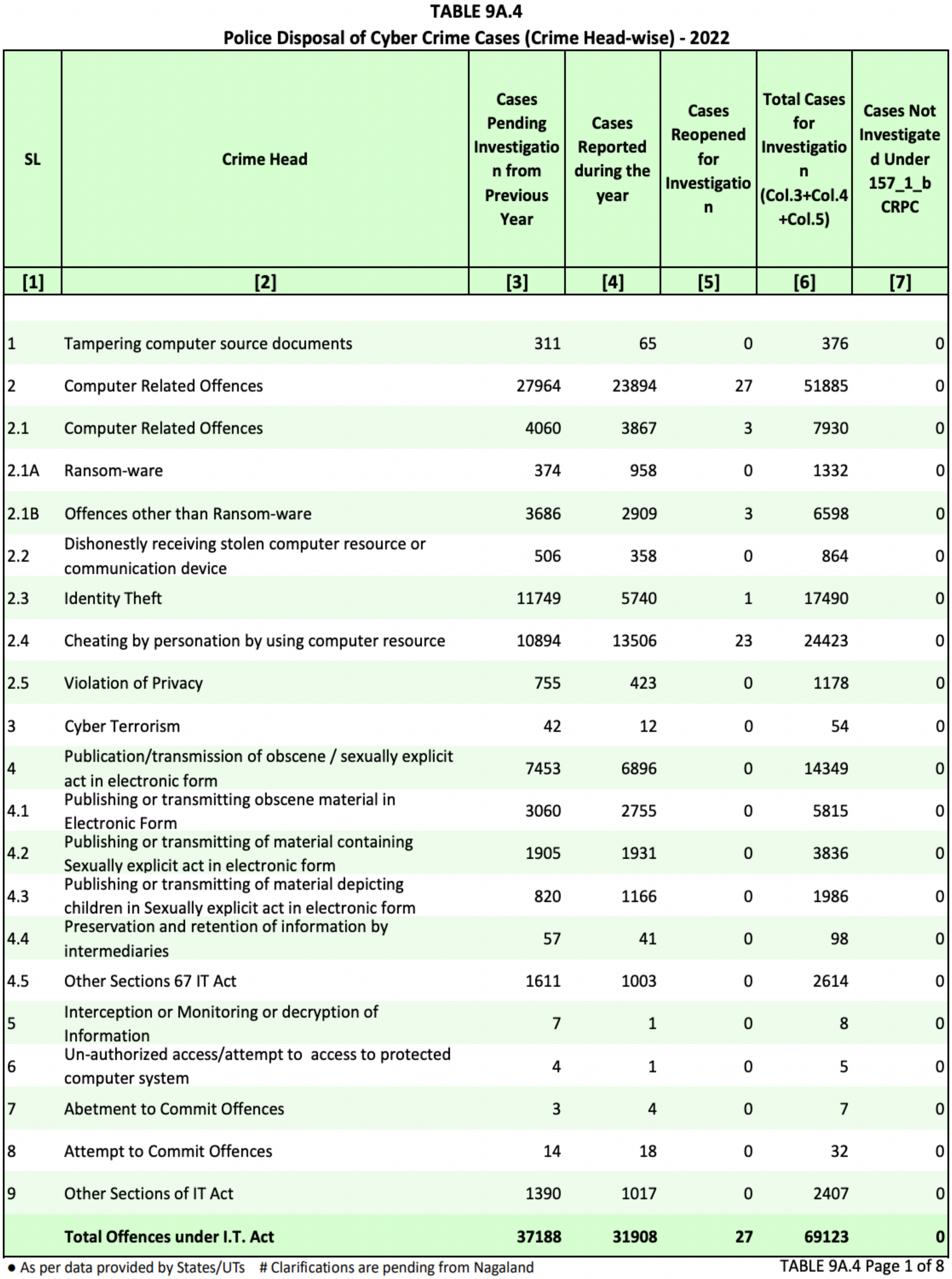


TABLE 9A.4

Police Disposal of Cyber Crime Cases (Crime Head-wise) - 2022

SL	Crime Head	Cases Pending Investigation from Previous Year	Cases Reported during the year	Cases Reopened for Investigation	Total Cases for Investigation (Col.3+Col.4+Col.5)	Cases Not Investigated Under 157_1_b CRPC
[1]	[2]	[3]	[4]	[5]	[6]	[7]
1	Tampering computer source documents	311	65	0	376	0
2	Computer Related Offences	27964	23894	27	51885	0
2.1	Computer Related Offences	4060	3867	3	7930	0
2.1A	Ransom-ware	374	958	0	1332	0
2.1B	Offences other than Ransom-ware	3686	2909	3	6598	0
2.2	Dishonestly receiving stolen computer resource or communication device	506	358	0	864	0
2.3	Identity Theft	11749	5740	1	17490	0
2.4	Cheating by personation by using computer resource	10894	13506	23	24423	0
2.5	Violation of Privacy	755	423	0	1178	0
3	Cyber Terrorism	42	12	0	54	0
4	Publication/transmission of obscene / sexually explicit act in electronic form	7453	6896	0	14349	0
4.1	Publishing or transmitting obscene material in Electronic Form	3060	2755	0	5815	0
4.2	Publishing or transmitting of material containing Sexually explicit act in electronic form	1905	1931	0	3836	0
4.3	Publishing or transmitting of material depicting children in Sexually explicit act in electronic form	820	1166	0	1986	0
4.4	Preservation and retention of information by intermediaries	57	41	0	98	0
4.5	Other Sections 67 IT Act	1611	1003	0	2614	0
5	Interception or Monitoring or decryption of Information	7	1	0	8	0
6	Un-authorized access/attempt to access to protected computer system	4	1	0	5	0
7	Abetment to Commit Offences	3	4	0	7	0
8	Attempt to Commit Offences	14	18	0	32	0
9	Other Sections of IT Act	1390	1017	0	2407	0
	Total Offences under I.T. Act	**37188**	**31908**	**27**	**69123**	**0**

● As per data provided by States/UTs # Clarifications are pending from Nagaland

TABLE 9A.4 Page 1 of 8

Fig: 10.2 National Crime Records Bureau (NCRB) Report 2022 Volume 2 Page No. 799

10.3 Indian IT Act (2000)

The Information Technology Act, 2000 (IT Act) is the primary law governing and dealing with cybercrime in India. The laws available in the IT Act regulate digital activities and safeguard users from cyber-crimes. It has following silent features:

➔ **Safeguards and penalties against Cyber Crime:** The Information Technology Act deals and provides safeguards and provisions of penalties, punishment against the following cyber-crimes:

- Tampering with computer Source Documents
- Hacking
- Publishing of Information, which is Obscene in Electronic Form
- Child Pornography
- Accessing Protected System or Breach of Confidentiality and Privacy
- Cyber Stalking
- Cyber squatting
- Data Diddling
- Cyber Defamation
- Trojan/virus/Worm Attack
- Forgery & Financial Crimes
- Internet Time Theft
- E-mail Bombing
- E-mail spoofing
- Salami Attack
- Web lacking

➔ **Power to Government:** It empowers the government to regulate and monitor unwanted and sensitive happenings over the Internet and other electronic forms.

The key powers:

1) Power of Interception (Sec 69)
2) Power of Blocking Website (Sec 69A)
3) Power to order Access to computer resources (Sec 69 B)

➔ **Proper Definitions of Computer related term**: It has clear cut definition computer terms related to cyber-crime. It defines computer, computer system, computer network, Data, electronic form, electronic record, Digital signature, Intermediary and many more such terms.

➔ **Legal recognition of electronic documents and records:** It specifies legal recognition of all types of electronic records, documents as evidence. It recognizes authentication of digital documents through digital signatures.

Example: It validates Email Communication, E-mail Addressee, Originator, Time and Place of dispatch and receive of electronic record, Delivering of Service. It legalizes retention of Electronic records and admissibility of Electronic Signature

➔ **Liability of Internet Service Provider, Subscriber and other authorities:** It fixes liability of ISP (Internet Service Providers), Controller of Certifying Authorities, defines function of controller, Licensing of certifying authorities. It defines rules and laws for the certifying authorities, subscribers, Adjudicating Officer, Cyber Appellate Tribunal, Civil Contravention etc.

➔ **Sections on Cyber contraventions and offences:**

- **Cyber Contraventions- (Chapter IX) – Section 43 - 47**

  (i) Section 43: unauthorized access to computer systems or networks (penalty: imprisonment up to 3 years and/or fine up to Rs. 5 lakhs)

- **Cyber offences- (Chapter XI) – Section 65 - 78**

  (i) Section 66: Computer-related offenses, such as hacking and unauthorized access (penalty: imprisonment up to 3 years and/or fine up to Rs. 5 lakhs).

  (ii) Section 66A: Sending offensive messages through communication service (penalty: imprisonment up to 3 years and/or fine) (Note: Section 66A was struck down by the Supreme Court of India in 2015).

  (iii) Section 67: Publishing or transmitting obscene information and material in electronic form (penalty: imprisonment up to 5 years and/or fine up to Rs.10 lakhs).

  (iv) Section 72: Breach of confidentiality and privacy (penalty: imprisonment up to 2 years and/or fine up to Rs. 1 lakh).

Points to remember:

- The **Indian IT Act**, 2000 is the primary law governing cybercrime in India. The IT Act provides penalties for various types of cybercrime, including hacking, publishing obscene information, and breach of confidentiality and privacy.
- The **Indian IT Act** (2000) provides legal frameworks with key sections like 43, 66, 67 & 72.

10.4 Need for Cyber Crime Cell

Cyber Crime Cells are specialized divisions of law enforcement dedicated to addressing cyber-crime cases. A cyber-crime cell is a specialized unit that deals with cybercrime investigations and prosecutions. The need for a cyber-crime cell arises from the increasing number of cybercrimes and the need for specialized skills and expertise to investigate and prosecute these crimes. Cyber Crime Cells are specialized units within law enforcement agencies dedicated to handling cyber-crime cases. They play a crucial role in investigating, preventing, and prosecuting cyber-crimes. The need for Cyber Crime Cells arises from the increasing complexity and sophistication of cyber-crimes, which require specialized skills and expertise.

Functions of Cyber Crime Cells:

- Investigation of cyber-crimes.
- Collection and analysis of digital evidence.
- Coordination with national and international agencies.
- Conducting cyber security awareness campaigns.

10.4.1 Cyber Fraud Helpline and Online Portals System in India

The Indian government has established a Cyber Fraud Helpline to assist victims of cyber fraud. This helpline allows individuals to report incidents of cyber fraud and seek immediate assistance. The helpline operates 24/7 and provides guidance on steps to take in case of a cyber fraud incident, including blocking compromised accounts and filing complaints with the relevant authorities. The Cyber Fraud Helpline assists victims of digital frauds. It provides real-time assistance, blocking fraudulent transactions. Referring to the NCRB crime report data 2022 on cyber-crime cases disposed of by police in figure 10.3, National Cyber Crime Reporting Portal facilitates immediate reporting of cyber fraud cases.

➔ **Helpline Number for cyber-crime and cyber fraud:** 1930

➔ **National Cyber Crime Reporting Portal:** www.cybercrime.gov.in

It is a comprehensive platform for reporting various types of cyber-crimes.

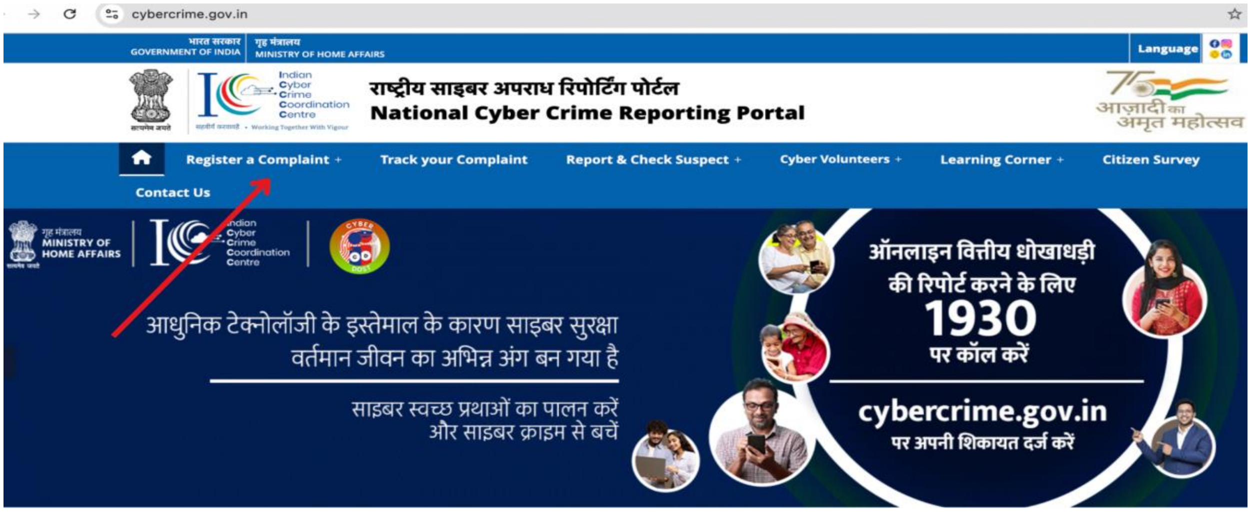

cybercrime.gov.in
भारत सरकार GOVERNMENT OF INDIA
गृह मंत्रालय MINISTRY OF HOME AFFAIRS
Language
Indian Cyber Crime Coordination Centre
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
आज़ादी का अमृत महोत्सव
Register a Complaint +
Track your Complaint
Report & Check Suspect +
Cyber Volunteers +
Learning Corner +
Citizen Survey
Contact Us
गृह मंत्रालय MINISTRY OF HOME AFFAIRS
आधुनिक टेक्नोलॉजी के इस्तेमाल के कारण साइबर सुरक्षा वर्तमान जीवन का अभिन्न अंग बन गया है
साइबर स्वच्छ प्रथाओं का पालन करें और साइबर क्राइम से बचें
ऑनलाइन वित्तीय धोखाधड़ी की रिपोर्ट करने के लिए
1930
पर कॉल करें
cybercrime.gov.in
पर अपनी शिकायत दर्ज करें

Fig: 10.3 Cyber Crime Reporting Portal Home Page

➔ **National Cyber Coordination Center (NCCC):** India's National Cyber Coordination Centre (NCCC) is an agency that monitors internet traffic and coordinates cybersecurity and electronic surveillance. The NCCC's purpose is to help India deal with malicious cyber activity by:

- Monitoring internet traffic
- Repelling domestic or international attacks
- Screening communication metadata
- Coordinating intelligence gathering activities

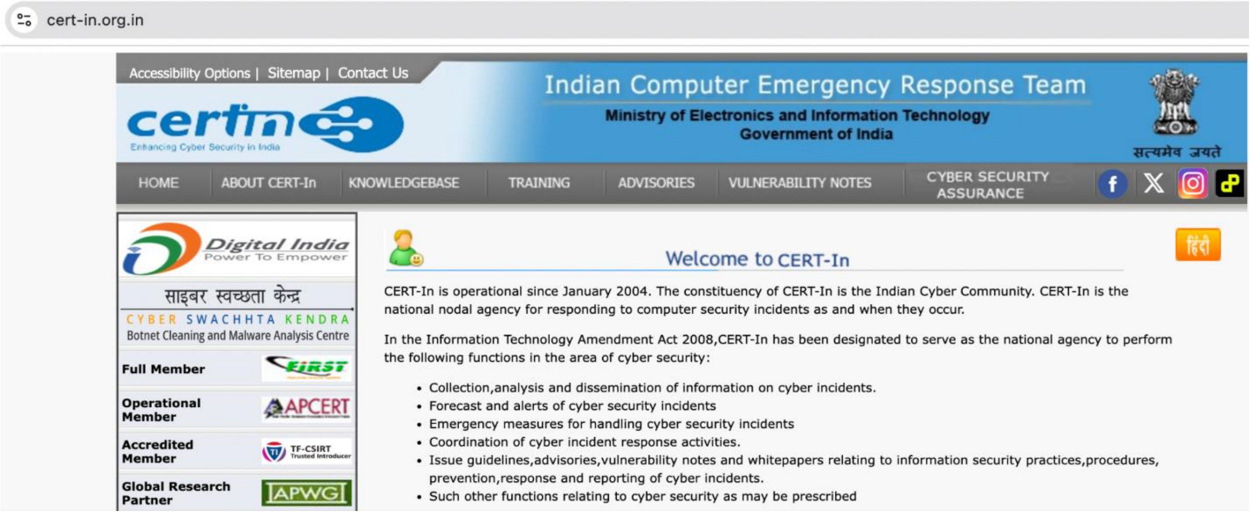
The NCCC's responsibilities include:

- Developing a cybercrime prevention strategy
- Providing cybercrime investigation training
- Reviewing outdated laws

The NCCC is governed by the Ministry of Home Affairs and collaborates with other agencies, including:

- Security and surveillance agencies
- CERT-In, which is part of the Ministry of Electronics and Information Technology

➔ **Indian Computer Emergency Response Team (CERT-In):** *www.cert-in.org.in*, It handles cybersecurity incidents and provides alerts and advisories.



Welcome to CERT-In

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection,analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

Fig: 10.4 Indian Computer Emergency Response Team Portal Home Page

➔ **Indian Cyber Crime Coordination Center (I4C):** *https://i4c.mha.gov.in/*

The Indian Cyber Crime Coordination Centre (I4C) is another agency in India established by the Ministry of Home Affairs (MHA) that deals with cybercrime. The I4C's purpose is to provide a framework for law enforcement agencies to deal with cybercrime in a coordinated manner. The I4C's responsibilities include:

- Improving coordination between law enforcement agencies and stakeholders
- Driving change in India's overall capability to tackle cybercrime
- Improving citizen satisfaction levels

Anyone can access I4C social media pages as mentioned below to report cyber-crime and take help:

X: *https://x.com/CyberDost*
Facebook: *https://www.facebook.com/CyberDostI4C*
Instagram: *https://www.instagram.com/CyberDostI4C/#*
Youtube: *https://www.youtube.com/c/CyberDostI4C*

i4c.mha.gov.in
भारत सरकार
GOVERNMENT OF INDIA
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
Indian Cyber Crime Centre
IndiaAI CyberGaurd AI Hackathon
Working Together With Vigour
सत्यमेव जयते
भारतीय साइबर अपराध समन्वय केंद्र
Indian Cybercrime Coordination Centre (I4C)
About Us
Verticals of I4C
Awareness & Capacity Building
Publications & Events
Digital India
INDIAai
CyberGuard

Fig: 10.5 Indian Cyber Coordination Center(I4C) Portal Home Page

➔ **Cyber Crime Investigation Cell:** Cyber-crime investigation cells have been set up at district level to address cyber-crime cases.

Example: Delhi Police Cyber Crime Unit

- Investigates and prosecutes cyber-crime cases within Delhi.

These platforms and helplines aim to provide immediate assistance and facilitate prompt investigation of cyber-crime cases. The Government of India (GOI) has taken numerous steps to spread awareness about cyber-crime. These include disseminating messages through SMS, caller tunes, social media accounts (e.g., X, Facebook, Instagram, Telegram), and radio campaigns. They have partnered with MyGov for multi-medium publicity, organized Cyber Safety and Security Awareness weeks with States/UTs, published a handbook for adolescents/students, and placed newspaper advertisements on digital arrest scams. Announcements in metros trains, use of social media influencers, and digital displays at railway stations and airports are also part of the awareness campaign.

Points to remember:

- **Need of Cyber Crime Cell:** A cyber-crime cell is a specialized unit in law enforcement that deals with cybercrime investigations and prosecutions. Cyber Crime Cells investigate cyber-crimes, collect evidence, and raise awareness.
- **Cyber Crime Cell** investigates, prevents, and prosecutes cyber-crimes. It addresses the complexity and sophistication of cyber-crimes.
- **Designated Cyber Fraud Helpline Number:** 1930
- **National Cyber Crime Reporting Portal in India:** *www.cybercrime.gov.in* provides assistance.

Practical Activity 10.1

Objective: Learners will explore and learn how to report a cybercrime incident using the designated helplines and online portals.

Tools & Platform Needed: Laptop/Desktop/Smartphone with internet access

Procedure:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group to explore a particular cyber-crime as discussed in chapter.

Step 3. Identify and Create a Simulated Cyber Crime Incident, scenario and role-play for different types of cyber-crimes, such as receiving a phishing email, digital arrest, identity theft, cyber defamation, fake job offer or experiencing a data breach.

Step 4. Access and go to the National Cyber Crime Reporting Portal:

htttps://www.cybercrime.gov.in

Step 5. Register on the portal using your email address and mobile number.

a) Log in to the portal and select the option to report a cyber-crime incident.

b) Provide details of the simulated incident, including the nature of the crime, date and time, and any evidence (e.g., screenshots of phishing emails).

Step 6. Follow Up on the Complaint:

a) Note the complaint reference number provided by the portal.

b) Follow up with the relevant authorities using the contact information provided.

Step 7. Document the above steps: Each group will showcase their findings in the form of presentation slides with screenshots in front of class. Describe each step taken to report the cyber-crime incident. Note any challenges encountered and how they were resolved.

Practical Activity 10.2

Objective: Learners will study, explore and analyse a real-world cybercrime incident that happened in the recent past and understand the application of cyber laws.

Tools & Platform Needed: Laptop/Desktop/Smartphone with internet access, IT Act 2000 documents (*https://www.meity.gov.in/content/information-technology-act-2000*)

Procedure:

Step 1. Divide the class into groups of 3-4 students.

Step 2. Assign each group to explore a particular real world cyber-crime case as case study.

Step 3. Ask them to analyze the incident: Analyse as per attack vector, damage caused, legal actions taken.

Step 4. Discuss the application of relevant cyber laws and penalties imposed.

Step 5. Students will gain insight into real-world cybercrime cases and understand the legal framework for addressing them.

Step 6. Document the above steps: Each group will showcase their findings in the form of presentation slides with screenshots in front of class. Describe each step of the cyber-crime incident. Note any challenges encountered and how they were resolved.

List of other suggested practical activities:

- **Creating a Cyber Security Policy Document:** To understand the importance of cyber security policies and create a basic policy document for an organization. Ensure the policy complies with relevant cyber laws and standards.
- **Real Case Study based on digital arrest:** To explore how digital arrest is happening, identify causes and aftermath. Prepare a report and present to the class.
- **Cyber Law for social media:** Prepare a report on cyber law applicable to social media platforms and present to class.
- **NCRB Cyber-crime report analysis:** Analyse cyber-crime on different angle from referring to latest NCRB report

Summary

- Introduction to Cyber Crime: Cybercrime refers to any criminal activity that involves the use of computers, the internet, or other digital technologies.
  - Illegal activities using computers, the internet, or digital technologies.
  - Targets individuals, businesses, and governments.
  - Refer Cyber Crimes Data from NCRB Report: *https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf*
- Types of Cyber Crime & Cyber Fraud:
  - Against Individuals: Phishing, cyber stalking, identity theft, online harassment.
  - Against Property: Credit card fraud, all financial fraud digitally, intellectual property theft, internet time theft, ransomware attacks.
  - Against Organizations: Hacking, denial of service (DoS) attacks, data breaches.
  - Against Society: Cyber terrorism, web jacking, spreading misinformation, cyber espionage
- Different Cybercrime Classifications:
  - Cybercrime can be classified based on targets computer-related crimes, computer-based crimes, and computer-assisted crimes. Financial crime, identity crime, content-related crime, cyber terrorism, intellectual property crime, and privacy invasion.
- Overview of Cyber Law:
  - Cyber law, also known as internet law, is a branch of law that deals with the regulation of digital technologies and the internet. Cyber laws offer protection, legal recognition, and enhance cybersecurity.
  - Cyber law provides a framework for regulating digital technologies, protects individuals and businesses from cybercrime, and promotes e-commerce and the digital economy.
  - Covers intellectual property, data protection, privacy, e-commerce.
- Indian IT Act and Sections with Penalties: The Indian IT Act, 2000 is the primary law governing cybercrime in India. The IT Act provides penalties for various types of cybercrime, including hacking, publishing obscene information, and breach of confidentiality and privacy.
- The Indian IT Act (2000) provides legal frameworks with key sections like 43, 66, and 67.
  - Section 66: Computer-related offenses (penalty: imprisonment up to 3 years and/or fine).
  - Section 67: Publishing obscene material (penalty: imprisonment up to 5 years and/or fine).

- Section 72: Breach of confidentiality and privacy (penalty: imprisonment up to 2 years and/or fine).
- Section 66A: Sending offensive messages (penalty: imprisonment up to 3 years and/or fine) (Note: Section 66A was struck down in 2015).

➔ Advantages of Cyber Law:

- Provides a legal framework.
- Protects rights in the digital space.
- Acts as a deterrent to cyber criminals.
- Promotes confidence in using digital technologies.

➔ Overview and Need of Cyber Crime Cell:

- A cyber-crime cell is a specialized unit in law enforcement that deals with cybercrime investigations and prosecutions. Cyber Crime Cells investigate cyber-crimes, collect evidence, and raise awareness.
- Investigate, prevent, and prosecute cyber-crimes.
- Address the complexity and sophistication of cyber-crimes.

➔ Cyber Fraud Helpline System:

- The Indian government has established a cyber fraud helpline system to report and investigate cybercrimes.
- Provides immediate assistance and guidance.

➔ Designated Helplines and Online Portals in India:

- Cyber Fraud Helpline Number: 1930
- National Cyber Crime Reporting Portal: www.cybercrime.gov.in provide assistance.
- Indian Computer Emergency Response Team (CERT-In): cert-in.org.in
- Cyber Crime Investigation Cell: Delhi Police Cyber Crime Unit
- National Cyber Security Coordinator (NCSC): National Cyber Coordination Centre (NCCC)
- Indian Cyber Crime Coordination Center (I4C): https://i4c.mha.gov.in/

Answer Key
Multiple Choice Questions (MCQs)

1. What is cyber-crime?
   a) Legal use of computers for business
   b) Criminal activities involving computers and the internet
   c) Developing computer software
   d) None of the above

2. Which of the following is a type of cyber-crime against individuals?
   a) Hacking
   b) Credit card fraud
   c) Cyber stalking
   d) Data breaches

3. What does the term "web jacking" refer to?
   a) Hacking into a computer system
   b) Taking control of a website for malicious purposes
   c) Sending phishing emails
   d) Installing malware on a computer

4. Under the Indian IT Act, what is the penalty for computer-related offenses under Section 66?

a) Imprisonment up to 3 years and/or fine
b) Imprisonment up to 5 years and/or fine
c) Imprisonment up to 2 years and/or fine
d) No penalty

5. What is the primary purpose of Cyber Crime Cells?

a) Selling computer hardware
b) Investigating, preventing, and prosecuting cyber crimes
c) Developing new software applications
d) Providing internet services

6. What is the role of the National Cyber Crime Reporting Portal?

a) Selling cybersecurity software
b) Reporting various types of cyber crimes
c) Providing internet connectivity
d) Conducting online exams

7. Which section of the Indian IT Act deals with publishing or transmitting obscene material in electronic form?

a) Section 66
b) Section 67
c) Section 72
d) Section 66A

8. Which organization handles cybersecurity incidents in India and provides alerts and advisories?

a) CERT-In
b) NCSC
c) FBI
d) Interpol

9. What is the main advantage of cyber law?

a) Promotes the use of paper documents
b) Provides a legal framework to address and prosecute cyber crimes
c) Discourages the use of digital technologies
d) Increases the cost of internet services

10. What is the helpline number for reporting cyber fraud in India?

a) 112
b) 1930
c) 100
d) 1800

11. Which section of the IT Act penalizes hacking?

a) Section 43

b) Section 66

c) Section 67

d) Section 72

12. What does CERT-In stand for?

a) Central Emergency Response Team

b) Computer Emergency Response Team

13. Which section of the IT Act deals with publishing obscene content?

a) Section 66

b) Section 67

c) Section 69

d) Section 68

14. Which portal is used for reporting cyber-crimes?

a) www.cybercrime.in

b) www.cybercrime.gov.in

c) www.cyberfraud.in

d) www.indiafraud.in

15. What is the primary law governing cybercrime in India?

a) Indian Penal Code
b) Information Technology Act, 2000
c) Cyber Law Act
d) Digital India Act

16. Which of the following is a type of cybercrime?

a) Hacking
b) Phishing
c) Identity Theft
d) All of the above

17.What is the penalty for hacking under the IT Act?

a) Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
b) Imprisonment up to 3 years and/or fine up to Rs. 5 lakhs
c) Imprisonment up to 5 years and/or fine up to Rs. 10 lakhs
d) Imprisonment up to 7 years and/or fine up to Rs. 20 lakhs

18. What is the purpose of a cyber-crime cell?

a) To promote e-commerce and digital economy
b) To regulate digital technologies and the internet
c) To investigate and prosecute cybercrimes
d) To provide a framework for cyber law

19. What is the penalty for publishing obscene information in electronic form under the IT Act?

   a) Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
   b) Imprisonment up to 3 years and/or fine up to Rs. 5 lakhs
   c) Imprisonment up to 5 years and/or fine up to Rs. 10 lakhs
   d) Imprisonment up to 7 years and/or fine up to Rs. 20 lakhs

20. What is the penalty for breach of confidentiality and privacy under the IT Act?

   a) Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
   b) Imprisonment up to 3 years and/or fine up to Rs. 5 lakhs
   c) Imprisonment up to 5 years and/or fine up to Rs. 10 lakhs
   d) Imprisonment up to 7 years and/or fine up to Rs. 20 lakhs

Fill in the Blanks

1. _______ refers to criminal activities that involve the use of computers and the internet.
2. Credit card fraud is an example of cyber-crime against _______.
3. _______ is the unauthorized access to computer systems to steal information or cause damage.
4. The Indian IT Act, 2000, is the primary legislation addressing _______ in India.
5. Publishing obscene material in electronic form is covered under Section _______ of the Indian IT Act.
6. The helpline number for reporting cyber frauds in India is _______.
7. _______ are specialized units within law enforcement agencies dedicated to handling cyber-crime cases.
8. The organization responsible for handling cybersecurity incidents in India is known as _______.
9. Using the internet to conduct acts of terrorism is referred to as _______.
10. The primary law governing cybercrime in India is the ______________________ Act, 2000.
11. Cybercrime can be classified into ______________________, computer-based crimes, and computer-assisted crimes.
12. The Indian government has established a ______________________ helpline system to report and investigate cybercrimes.
13. The penalty for hacking under the IT Act is imprisonment up to ______________________ years and/or fine up to Rs. 5 lakhs.
14. The cyber fraud helpline number in India is ______________________.
15. The National Cyber Crime Reporting Portal is a ______________________ for reporting cyber-crimes in India.

True or False

1. Email spoofing is a type of cyber-crime against organizations.
2. Skimming devices are used to capture card information at ATMs.
3. The Indian IT Act, 2000, does not address cyber-crimes.
4. Denial of Service (DoS) attacks are a type of cyber-crime against individuals.
5. Publishing obscene material in electronic form is covered under Section 66 of the Indian IT Act.
6. CERT-In handles cybersecurity incidents and provides alerts and advisories in India.
7. Cybercrime is a type of traditional crime.
8. The IT Act provides penalties for hacking, phishing, and identity theft.
9. The Indian government has established a cyber-crime cell to investigate and prosecute cybercrimes.
10. The cyber fraud helpline number in India is 100.

11. The National Cyber Crime Reporting Portal is an offline portal for reporting cyber-crimes in India.
12. The penalty for publishing obscene information in electronic form under the IT Act is imprisonment up to 2 years and/or fine up to Rs. 1 lakh.
13. The Indian Computer Emergency Response Team (CERT-In) deals with physical security incidents in India.
14. Cyber law provides a framework for regulating digital technologies, protects individuals and businesses from cybercrime, and promotes e-commerce and the digital economy.
15. The penalty for breach of confidentiality and privacy under the IT Act is imprisonment up to 5 years and/or fine up to Rs. 10 lakhs.

Short Answer Questions

1. What is cybercrime?
2. What are the primary categories of cyber-crime against individuals, property, organizations, and society?
3. Describe the significance of the Indian IT Act in combating cyber-crime.
4. Explain the role and importance of Cyber Crime Cells in law enforcement.
5. How does the Cyber Fraud Helpline system assist victims of cyber fraud in India?
6. Mention two advantages of cyber law.
7. What is the penalty for hacking under the IT Act?
8. What is the purpose of a cyber-crime cell?
9. What is the National Cyber Crime Reporting Portal?
10. What is the penalty for publishing obscene information in electronic form under the IT Act?
11. What is the role of the Indian Computer Emergency Response Team (CERT-In)?
12. What is the penalty for breach of confidentiality and privacy under the IT Act?

Long Answer Questions

1. Discuss the various types of cyber-crime and cyber fraud, providing examples and their impact on individuals, organizations, and society.
2. Analyze the key provisions and penalties of the Indian IT Act. How does this legislation address cyber-crimes and protect digital rights?
3. Explain the advantages of cyber law in promoting digital security and confidence. How do Cyber Crime Cells and helplines contribute to combating cyber-crime effectively?

Answer Key

Multiple Choice Questions

1. b), 2. c), 3. b), 4. a), 5. b), 6. b), 7. b), 8. a), 9. b), 10. b), 11. b), 12. b), 13. b), 14. b), 15. b), 16. d), 17. b), 18. c), 19. b), 20. a)

Fill-in-the-blanks

1. Cybercrime, 2. Individuals, 3. Hacking, 4. Cybercrime, 5. 67, 6. 1930, 7. Cyber Crime Cells, 8. CERT-In, 9. Cyberterrorism, 10. Information Technology, 11. Cybercrimes against individuals, 12. National Cyber Crime Reporting, 13. 3, 14. 1930, 15. Portal

True/False questions

1. True, 2. True, 3. False, 4. False, 5. False, 6. True, 7. False, 8. True, 9. True, 10. False (correct number is 1930), 11. False (it's an online portal), 12. True, 13. False, 14. True, 15. True

PSS Central Institute of Vocational Education

[A constituent unit of NCERT, Under Ministry of Education, Government of India)

Shyamla Hills, Bhopal - 462 002, Madhya Pradesh, India

www.psscive.ac.in